В.П.Платонов, А.С.Рапинчук

АЛГЕБРАИЧЕСКИЕ ГРУППЫ И ТЕОРИЯ ЧИСЕЛ

М.: Наука. Гл. ред. физ.-мат. лит., 1991, 656 с.

Первое в мировой математической литературе систематическое изложение арифметической теории алгебраических групп. Представлены практически все основные результаты арифметической теории линейных алгебраических групп, полученные к настоящему времени. Изложение начинается с обзора необходимых сведений из теории алгебраических групп и алгебраической теории чисел, что делает книгу доступной неспециалистам. По ходу изложения формулируется ряд нерешенных проблем и гипотез, которые могут явиться стимулом для новых исследований в этой активно развивающейся области современной математики.

Для математиков разных специальностей — студентов, аспирантов и научных работников.

ОГЛАВЛЕНИЕ

Предисловие 5

Глава I. Алгебраическая теория чисел 9

§ 1.1. Поля алгебраических чисел, их нормирования и пополнения 9

§ 1.2. Адели и идели. Сильная и слабая аппроксимации. Локально-глобальный принцип 20

§ 1.3. Когомологии 26

§ 1.4. Простые алгебры над локальными полями 38

§ 1.5. Простые алгебры над полями алгебраических чисел 49

Глава II. Алгебраические группы 60

§ 2.1. Структурные свойства алгебраических групп 60

§ 2.2. Классификация K-форм при помощи когомологий Галуа 82

§ 2.3. Классические группы 94

§ 2.4. Некоторые результаты из алгебраической геометрии 112

Глава III. Алгебраические группы над локально компактными полями 125

§ 3.1. Топология и аналитическая структура 125

§ 3.2. Архимедов случай 138

§ 3.3. Неархимедов случай 154

§ 3.4. Элементы теории Брюа — Титса 171

§ 3.5. Необходимые сведения из теории меры 182

Глава IV. Арифметические группы и теория приведения 195

§ 4.1. Арифметические группы 195

§ 4.2. Теория приведения (общая схема). Приведение в группе $GL_n(K)$ 200

§ 4.3. Приведение в произвольных группах 214

§ 4.4. Теоретико-групповые свойства арифметических групп 220

§ 4.5. Критерий компактности факторпространства G_R/G_Z 234

§ 4.6. Конечность объема факторпространства G_R/G_Z 240

§ 4.7. Заключительные замечания по теории приведения 251

§ 4.8. Конечные арифметические группы 257

Глава V. Адели **271**
§ 5.1. Основные определения 271
§ 5.2. Теория приведения для G_A относительно G_R 282
§ 5.3. Критерии компактности и конечности объема факторпространства G_A/G_K 291
§ 5.4. Теория приведения и структурные теоремы для S-арифметических подгрупп 298
Глава VI. Когомологии Галуа **312**
§ 6.1. Основные результаты 312
§ 6.2. Когомологии алгебраических групп над конечными полями 318
§ 6.3. Когомологии Галуа алгебраических торов 332
§ 6.4. Теоремы конечности для когомологий Галуа 348
§ 6.5. Когомологии полупростых алгебраических групп над локальными и числовыми полями 359
§ 6.6. Когомологии Галуа и квадратичные, эрмитовы и другие формы 377
§ 6.7. Доказательство теорем 4 и 6: группы классических типов 391
§ 6.8. Доказательство теорем 4 и 6: группы исключительных типов 404
Глава VII. Аппроксимация в алгебраических группах **435**
§ 7.1. Сильная и слабая аппроксимация в алгебраических многообразиях 435
§ 7.2. Гипотеза Кнезера — Титса 442
§ 7.3. Слабая аппроксимация в алгебраических группах 452
§ 7.4. Теорема о сильной аппроксимации 466
§ 7.5. Обобщения сильной аппроксимацнонной теоремы 472
Глава VIII. Числа и группы классов алгебраических групп **478**
§ 8.1. Числа классов алгебраических групп и числа классов в роде 479
§ 8.2. Числа и группы классов полупростых групп некомпактного типа. Теорема реализации 489
§ 8.3. Числа классов алгебраических групп компактного типа ЫI
§ 8.4. Оценки чисел классов редуктивных групп 524
§ 8.5. Проблема рода ЬЗЬ
Глава IX. Нормальное строение групп рациональных точек алгебраических групп **551**
§ 9.1. Основные гипотезы и результаты 552
§ 9.2. Группы типа A_n 561
§ 9.3. Группы классических типов 581
§ 9.4. Группы, разложимые над квадратичным расширением 591
§ 9.5. Конгруэнц-проблема (обзор) Ь9У
Дополнение ЫЬ
Список литературы 623
Основные обозначения 647
Предметный указатель 650

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Автоморфизм Фробениуса 15 Адели 20, 271

Аделизация морфизма 272
Алгебра Ли алгебраической группы 64
— — аналитической группы 135
Алгебраическая группа 60—61
— — анизотропная 80
— — диагонализируемая 66
— — изотропная 80
— — квазиразложимая 72
— — компактного типа 231, 256
— — *K*-определенная 62
— — *K*-разложимая 72
— — односвязная 77
— — полупростая 72
— — — некомпактного типа 231,256
— — — смешанного типа 231, 256
— — присоединенная 77
— — простая 77
— — разрешимая *K*-разложимая 71
— — редуктивная 72
— — унипотентная 70
Аналитическая структура 129—130
Анизотропное ядро 82
Аппроксимация сильная для алгебраической группы 279, 466
— — для многообразия 436
— — — — абсолютная 436
— — — поля 24
— слабая для алгебраической группы 452—465
— — для многообразия 436
— — — поля 24
Базис Шевалле 78
Бирациональный изоморфизм 114
BN-пара 172
Выделенная вершина 81
Гильбертово поле классов 482
Гипотеза Кнезера-Титса 39, 443
Гипотеза Маргулиса 554
— Платонова о проективной простоте 552
— — об арифметичности 477
Гомоморфизм инфляции 29
— кограничный 33
— коограничения 30
— ограничения 29
— трансгрессии 30
Группа аделей 278
— — главных 278
— — конечных 279
— — S-целых 278
— — целых 279
— арифметическая 195, 255
— Брауэра 39
— Вейля 74, 80, 173
— ветвления 19
— единиц 195
— иделей поля 21
— — главных 22
— — специальных 22
— — *S*-целых 22
— — целых 22
— инерции 19
— классов алгебраической группы 492
— — идеалов поля 10
— когомологий 26
— — Тейта 333
— компактно определенная 176
— конечных аделей 279
— кохарактеров 67
— ограниченной ширины 229
— ортогональная 96
— проконечная 159
— — типа (*F*) 349
— разложения 15
— *S*-аделей 279
— — главных 279
— — *T*-целых 279
— самосопряженная 144
— *S*-арифметическая 200, 298
Группа *S*-единиц 298
— симплектическая 96
— специальная линейная 94
— — ортогональная 96
— — унитарная 100
— спинорная 98
— унимодулярная 184

— унитарная 98, 100
— финитно аппроксимируемая относительно сопряженности 543
— характеров 66
— Шафаревича—Тейта 315, 357
— Шевалле 80
Действие группы на многообразии 115
Дифференциальная форма 190
— — инвариантная 190
Доминантный морфизм 112
Идеал дробный 10
— нормирования 14
Идели поля 21
Изогения 69, 76
Инвариант тела 41
— простой алгебры 41
— Хассе—Витта 384
Инволюция 98
— второго рода 99
— первого рода 99
— — — второго типа 101
— — — первого типа 101
Индекс ветвления 14
— Витта 98
— простой алгебры 38
— тела 38
— Титса 81—82
Индуцированное множество 36
Интегрирование дифференциальной формы 192—193
Касательное пространство 113, 131
Класс решетки 488
— элемента 484
Классификация K-форм алгебраических групп 91—94
— полупростых алгебраических групп 77—78
Когомологии 26—37
— алгебраических групп 87
— — — вещественные 353
— Галуа 31
— групп аделей 329—332
— — целых v-адических точек 324—329
— неабелевы 31—37
— непрерывные 30
— неразветвленные 327
Когомологии Тейта 333
Когомологическая размерность 375
Кограничное отображение 88
Кольцо аделей 20
— — главных 21
— — конечных 23
— — S-целых 20
— — целых 20
— дедекиндово 10
— нормирования 14
— S-аделей 23
— — T-целых 23
— S-целых элементов 21
Конгруэнц-гипотеза Серра 601
Конгруэнц-подгруппа 43, 155, 197, 598
Конгруэнц-проблема 598
Конгрунэц-теорема 569
Конгруэнц-топология 600
Конгруэнц-ядро 600
Корневая подгруппа 388, 592
Критерий Малера 238
— компактности факторпространства G_R/G_Z 237
— — — G_A/G_K 291
— — — $G_S/G_{O(S)}$ 299
— конечности объема факторпространства G_R/G_Z 240
— — — — G_A/G_K 291
— — — — $G_S/G_{O(S)}$ 299
— свободы решетки 482
Лемма Гензеля 165
— Краснера 350
— —, унитарный вариант 400
— Минковского 261, 534
— о замкнутых орбитах 116
— Шапиро 30, 36

Локально-глобальный принцип (принцип Хассе) 24—25
— — для алгебраических групп 317
— — — когомологий арифметических групп 532
— — — односвязных алгебраических групп 317
— — — полуторалинейных форм 381—382
— — — — — сильный 382
— — — — — слабый 382
— — — торов 315, 340
— — мультинорменный 346
— — норменный 25, 340—346
L/K-форма 82
Мера 182—194
— борелевская 183
— инвариантная 183
— на произведении 184
Мера на факторпространстве 186—187
— Тамагавы 291
— Хаара 183
Метаплектическое ядро 602
Многомерный класс сопряженности 117
Многообразие борелевских подгрупп 123
— гладкое 114
— *K*-определенное 112
— представлений 120
— рациональное 114
— торов 121
— унирациональное 115
— характеров 474
Многочлен Эйзенштейна 19
Множители сходимости 291
Модуль автоморфизма 184
— группы 184
Морфизм алгебраических групп 62
— — — *K*-определенный 62
Мультипликативная арифметика 580
Мультипликатор Шура 28, 344
Накрытие универсальное 77, 92
— специальное 92
Норма приведенная 38
Нормирование поля 10
— — архимедово 11
— — вещественное 13
— — комплексное 13
— — логарифмическое 11
— — неархимедово 11
— — нормализованное 22
— — *p*-адическое 11
— тела 40
Нормирования эквивалентные 11
Область Зигеля 201
— — обобщенная 252
— — относительная 242
Ограничение основного поля 62
Ограниченное топологическое произведение 185
Определитель Дьедонне 51
Основа 172
Отображение логарифмическое 136
— — усеченное 70
— редукции 165
— экспоненциальное 136
— — усеченное 70
Параметризация Кэли—Диксона 440
Подгруппа арифметическая 195, 255
— Бореля 71
— Ивахори 172
— параболическая 72
Подгруппа параболическая стандартная 76
— парахорическая 172
— *S*-арифметическая 200, 298
— соизмеримости 233
Поле вычетов 14
— локальное 13—14
— определения 112
— разложения 38, 66
— типа (*F*) 349
— числовое 9
Пополнение 12
Порядок 54
— локальный 54

— максимальный 54
Последовательность Хохшильда—Серра 30
— — для неабелевых когомологий 36
Препятствие к принципу Хассе 342 — 344
— — — — первое 342
Приведенная группа Уайтхеда 39
— — — унитарная 446
Принцип Хассе — см. локально-глобальный принцип
Присоединенное представление 65
Проблема Бартельса 341
— Гротендика 474
— рода 535—549
— — в арифметических группах 535
— — для целочисленных представлений 545
— Таннака—Артина 39, 446
Продолжение нормирования 11
Проективная система 159
Проективный предел 159
Про-p-группа 160
— силовская 160
Простая точка редукции 164
Пространство аделей 271
— — главных 272
— — S-целых 272
— — целых 272
Процедура выбрасывания вершин 448
Псевдобазис 54
Радикал 72
— унипотентный 72
Ранг 72
— над K 80
Расширение полей адекватное 341
— — вполне вещественное 258
— — — разветвленное 14
— — неразветвленное 14
Разложение Брюа 74
— Жордана 65
Разложение Жордана аддитивное 65
— Ивасавы в GL_n(R) 150
— — — произвольной группе 152
— Картана 174
— Леви 72
— полярное в GL_n(R)142
— — — произвольной группе 146
Реализация алгебраической группы 479
Регулярный полупростой элемент 76
Редукция 163, 169
— гладкая 164
Решетка (на векторном пространстве) 53
— локальная 54
— (в локально компактной группе 248
Род решетки 488
— элемента 484
—Связная компонента 65
Система корней 73
— — относительная 80
— простых корнел 73
— Титса — см. BN-пара
Скручивание 34, 83
Слабая метаплектическая гипотеза 576, 605
— Список классических групп 108
Стабилизатор решетки 56, 57
Стандартное описание нормальных делителей 581
—Степень алгебраической группы 61
— поля вычетов 14
Тело вычетов 40
Теорема Бартельса—Китаоки 262
— Бера 176
— Бореля о плотности 231
— Бореля—Хариш-Чандры 217
— Ванга 50
— Витта 109
— — для алгебры октав 589
— 90 Гильберта 85
— Дирихле о единицах 236
— — — — обобщенная 311

— инвариантности для арифметических подгрупп 199, 230
— — для S-арифметических подгрупп 301
— Э. Картана 137, 444
— Кнезера 502
— конечности для орбит арифметических групп 218
— — — — групп аделей 287
— — — — S-арифметических групп 300
Теорема конечности для числа классов 280
— — несопряженных конечных подгрупп 199, 302
— Ландера 395
— Ленга 313
— — об изогениях 322
— Маргулиса 560
— Мацумото 161
— Мейера 377
— Минковского—Хассе 25
— Мостова 144, 148
— Накаямы—Тейта локальная 314
— — глобальная 315
— Нётер 165
— о конечной определенности арифметических групп 199, 220
— — — — S-арифметических групп 304
— — неограниченности чисел классов 525
— — реализации 492
— — сильной аппроксимации 24, 466
— — слабой аппроксимации 24,452— 453
— — стабилизаторе 484
— — централизаторе 488
— об обратной функции 129
— — одноклассных решетках 492
— Островского 11
— Платонова 451, 464
— — о слабой аппроксимации над произвольным полем 465
— — об изогениях 444
— Платонова—Бондаренко—Рапинчука 527
— Платонова—Янчевского 42
— плотности Чеботарева 18
— Прасада—Маргулиса 559
— Прасада—Рагунатана 449, 606
— Рапинчука 613
— Рима 134
— Рольфса 531
— Сколема—Нётер 38
— Стейнберга 372, 376
— Тейта 334, 339, 341
— Титса 443
— Уитни 138
— Фробениуса 320
— Хариш-Чандры 208
— Хассе о нормах 341
— Хассе—Брауэра—Нётер 49
— Черноусова 424
— Шевалле 116
— — усиленная 116
— Эйхлера 50
— —, унитарный вариант 396
Теорема Эрмита 19
Теоремы конечности для когомологий Галуа 326, 348
Теория приведения 200—220
— — для арифметических групп 214
— — — GL_n(R) 200
— — — групп аделей 282—290
— — — S-арифметических групп 298—299
Топология адельная 20, 272
— арифметическая 600
— v-адическая 126
— идельная 21
Тор (алгебраический) 66
— анизотропный 67
— квазиразложимый 68
— мультинорменный 68

— норменный 68
— разложимый 66
Точка простая 114
— особая 114
Униформизующий элемент 14
— — в теле 40
Фактормногообразие 65
Форма внешняя 81
Форма внутренняя 81
— Киллинга 65
Формула произведения 22
Фундаментальная группа алгебраической группы 77
— область 187, 204
Фундаментальное множество 188, 218, 256, 283, 298
Характер 66
Центры простых односвязных групп- 79, 366
Число классов алгебраической группы 280, 479
— — в роде 484
— — — — квадратичной формы 486, 502, 515
— — — — решетки 488
— — — — — на $M_n(K)$относительно сопряженности 505
— — — — целочисленного представления 487
— — — — целочисленной матрицы относительно сопряженности 488
— — идеалов поля 10
— Тамагавы 292, 297

ПРЕДИСЛОВИЕ

Данная книга представляет собой первое в мировой математической литературе систематическое изложение теории, лежащей на стыке теории групп, алгебраической геометрии и теории чисел. Это направление исследований сравнительно недавно оформилось в самостоятельную область математики, которую часто называют арифметической теорией алгебраических (линейных) групп. В 1967 году в предисловии к своей книге «Основы теории чисел» А. Вейль писал: «Прокладывая курс своего корабля, я старался избегать арифметической теории алгебраических групп, это весьма интересный предмет, но он, очевидно, не созрел еще для изложения в книге».

У истоков арифметической теории линейных алгебраических групп лежат классические исследования по арифметике квадратичных форм (Гаусс, Эрмит, Минковский, Хассе, Зигель), структуре групп единиц полей алгебраических чисел (Дирихле), дискретным подгруппам групп Ли в связи с теорией автоморфных функций, топологией и кристаллографией (Риман, Клейн, Пуанкаре и др.). Но именно последние 20—25 лет были периодом ее чрезвычайно интенсивного развития. В эти годы была построена теория приведения для арифметических групп, изучены свойства групп аделей и решена проблема сильной аппроксимации, получены глубокие результаты о строении групп рациональных точек над локальными и глобальными полями, исследованы различные варианты локально-глобального принципа для алгебраических групп, в существенной степени решена конгруэнц-проблема для изотропных групп.

Даже из этого далеко не полного перечня основных достижений арифметической теории линейных алгебраических групп видно, что накоплен большой содержательный материал, представляющий значительный интерес для математиков разных специальностей. К сожалению, главные результаты здесь и по сей день доступны лишь в форме журнальных публикаций, хотя необходимость их обстоятельного изложения с единых позиций назрела уже давно. Однако появление соответствующей книги задерживалось, что в существенной мере объясняется трудностью монографического изложения теории из-за обилия

глубоких результатов и синтетичности используемых методов, относящихся к алгебре, алгебраической геометрии, теории чисел, анализу и топологии. И вот, наконец, такая книга предлагается читателю.

Первые две главы имеют вводный характер и содержат основные результаты алгебраической теории чисел и теории алгебраических групп, широко используемые в последующих главах.

В третьей главе излагаются основные факты о строении алгебраических групп над локально компактными полями. Некоторые из них остаются справедливыми и в случае любого поля, полного относительно дискретного нормирования.

В четвертой главе представлено все наиболее существенное об арифметических группах, базирующееся на результатах А. Бореля и Хариш-Чандры.

Одним из основных инструментов исследования в арифметической теории алгебраических групп являются группы аделей, свойства которых изучаются в гл. V.

Центральное место в шестой главе, несомненно, занимает полное доказательство принципа Хассе для односвязных алгебраических групп, которое в окончательном виде публикуется впервые.

В седьмой главе исследуется сильная и слабая аппроксимация в алгебраических группах. В частности, приводится решение проблемы сильной аппроксимации и доказательство гипотезы Кнезера — Титса над локальными полями, полученные первым из авторов книги.

Под влиянием классических проблем о числе классов в роде квадратичных форм и о числе классов идеалов полей алгебраических чисел возникла необходимость в изучении чисел классов для произвольных алгебраических групп, определенных над числовыми полями. Основные результаты, полученные к настоящему времени, излагаются в гл. VIII. Большинство из них принадлежит авторам.

Девятая глава, посвященная группам рациональных точек, занимает особое место в книге по новизне и сложности результатов. В последние годы в этой области был достигнут значительный прогресс. В первую очередь здесь следует отметить работы Кнезера, Маргулиса, Платонова, Рапинчука, Прасада, Рагунатана и др. о нормальном строении групп рациональных точек анизотропных групп и мультипликативной арифметике тел, использующие весь арсенал арифметической теории алгебраических групп. Ряд результатов публикуется здесь впервые.

В заключительном параграфе этой главы приводится обзор новейших результатов по так называемой конгруэнц-проблеме.

Таким образом, в книге представлены (в разной степени) почти все основные результаты арифметической теории линейных алгебраических групп, полученные к настоящему времени. В то же время круг вопросов, связанных с конгруэнц-проблемой, заслуживает самостоятельного монографического изложения, и авторы намерены вернуться к этой теме в ближайшем будущем. Не затронута у нас и такая важная тема как когомологии арифметических групп. Тем не менее в книге содержится весь необходимый для этого подготовительный материал (за исключением некоторых фактов чисто топологического характера), так что заинтересованный читатель, после ознакомления с соответствующими разделами книги, сможет перейти к чтению весьма обширной литературы по когомологиям арифметических групп и их связям с теорией представлений.

Отметим, что для многих известных утверждений (особенно в гл. V, VI, VII, IX) мы даем новые доказательства, как правило, более концептуальные. В ряде мест эффективно используется геометрический подход к классификации представлений групп с конечным числом образующих.

По ходу изложения мы формулируем значительное число нерешенных проблем и гипотез, которые могут явиться стимулом для новых исследований в этой активно развивающейся области современной математики.

Большинство результатов, изложенных в книге, либо распространяется на случай алгебраических групп над глобальными полями положительной характеристики, либо имеет в этом случае свои аналоги. Во многих ситуациях это достигается путем незначительной модификации рассуждений, однако иногда связано с использованием других подходов и развитием принципиально новой техники. В целом приходится констатировать, что арифметическая теория алгебраических групп в положительной характеристике пока не обрела той стройности и завершенности, какая имеет место для случая полей алгебраических чисел. По этой причине мы приняли решение не уделять случаю положительной характеристики специальное внимание, ограничиваясь краткими комментариями библиографического характера.

На структуру книги и изложение многих ее результатов существенное влияние оказала обзорная статья В. П. Платонова «Арифметическая теория алгебраических групп», опубликованная в журнале «Успехи математических наук» (1982. № 3. С. 3—54).

При подготовке рукописи к печати большую помощь нам оказали О. И. Тавгень, Ю. А. Дракохруст, В. В. Беняш-Кривец, В. В. Курсов, И. И. Воронович. Особо следует отметить вклад В. И. Черноусова, который предоставил нам полное доказательство принципа Хассе для односвязных групп и затратил

немало времени на усовершенствование изложения в гл. VI. Всем им мы сердечно благодарны.

О нумерации: теоремы, леммы и предложения нумеруются отдельно в пределах каждой главы. При ссылках указывается сначала номер главы, а потом номер утверждения; например, ссылаясь на теорему 4.6, мы имеем в виду теорему 6 из гл. IV.

В. П. Платонов
А. С. Рапинчук

ГЛАВА I

АЛГЕБРАИЧЕСКАЯ ТЕОРИЯ ЧИСЕЛ

Настоящая глава носит вводный характер. В первых двух параграфах мы даем краткий обзор некоторых понятий и результатов теоретико-числового характера. Подробное изложение этих вопросов содержится в книгах Ленга [2], Вейля [7] (см. также гл. 1—3 книги [АТЧ]). Отметим только, что в отличие, скажем, от Вейля мы формулируем результаты лишь для случая числовых полей, хотя подавляющее большинство их справедливо и в случае глобальных полей положительной характеристики, т. е. полей алгебраических функций с конечным полем констант. В § 1.3 излагаются необходимые для дальнейшего сведения о когомологиях групп, включая определение и простейшие свойства некоммутативных когомологий. В § 1.4—1.5 содержатся основные результаты о простых алгебрах над локальными и глобальными полями. При этом особое внимание уделяется исследованию мультипликативной структуры алгебр с делением над этими полями, в частности, тривиальности приведенной группы Уайтхеда. Кроме того, в § 1.5 мы приводим в удобной для нас форме результаты о решетках на векторных пространствах и порядках в полупростых алгебрах.

На протяжении всей книги мы предполагаем у читателя хорошее знание теории полей, в частности, теории Галуа (конечной и бесконечной), а также элементов топологической алгебры, включая теорию проконечных групп.

§ 1.1. Поля алгебраических чисел, их нормирования и пополнения

1. Арифметика полей алгебраических чисел. Пусть K — поле алгебраических чисел, т. е. конечное расширение поля $\mathbb{Q}$, $\mathcal{O}_K$ — кольцо целых элементов K. Кольцо $\mathcal{O}_K$ является классическим объектом алгебраической теории чисел. Изучение его структуры и арифметики, начатое Гауссом, Дедекиндом, Дирихле и другими в прошлом веке, активно продолжается и по сей день. С чисто алгебраической точки зрения кольцо $\mathcal{O}=\mathcal{O}_K$ устроено весьма просто: если $[K:\mathbb{Q}]=n$, то $\mathcal{O}$ является свободным $\mathbb{Z}$-модулем ранга n. Для любого ненулевого идеала $\mathfrak{a}\subset\mathcal{O}$ факторкольцо $\mathcal{O}/\mathfrak{a}$ конечно; в частности, любой простой идеал максимален. В теории колец кольца с такими свойствами (а именно

нетеровы, целозамкнутые, каждый простой идеал которых максимален) называются *дедекиндовыми*. Из дедекиндовости кольца $\mathcal{O}$ вытекает, что любой ненулевой идеал $\mathfrak{a} \subset \mathcal{O}$ однозначно разлагается в произведение простых идеалов: $\mathfrak{a} = \mathfrak{p}^{a_1} \ldots \mathfrak{p}^{a_r}$. Это свойство является обобщением основной теоремы арифметики об однозначности разложения любого целого числа в произведение простых чисел. Тем не менее полная аналогия здесь отсутствует: однозначность разложения элементов кольца $\mathcal{O}$ на неприводимые, вообще говоря, не имеет места. Этот факт, показывающий, что арифметика кольца $\mathcal{O}$ может существенно отличаться от арифметики кольца целых чисел $\mathbb{Z}$, явился ключевым моментом в осмыслении задач алгебраической теории чисел. Точной мерой отклонения является так называемая группа классов идеалов (или, как говорили раньше, дивизоров) поля K. Ее элементами являются *дробные идеалы* поля K, т. е. такие $\mathcal{O}$-подмодули $\mathfrak{a} \subset K$, что $x\mathfrak{a} \subset \mathcal{O}$ для подходящего $x \in \mathcal{O}$, $x \neq 0$. Беря в качестве произведения двух дробных идеалов $\mathfrak{a}, \mathfrak{b} \subset K$ $\mathcal{O}$-подмодуль в K, порожденный всеми произведениями xy, где $x \in \mathfrak{a}$, $y \in \mathfrak{b}$, мы получаем операцию на множестве дробных идеалов, относительно которой оно оказывается группой $\mathrm{Id}(\mathcal{O})$, называемой *группой идеалов* поля K. *Главные дробные идеалы*, т. е. идеалы вида $x\mathcal{O}$, где $x \in K^*$, образуют подгруппу $P(\mathcal{O}) \subset \mathrm{Id}(\mathcal{O})$ и факторгруппа $\mathrm{Cl}(\mathcal{O}) = \mathrm{Id}(\mathcal{O})/P(\mathcal{O})$ называется *группой классов идеалов поля* K. Классический результат, восходящий к Гауссу, состоит в том, что группа $\mathrm{Cl}(\mathcal{O})$ всегда конечна; ее порядок, обозначаемый h_K, есть *число классов* поля K. При этом разложение элементов из $\mathcal{O}$ на неприводимые однозначно в том и только том случае, если $h_K = 1$. Другой классический результат (теорема Дирихле о единицах) устанавливает конечную порожденность группы обратимых элементов $\mathcal{O}^*$. Эти два факта явились отправным пунктом при построении арифметической теории алгебраических групп (см. предисловие). При этом распространение классической арифметики на алгебраические группы, естественно, не могло идти по линии обобщения «внутренней» арифметики поля K и кольца $\mathcal{O}$, ибо в ней существенную роль играют кольцевые соображения, неприменимые в случае произвольной алгебраической группы, а потребовало привлечения развитых в теории чисел внешних конструкций, таких, как нормирования, пополнения, а также адели, идели и др.

2. Нормирования полей алгебраических чисел и их пополнения. *Нормированием* поля K называется функция $|\,|_v\colon K \to \mathbb{R}$, удовлетворяющая условиям:

1) $|x|_v \geqslant 0$, причем $|x|_v = 0$ тогда и только тогда, когда $x = 0$,

2) $|xy|_v = |x|_v |y|_v$,

3) $|x+y|_v \leqslant |x|_v + |y|_v$.

Если наряду с 3) выполняется более сильное условие

3′) $|x+y|_v \leqslant \max\{|x|_v, |y|_v\}$,

то нормирование называется *неархимедовым*, в противном случае — *архимедовым*.

Примером нормирования может служить тривиальное нормирование, которое определяется следующим образом: $|x|_v = 1$ при всех $x \in K^*$ и $|0|_v = 0$. Примеры нетривиальных нормирований приведем вначале для случая $K = \mathbb{Q}$. Так, на $\mathbb{Q}$ существует архимедово нормирование $|\ |_\infty$, индуцируемое обычной абсолютной величиной. Далее, с каждым простым числом p можно связать нормирование $|\ |_p$, называемое p-адическим. А именно, представив произвольное рациональное число $\alpha \neq 0$ в виде $\alpha = p^r \cdot \beta/\gamma$, где $r, \beta, \gamma \in \mathbb{Z}$, причем β и γ не делятся на p, полагаем $|\alpha|_p = p^{-r}$ и $|0|_p = 0$. Иногда бывает удобно вместо p-адического нормирования $|\ |_p$ рассматривать соответствующее логарифмическое нормирование $v = v_p$, которое определяется формулой $v(\alpha) = r$ и $v(0) = -\infty$, так что $|\alpha|_p = p^{-v_p(\alpha)}$. Аксиоматически v задается условиями:

1) $v(x)$ есть элемент аддитивной группы целых чисел $\mathbb{Z}$ (или другой упорядоченной группы) и $v(0) = -\infty$,

2) $v(xy) = v(x) + v(y)$,

3) $v(x+y) \geqslant \min\{v(x), v(y)\}$.

Мы будем пользоваться как обычными нормированиями, так и соответствующими логарифмическими нормированиями; из контекста всегда будет ясно, о каком нормировании идет речь.

Замечательно, что приведенными примерами исчерпываются, фактически, все нетривиальные нормирования поля $\mathbb{Q}$.

Теорема 1 (Островский). *Любое нетривиальное нормирование поля $\mathbb{Q}$ эквивалентно либо архимедову нормированию $|\ |_\infty$, либо одному из p-адических нормирований $|\ |_p$.*

(Напомним, что два нормирования $|\ |_1$ и $|\ |_2$ на поле K называются эквивалентными, если они индуцируют на K одну и ту же топологию; в этом случае $|\ |_1 = |\ |_2^\lambda$ для подходящего положительного вещественного числа λ.)

Таким образом, ограничивая любое нетривиальное нормирование $|\ |_v$ некоторого поля алгебраических чисел K на поле $\mathbb{Q}$, мы получим либо архимедово нормирование $|\ |_\infty$ (или эквивалентное ему), либо одно из p-адических нормирований (можно показать, что ограничение нетривиального нормирования обязательно нетривиально). Тем самым любое нетривиальное нормирование поля K получается *продолжением* на K одного из нормирований поля $\mathbb{Q}$. С другой стороны, известно, что для любого алгебраического расширения L/K и любого нормирования $|\ |_v$ поля K существует его продолжение на L, т. е. такое

нормирование $|\ |_w$ поля L, что $|x|_w = |x|_v$ для всех $x \in K$ (в этом случае пишут $w|v$). В частности, исходя из указанных нормирований поля $\mathbb{Q}$, мы можем получать нормирования произвольного числового поля K. Проанализируем процедуру продолжения более подробно. Для этого удобно ввести вначале пополнение K_v поля K относительно нормирования $|\ |_v$. А именно, рассмотрев пополнение K как метрического пространства относительно расстояния, определяемого нормированием $|\ |_v$, мы получим полное метрическое пространство K_v, которое наделяется естественными операциями и тем самым превращается в поле, полное относительно соответствующего продолжения нормирования $|\ |_v$, для которого мы сохраняем прежнее обозначение. Известно, что если L — алгебраическое расширение поля K_v (и вообще любого поля, полного относительно некоторого нормирования $|\ |_v$), то нормирование $|\ |_v$ обладает единственным продолжением $|\ |_w$ на L (ниже, пользуясь фактом существования и единственности продолжения, мы получим явную формулу для $|\ |_w$, которую читатель может принять в качестве определения $|\ |_w$). В частности, $|\ |_v$ однозначно продолжается до нормирования алгебраического замыкания $\bar{K}_v$. Отсюда следует, что $|\sigma(x)|_w = |x|_w$ для любого $x \in \bar{K}_v$ и любого $\sigma \in \mathrm{Gal}(\bar{K}_v/K_v)$. Пусть теперь L/K_v — конечное расширение степени n и $\sigma_1, \ldots, \sigma_n$ — различные вложения L в $\bar{K}_v$ над K_v. Тогда для любого $a \in L$ и его нормы $\mathrm{N}_{L/K}(a)$ имеем

$$|\mathrm{N}_{L/K}(a)|_v = \left|\prod_{i=1}^{n} \sigma_i(a)\right|_v = \prod_{i=1}^{n} |\sigma_i(a)|_w = |a|_w^n.$$

В результате получаем явное описание продолжения $|\ |_w$:

$$|a|_w = |\mathrm{N}_{L/K}(a)|_v^{1/n} \quad \text{для любого} \quad a \in L. \tag{1}$$

Рассмотрим теперь вопрос о продолжении нормирований на конечное расширение L/K, где K — поле алгебраических чисел. Пусть $|\ |_v$ — нормирование поля K и $|\ |_w$ — его единственное продолжение на алгебраическое замыкание $\bar{K}_v$. Тогда для любого вложения τ: $L \to \bar{K}_v$ над K (а их имеется n штук, где $n = [L:K]$) можно определить нормирование $|x|_u = |\tau(x)|_w$ на поле L, которое, как легко видеть, продолжает исходное нормирование $|\ |_v$ поля K. В этом случае пополнение L_u может быть отождествлено с композитом $\tau(L)K_v$. При этом любое продолжение получается таким образом, а два вложения τ_1, τ_2: $L \to \bar{K}_v$ задают одно и то же продолжение, если они сопряжены над K_v, т. е. существует $\lambda \in \mathrm{Gal}(\bar{K}_v/K_v)$ со свойством $\tau_2 = \lambda\tau_1$. Другими словами, если $L = K(\alpha)$ и $f(t)$ — неприводимый полином элемента α над K, то продолжения $|\ |_{u_1}, \ldots, |\ |_{u_r}$ нормирования $|\ |_v$ на L взаимно однозначно соответствуют множителям в раз-

ложении $f(t)=f_1(t)\ \ldots\ f_r(t)$ полинома f на неприводимые над полем K_v, а именно $|\ |_{u_i}$ отвечает вложению $\tau_i\colon L\to\bar{K}_v$, переводящему α в некоторый корень многочлена f_i. При этом пополнение L_{u_i} является конечным расширением K_v, порождаемым корнем f_i. Отсюда следует, что

$$L\bigotimes_K K_v\simeq\bigoplus_{i=1}^{r}L_{u_i};\tag{2}$$

в частности, степень $[L:K]$ есть сумма всех локальных степеней $[L_{u_i}:K_v]$.

Кроме того, имеют место следующие формулы для нормы и следа элемента $a\in L$:

$$\begin{aligned}\mathrm{N}_{L/K}(a)&=\prod_{u\mid v}\mathrm{N}_{L_u/K_v}(a),\\ \mathrm{Tr}_{L/K}(a)&=\sum_{u\mid v}\mathrm{Tr}_{L_u/K_v}(a).\end{aligned}\tag{3}$$

Таким образом, множество V^K всех попарно неэквивалентных нормирований поля K (лучше сказать, классов эквивалентности нормирований K) является объединением конечного множества V_∞^K архимедовых нормирований, которое состоит из продолжений на K нормирования $|\ |_\infty$ поля $\mathbb{Q}$, индуцируемого обычной абсолютной величиной, и множества V_f^K неархимедовых нормирований, которые получаются продолжением p-адических нормирований $|\ |_p$ поля $\mathbb{Q}$. Архимедовы нормирования отвечают вложениям K либо в поле вещественных чисел $\mathbb{R}$, либо в поле комплексных чисел $\mathbb{C}$ (но не в $\mathbb{R}$), и тогда они называются соответственно вещественными или комплексными нормированиями (при этом соответствующие пополнения совпадают либо с $\mathbb{R}$, либо с $\mathbb{C}$). Если $v\in V_\infty^K$ — вещественное нормирование, то элемент $\alpha\in K$ называется положительным относительно v, если при соответствующем вложении он переходит в положительное число. Обозначим через s (соответственно t) число вещественных (соответственно попарно несопряженных комплексных) вложений K; тогда $s+2t=n$ — степень L над K.

Неархимедовы нормирования приводят к более сложным пополнениям. А именно, если нормирование $v\in V_f^K$ является продолжением p-адического нормирования, то пополнение K_v является конечным расширением поля p-адических чисел $\mathbb{Q}_p$. Поэтому из локальной компактности поля $\mathbb{Q}_p$ вытекает локальная компактность поля K_v (имеется в виду топология, определяемая нормированием)*). Замыкание кольца целых $\mathcal{O}$ в K_v

*) В дальнейшем пополнения числового поля относительно его нетривиальных нормирований называются локальными полями. Можно показать, что определенный таким образом класс локальных полей совпадает с

совпадает с **кольцом нормирования** $\mathcal{O}_v = \{a \in K_v \mid |a|_v \leqslant 1\}$, которое иногда называют кольцом целых v-адических чисел. Кольцо $\mathcal{O}_v$ является локальным кольцом с максимальным идеалом $\mathfrak{p}_v = \{a \in K_v \mid |a|_v < 1\}$ (называемым идеалом нормирования) и группой обратимых элементов $U_v = \mathcal{O}_v \setminus \mathfrak{p}_v = \{a \in K_v \mid |a|_v = 1\}$. Легко видеть, что для поля p-адических чисел $\mathbb{Q}_p$ кольцо нормирования совпадает с кольцом целых p-адических чисел $\mathbb{Z}_p$, а идеал нормирования есть $p\mathbb{Z}_p$. В общем случае $\mathcal{O}_v$ является свободным модулем над кольцом целых p-адических чисел $\mathbb{Z}_p$, ранг которого совпадает со степенью $[K_v : \mathbb{Q}_p]$, так что $\mathcal{O}_v$ служит открытым компактным подкольцом в K_v. При этом полную систему окрестностей нуля в $\mathcal{O}_v$ образуют степени $\mathfrak{p}_v^i$ идеала $\mathfrak{p}_v$. Факторкольцо $k_v = \mathcal{O}_v/\mathfrak{p}_v$ является конечным полем и носит название *поля вычетов* нормирования v. Идеал $\mathfrak{p}_v \subset \mathcal{O}_v$ оказывается главным; любая его образующая π называется *униформизующим элементом* и характеризуется тем свойством, что $v(\pi)$ является (положительной) образующей *группы значений* $\Gamma = v(K_v^*) \simeq \mathbb{Z}$. Зафиксировав униформизующий элемент π, мы для любого элемента $a \in K_v^*$ получаем представление $a = \pi^r u$, где $u \in U_v$, которое приводит к изоморфизму топологических групп $K_v^* \simeq \mathbb{Z} \times U_v$, $a \mapsto (r, u)$, где группа $\mathbb{Z}$ наделяется дискретной топологией. Поэтому для выяснения структуры K_v^* остается описать группу U_v. Несложно показать, что U_v является компактной группой, которая локально изоморфна $\mathcal{O}_v$. Отсюда следует, что $U_v \simeq F \times \mathbb{Z}_p^n$, где $n = [K_v : \mathbb{Q}_p]$, F — группа всех корней из единицы в K_v. Таким образом, $K_v^* \simeq \mathbb{Z} \times F \times \mathbb{Z}_p^n$.

При изучении арифметики полей и их расширений важную роль играют понятия индекса ветвления и степени поля вычетов, которые мы введем вначале в локальной ситуации. Пусть L_w/K_v — конечное расширение степени n. Тогда группа значений $\Gamma_v = v(K_v^*)$ имеет конечный индекс в группе значений $\Gamma_w = w(L_w^*)$, и соответствующий индекс $e(w|v) = [\Gamma_w : \Gamma_v]$ называется *индексом ветвления*. Поле вычетов $l_w = \mathcal{O}_{L_w}/\mathfrak{P}_{L_w}$ для L_w является конечным расширением поля вычетов k_v, и степень $f(w|v) = [l_w : k_v]$ называется *степенью поля вычетов*. При этом $e(w|v)f(w|v) = n$. Расширения, для которых $e(w|v) = 1$, называются *неразветвленными*, а расширения, для которых $f(w|v) = 1$, — *вполне разветвленными*.

Пусть теперь L/K — конечное расширение полей алгебраических чисел степени n. Тогда для любого нормирования $v \in V_f^K$

классом недискретных локально компактных полей. Отметим также, что мы будем преимущественно использовать термин «локальное поле» применительно к неархимедовым пополнениям, причем, желая подчеркнуть это обстоятельство, мы будем говорить «неархимедово локальное поле».

и любого его продолжения w на поле L индекс ветвления $e(w|v)$ и степень поля вычетов $f(w|v)$ определяются соответственно как индекс ветвления и степень поля вычетов соответствующего расширения пополнений L_w/K_v. (Можно дать и внутреннее определение, основанное на рассмотрении групп значений $\tilde{\Gamma}_v = v(K^*)$, $\tilde{\Gamma}_w = w(L^*)$ и полей вычетов

$$\tilde{k}_v = \mathcal{O}_K(v)/\mathfrak{p}_K(v), \quad \tilde{l}_w = \mathcal{O}_L(w)/\mathfrak{P}_L(w),$$

где $\mathcal{O}_K(v)$, $\mathcal{O}_L(w)$ — кольца нормирований v и w в полях K и L, $\mathfrak{p}_K(v)$, $\mathfrak{P}_L(w)$ — соответствующие идеалы нормирований, однако в действительности $\tilde{\Gamma}_v = \Gamma_v$, $\tilde{\Gamma}_w = \Gamma_w$, $\tilde{k}_v = k_v$ и $\tilde{l}_w = l_w$.) Имеем $[L_w : K_v] = e(w|v)f(w|v)$. Таким образом, если $w_1, \ldots, w_r$ — все продолжения v на L, то

$$\sum_{i=1}^{r} e(w_i|v)f(w_i|v) = \sum_{i=1}^{r} [L_{w_i} : K_v] = n.$$

Вообще говоря, числа $e(w_i|v)$ и $f(w_i|v)$ для разных i могут различаться, однако имеется важный случай, когда они совпадают. А именно, так обстоит дело, когда L/K — расширение Галуа. Обозначим его группу Галуа через $\mathcal{G}$. Тогда все продолжения $w_1, \ldots, w_r$ нормирования $v \in V_f^K$ на L сопряжены относительно $\mathcal{G}$, т. е. для любого $i = 1, \ldots, r$ найдется такой $\sigma_i \in \mathcal{G}$, что $w_i(x) = w_1(\sigma_i(x))$ при всех $x \in L$. Отсюда следует, что числа $e(w_i|v)$ и $f(w_i|v)$ не зависят от i (мы их обозначим через e и f), причем число r различных продолжений совпадает с индексом $[\mathcal{G} : \mathcal{G}(w_1)]$ так называемой *группы разложения* $\mathcal{G}(w_1) = \{\sigma \in \mathcal{G} \mid w_1(\sigma x) = w_1(x)$ для всех $x \in L\}$. При этом $efr = n$, а группа $\mathcal{G}(w_1)$ совпадает с группой Галуа соответствующего расширения пополнений L_{w_1}/K_v.

3. Неразветвленные и вполне разветвленные расширения. Пусть $v \in V_f^K$ и соответствующее поле вычетов k_v является конечным полем F_q из q элементов.

Предложение 1. *Для любого целого $n \geqslant 1$ существует единственное неразветвленное расширение L/K_v степени n. Оно порождается над K_v всеми корнями степени $(q^n - 1)$ из единицы и поэтому является расширением Галуа. Сопоставление автоморфизму $\sigma \in \mathrm{Gal}(L/K_v)$ его редукции $\bar{\sigma} \in \mathrm{Gal}(l/k_v)$, где $l \simeq F_{q^n}$ — поле вычетов для L, индуцирует изоморфизм групп Галуа $\mathrm{Gal}(L/K_v) \simeq \mathrm{Gal}(l/k_v)$.*

Для определения *редукции* $\bar{\sigma}$ автоморфизма $\sigma \in \mathrm{Gal}(L/K_v)$ следует заметить, что кольцо нормирования $\mathcal{O}_L$ и идеал нормирования $\mathfrak{P}_L$ инвариантны относительно σ, и тогда σ индуцирует автоморфизм поля вычетов $l = \mathcal{O}_L/\mathfrak{P}_L$, который и есть $\bar{\sigma}$. Отметим также, что группа $\mathrm{Gal}(l/k_v)$ циклическая и порождается так называемым *автоморфизмом Фробениуса*, который

определяется условием $\varphi(x) = x^q$ для всех $x \in k_v$; отвечающий ему элемент группы $\mathrm{Gal}(L/K_v)$ также называется автоморфизмом Фробениуса (расширения L/K_v) и обозначается $\mathrm{Fr}(L/K_v)$.

Норменные свойства неразветвленных расширений описывает

Предложение 2. *Пусть L/K_v — неразветвленное расширение. Тогда $U_v = N_{L/K}(U_L)$, в частности $U_v \subset N_{L/K_v}(L^*)$.*

Доказательство основано на изучении канонической фильтрации в группах единиц, которая оказывается полезной и в других случаях. А именно, для любого целого $i \geqslant 1$ положим $U_v^{(i)} = 1 + \mathfrak{p}_v^i$, $U_L^{(i)} = 1 + \mathfrak{P}_L^i$. Легко видеть, что эти множества являются открытыми подгруппами и в действительности образуют базу окрестностей единицы в группах U_v и U_L соответственно. Имеют место следующие изоморфизмы:

$$U_v/U_v^{(1)} \simeq k_v^*, \quad U_v^{(i)}/U_v^{(i+1)} \simeq k_v^+, \quad i \geqslant 1 \tag{4}$$

(первый изоморфизм индуцируется редукцией по модулю $\mathfrak{p}_v$: $a \mapsto a \pmod{\mathfrak{p}_v}$, а для построения второго следует зафиксировать униформизующий элемент $\pi \in K_v$, и тогда $1 + \pi^i a \mapsto \mapsto a \pmod{\mathfrak{p}_v}$).

Аналогично,

$$U_L/U_L^{(1)} \simeq l^*, \quad U_L^{(i)}/U_L^{(i+1)} \simeq l^+, \quad i \geqslant 1. \tag{5}$$

В силу неразветвленности L/K_v элемент π является также униформизующим элементом в L, и мы в дальнейшем будем считать, что второй изоморфизм в (5) определен при помощи π. Для $a \in U_l$ имеем (черта означает редукцию по модулю $\mathfrak{P}_l$)

$$\overline{\mathrm{N}_{L/K_v}(a)} = \overline{\prod_{\sigma \in \mathrm{Gal}(L/K_v)} \sigma(a)} = \prod_{\tau \in \mathrm{Gal}(l/k_v)} \tau(\bar{a}) = \mathrm{N}_{l/k_v}(\bar{a}).$$

Таким образом, норменное отображение индуцирует гомоморфизм $U_L/U_L^{(1)} \to U_v/U_v^{(1)}$, который при отождествлениях (4) и (5) совпадает с N_{l/k_v}. Далее, для любого целого $i \geqslant 1$ и любого $a \in \mathcal{O}_L$ имеем

$$\mathrm{N}_{L/K_v}(1 + \pi^i a) = \prod_{\sigma \in \mathrm{Gal}(L/K_v)} \sigma(1 + \pi^i a) \equiv$$
$$\equiv 1 + \pi^i \mathrm{Tr}_{L/K_v}(a) \pmod{\mathfrak{P}_v^{(i+1)}}.$$

Отсюда следует, что N_{L/K_v} индуцирует гомоморфизмы $U_L^{(i)}/U_L^{(i+1)} \to U_v^{(i)}/U_v^{(i+1)}$, которые в смысле отождествлений (4) и (5) совпадают со следом Tr_{l/k_v}. Но в расширении конечных полей норма и след сюръективны, поэтому группа $W = \mathrm{N}_{L/K_v}(U_L)$ обладает свойством $U_v = WU_v^{(i)}$ для всех $i \geqslant 1$.

Так как $U_v^{(i)}$ образуют базу окрестностей единицы, то последнее условие означает плотность W в U_v. С другой стороны, из компактности U_L и непрерывности нормы вытекает замкнутость W, и поэтому $W = U_v$. Предложение 2 доказано.

Из доказательства предложения 2 вытекает

Следствие. *Если расширение L/K_v неразветвлено, то для любого целого $i \geqslant 1$ имеем* $\mathrm{N}_{L/K_v}(U_L^{(i)}) = U_v^{(i)}$.

Нам понадобится еще одно утверждение о связи норменного отображения с фильтрацией группы единиц в произвольных расширениях.

Предложение 3. *Для любого конечного расширения L/K_v имеют место следующие утверждения:*

1) $U_v^{(1)} \cap \mathrm{N}_{L/K_v}(L^*) = \mathrm{N}_{L/K_v}(U_L^{(1)})$;

2) *если индекс ветвления L/K_v равен e, то для любого целого $i \geqslant 1$ имеем* $\mathrm{N}_{L/K_v}(U_L^{(i)}) \subset U_v^{(j)}$, *где j — минимальное из целых чисел, не меньших i/e.*

Доказательство. Докажем вначале второе утверждение.

Пусть M — конечное расширение Галуа поля K_v, содержащее L. Тогда для $a \in L$ имеем $\mathrm{N}_{L/K}(a) = \prod_\sigma \sigma(a)$, где произведение берется по всем вложениям σ: $L \hookrightarrow M$ над K_v. Из однозначности продолжения нормирования в локальном случае вытекает, что для любого $a \in L$ и любого σ значения нормирования на a и $\sigma(a)$ совпадают; в частности, для униформизующего элемента $\pi_L \in L$ имеем $\sigma(\pi_L) = \pi_L b_\sigma$ для подходящего $b_\sigma \in U_M$. Отсюда следует, что для $a = 1 + \pi_L^i c \in U_L^{(i)}$ имеем

$$\mathrm{N}_{L/K_v}(a) = \prod_\sigma \sigma(1 + \pi_L^i c) = \prod_\sigma (1 + \pi_L^i b_\sigma \sigma(c)) \in (1 + \pi_L^i \mathcal{O}_M) \cap K_v.$$

Но из определения индекса ветвления имеем $\mathfrak{p}_v \mathcal{O}_L = \mathfrak{P}_L^e$ так, что $\pi_L^i \mathcal{O}_M \cap K_v = \pi_L^i \mathcal{O}_L \cap K_v = \mathfrak{P}_L^i \cap \mathcal{O}_v \subset \mathfrak{p}_v^j$ (где j выбирается, как указано в формулировке предложения) и $\mathrm{N}_{L/K_v}(a) \in U_v^j$. Из доказанного вытекает, что $\mathrm{N}_{L/K_v}(U_L^{(1)}) \subset U_v^{(1)}$, поэтому для доказательства 1) остается установить, что $U_v^{(1)} \cap \mathrm{N}_{L/K_v}(L^*) \subset \subset \mathrm{N}_{L/K_v}(U_L^{(1)})$.

Пусть $a \in L^*$ и $\mathrm{N}_{L/K_v}(a) \in U_v^{(1)}$. Тогда из формулы (1) вытекает, что $a \in U_L$. Изоморфизм (5) показывает, что $U_L^{(1)}$ является максимальной про-p-подгруппой в U_L относительно простого p, отвечающего нормированию v, откуда следует, что $U_L \simeq \simeq U_L/U_L^{(1)} \times U_L^{(1)}$. В частности, $a = bc$, где $c \in U_L^{(1)}$, b — элемент

конечного порядка, взаимно простого с p. Имеем $d = \mathrm{N}_{L/K_v}(b) = \mathrm{N}_{L/K_v}(a)\mathrm{N}_{L/K_v}(c)^{-1} \in U_v^{(1)}$. Порядок любого элемента конечного порядка из $U_v^{(1)}$ является степенью p; с другой стороны, порядок d является делителем порядка b и поэтому взаимно прост с p. Таким образом, $d = 1$ и $\mathrm{N}_{L/K_v}(a) = \mathrm{N}_{L/K_v}(c) \in \mathrm{N}_{L/K_v}(U_L^{(1)})$. Предложение 3 доказано.

Вернемся к рассмотрению неразветвленных расширений поля K_v. Можно показать, что композит неразветвленных расширений является неразветвленным, и поэтому существует *максимальное неразветвленное расширение* K_v^{nr} поля K_v, которое является расширением Галуа, и группа Галуа $\mathrm{Gal}(K_v^{\mathrm{nr}}/K_v)$ изоморфна группе Галуа $\mathrm{Gal}(\bar{k}_v/k_v)$ алгебраического замыкания поля вычетов k_v, т. е. изоморфна $\hat{\mathbb{Z}}$-проконечному пополнению бесконечной циклической группы, образующей которой является автоморфизм Фробениуса.

Пусть теперь L/K — некоторое конечное расширение числового поля K. Известно тогда, что почти все нормирования $v \in V_f^K$ неразветвлены в K, т. е. соответствующее расширение пополнений L_w/K_v является неразветвленным для любого продолжения $w|v$, в частности, определен автоморфизм Фробениуса $\mathrm{Fr}(L_w/K_v)$. Если L/K — расширение Галуа, то, как мы отмечали, группа Галуа $\mathrm{Gal}(L_w/K_v)$ может быть отождествлена с группой разложения $\mathcal{G}(w)$ нормирования в группе Галуа $\mathcal{G} = \mathrm{Gal}(L/K)$, так что $\mathrm{Fr}(L_w/K_v)$ можно рассматривать как элемент группы $\mathcal{G}$.

Мы знаем, что любые два продолжения $w_1, w_2|v$ сопряжены относительно группы $\mathcal{G}$, откуда следует, что автоморфизмы Фробениуса $\mathrm{Fr}(L_w/K_v)$, отвечающие *всем* продолжениям некоторого нормирования v, образуют класс сопряженности $F(v)$ в группе $\mathcal{G}$. Возникает вопрос, все ли классы сопряженности в $\mathcal{G}$ получаются таким образом. Другими словами, для любого ли $\sigma \in \mathcal{G}$ найдется такое нормирование $v \in V_f^K$, что для подходящего $w|v$ расширение L_w/K_v неразветвлено и $\mathrm{Fr}(L_w/K_v) = \sigma$.

Теорема 2 (Чеботарев). *Пусть L/K — конечное расширение Галуа с группой Галуа $\mathcal{G}$. Тогда для любого $\sigma \in \mathcal{G}$ найдется бесконечно много таких $v \in V_f^K$, что для подходящего $w|v$ расширение L_w/K_v неразветвлено и $\mathrm{Fr}(L_w/K_v) = \sigma$. В частности, существует бесконечно много таких v, что $L_w = K_v$, т. е. $L \subset K_v$.*

В действительности Чеботаревым была определена количественная мера (плотность) множества таких $v \in V_f^K$, что класс сопряженности $F(v)$ совпадает с фиксированным классом со-

пряженности $C \subset \mathcal{G}$. Она равна $[C]/[\mathcal{G}]$ (при этом плотность всего множества V_f^K принимается за единицу). Поэтому теорему 2 (точнее, соответствующее утверждение о плотности) называют *теоремой плотности Чеботарева*. Для случая круговых расширений поля $K = \mathbb{Q}$ она эквивалентна теореме Дирихле о простых числах в арифметической прогрессии.

Методами геометрической теории чисел доказывается

Теорема 3 (Эрмит). *Если $K/\mathbb{Q}$ — конечное расширение, неразветвленное относительно всех простых p (т. е. $K_v/\mathbb{Q}_p$ неразветвлено для всех p и всех $v|p$), то $K = \mathbb{Q}$.*

Мы не будем здесь подробно анализировать строение вполне разветвленных расширений (в частности, выделять слабо и сильно разветвленные расширения), а ограничимся их описанием с помощью многочленов Эйзенштейна. Напомним, что многочленом Эйзенштейна называется многочлен $e(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0 \in K_v[t]$ такой, что $a_i \in \mathfrak{p}_v$ для всех $i = 0, 1, \ldots, n-1$ и $a_0 \notin \mathfrak{p}_v^2$. Хорошо известно, что многочлен Эйзенштейна неприводим в $K_v[t]$.

Предложение 4. *Если Π — корень многочлена Эйзенштейна $e(t)$, то $L = K_v[\Pi]$ — вполне разветвленное расширение K_v с униформизующим элементом Π. Обратно, если L/K_v вполне разветвлено и Π — униформизующий элемент в L, то $L = K_v[\Pi]$ и минимальный полином Π над K_v является многочленом Эйзенштейна.*

Следствие. *Если L/K_v вполне разветвлено, то норменная группа $\mathrm{N}_{L/K_v}(L^*)$ содержит униформизующий элемент поля K_v.*

При исследовании ветвления в расширении Галуа L/K с группой Галуа $\mathcal{G}$ используются так называемые *группы ветвления* $\mathcal{G}^i (i \geqslant 0)$, являющиеся подгруппами в $\mathcal{G}$. Если $w|v$, то по определению $\mathcal{G}^0$ — это группа разложения $\mathcal{G}(w)$ нормирования w, которую можно отождествлять с локальной группой Галуа $\mathrm{Gal}(L_w/K_v)$. Далее, $\mathcal{G}^{(1)} = \{\sigma \in \mathcal{G}^{(0)} \mid \sigma(a) \equiv a \pmod{\mathfrak{P}_{L_w}}\ \forall a \in \mathcal{O}_{L_w}\}$ — так называемая группа инерции. Она является ядром гомоморфизма $\mathrm{Gal}(L_w/K_v) \to \mathrm{Gal}(l_w/k_v)$, сопоставляющего каждому автоморфизму его редукцию. Поэтому $\mathcal{G}^{(1)}$ является нормальным делителем в $\mathcal{G}^{(0)}$ и, в силу сюръективности указанного гомоморфизма, $\mathcal{G}^{(0)}/\mathcal{G}^{(1)} \simeq \mathrm{Gal}(l_w/k_v)$. При этом неподвижное поле $E = L_w^{\mathcal{G}^{(1)}}$ является максимальным неразветвленным расширением поля K_v, содержащимся в L_w, и расширение L_w/E вполне разветвлено. Высшие группы ветвления определяются следующим образом: $\mathcal{G}^{(i)} = \{\sigma \in \mathcal{G}^{(0)} \mid \sigma(a) \equiv a \pmod{\mathfrak{P}_{L_w}^i}\}$. Они являются нормальными делителями в $\mathcal{G}^{(0)}$, и $\mathcal{G}^{(i)} = \{e\}$ для достаточно больших i. При этом последовательные факторы $\mathcal{G}^{(i)}/\mathcal{G}^{(i+1)}$ $(i \geqslant 1)$ являются p-группами относи-

тельно простого p, отвечающего v. Отметим, что определенные таким образом группы $\mathscr{G}^{(i)} = \mathscr{G}^{(i)}(v)$ зависят от продолжения $w|v$, и при другом выборе w меняются на сопряженные. В частности, неподвижное поле $L^{\mathscr{H}}$ подгруппы $\mathscr{H} \subset \mathscr{G}$, порожденной группами инерции $\mathscr{G}^{(1)}(w)$ для всех продолжений $w|v$, является максимальным нормальным подрасширением в L, которое не разветвлено относительно всех продолжений нормирования v.

§ 1.2. Адели и идели. Сильная и слабая аппроксимации. Локально-глобальный принцип

Поведение поля K относительно какого-либо индивидуального нормирования $v \in V_f^K$ не оказывает существенного влияния на его арифметику, однако, изучая свойства K по совокупности нормирований (например, относительно всего множества V^K), мы получаем весьма существенную арифметическую информацию. В настоящем параграфе вводятся конструкции, которые позволяют изучать все пополнения поля K одновременно.

1. Адели и идели. Множеством *аделей* A_K поля алгебраических чисел K называется подмножество прямого произведения $\prod_{v \in V^K} K_v$, состоящее из таких $x = (x_v)$, что $x_v \in \mathcal{O}_v$ для почти всех $v \in V_f^K$. Множество A_K является кольцом относительно операций, индуцированных с прямого произведения. На множестве A_K можно ввести топологию, базу открытых множеств которой составляют множества вида $\prod_{v \in S} W_v \times \prod_{v \in V^K \setminus S} \mathcal{O}_v$, где $S \subset V^K$ — конечное подмножество, содержащее V_∞^K, и $W_v \subset K_v$ — открытые подмножества для $v \in S$. (Эта топология, называемая *адельной*, сильнее топологии, индуцированной с прямого произведения $\prod_{v \in V^K} K_v$). Относительно адельной топологии A_K является локально компактным топологическим кольцом. Для любого конечного подмножества $S \subset V^K$, содержащего V_∞^K, определяется *кольцо S-целых аделей* $A_K(S) = \prod_{v \in S} K_v \times \prod_{v \notin S} \mathcal{O}_v$; если $S = V_\infty^K$, то соответствующее кольцо называется *кольцом целых аделей* и обозначается $A_K(\infty)$. Ясно, что $A_K = \bigcup_S A_K(S)$, где объединение берется по всем конечным подмножествам $S \subset V^K$, содержащим V_∞^K. Несложно показать, что для любого $a \in K$ и почти всех $v \in V_f^K$ справедливо неравенство $|a|_v \leqslant 1$, т. е. $a \in \mathcal{O}_v$. Если $a \in K^*$, то, применяя указанное неравенство к элементу a^{-1}, получим, что в действительности $a \in U_v$ для почти всех $v \in V_f^K$. Ниже будет использоваться

обозначение: $V(a)=\{v\in V_f^K \mid a\notin U_v\}$. Из этих фактов вытекает, что имеется диагональное вложение $K\to A_K$, $x\mapsto(x, x, \ldots)$, образ которого называется *кольцом главных аделей* и обычно будет отождествляться с K.

Предложение 5. *Кольцо главных аделей дискретно в A_K.*

Для доказательства следует заметить, что поскольку $\mathcal{O}=\bigcap_{v\in V_f^K}(K\cap\mathcal{O}_v)$, пересечение $K\cap A_K(\infty)$ совпадает с кольцом целых элементов $\mathcal{O}\subset K$, и достаточно установить дискретность $\mathcal{O}$ в $\prod_{v\in V_\infty^K}K_v=K\otimes_{\mathbb{Q}}\mathbb{R}$. Пусть $x_1, \ldots, x_n$ — некоторый $\mathbb{Z}$-базис $\mathcal{O}$, который одновременно является $\mathbb{Q}$-базисом K, а следовательно, и $\mathbb{R}$-базисом $K\otimes_{\mathbb{Q}}\mathbb{R}$. С его помощью $\mathcal{O}$ отождествляется с решеткой $\mathbb{Z}^n$ в пространстве $K\otimes_{\mathbb{Q}}\mathbb{R}$, и требуемая дискретность вытекает из дискретности $\mathbb{Z}$ в $\mathbb{R}$. (Попутно отметим, что пересечение $K\cap A_K(S)$ (где $S\supset V_\infty^K$) совпадает с *кольцом S-целых элементов* $\mathcal{O}(S)=\{x\in K \mid |x|_v\leqslant 1$ для всех $v\in V^K\setminus S\}$, причем $\mathcal{O}(V_\infty^K)$ совпадает с обычным кольцом целых $\mathcal{O}$.)

Мультипликативным аналогом аделей являются *идели* поля K, множество J_K которых по определению состоит из таких $x=(x_v)\in\prod_{v\in V^K}K_v^*$, что $x_v\in U_v$ для почти всех $v\in V_f^K$. Ясно, что J_K является подгруппой прямого произведения $\prod_v K_v^*$; более того, J_K в действительности совпадает с группой обратимых элементов кольца A_K. Любопытно, однако, отметить, что J_K не является топологической группой относительно топологии, индуцированной с A_K (взятие обратного элемента не является в этой топологии непрерывной операцией). «Правильная» топология на J_K индуцируется топологией на произведении $A_K\times A_K$ при вложении $J_K\to A_K\times A_K$, $x\mapsto(x, x^{-1})$. В явном виде эта топология может быть задана при помощи базы открытых множеств, состоящей из множеств вида $\prod_{v\in S}W_v\times\prod_{v\in V^K\setminus S}U_v$, где $S\subset V^K$ — конечное подмножество, содержащее V_∞^K, и $W_v\subset K_v^*$ — открытые подмножества для $v\in S$. Эта топология называется *идельной*; она сильнее индуцированной адельной топологии, и относительно нее J_K является локально компактной топологической группой. (Нельзя не заметить прямых аналогий в определении аделей и иделей. В действительности оба эти понятия являются частными случаями понятия аделей алгебраической группы, или еще более общей конструкции ограниченного

топологического произведения, которые мы рассмотрим в § 3.5.) Аналогии между аделями и иделями можно проводить и дальше. Так, для любого конечного подмножества $S \subset V^K$, содержащего V_∞^K, определяется *группа S-целых иделей* $J_K(S) = \prod_{v \in S} K_v^* \times \prod_{v \notin S} U_v$, которая при $S = V_\infty^K$ называется *группой целых иделей* и обозначается $J_K(\infty)$. Как мы уже отмечали, если $a \in K^*$, то $a \in U_v$ для почти всех v, и, следовательно, имеем диагональное вложение $K^* \to J_K$, образ которого называется *группой главных иделей*.

Предложение 6. *Группа главных иделей дискретна в J_K.*

Доказательство вытекает из предложения 5 и того факта, что индуцированная адельная топология на J_K слабее идельной. Другое доказательство можно получить с помощью так называемой формулы произведения, которая утверждает, что для любого $a \in K^*$ имеем $\prod_{v \in V^K} |a|_v^{n_v} = 1$, если V^K состоит из продолжений нормирований $|\ |_p$ и $|\ |_\infty$ поля $\mathbb{Q}$, $n_v = [K_v : \mathbb{Q}_p]$ (соответственно $n_v = [K_v : \mathbb{R}]$) — локальная степень относительно p-адического (соответственно архимедова) нормирования v. Формуле произведения можно придать более изящный вид $\prod_{v \in V^K} \|a\|_v = 1$, введя так называемые *нормализованные нормирования* $\|a\|_v = |a|_v^{n_v}$. Эти функции определяют ту же топологию на K, что и исходные нормирования $|\ |_v$, и в действительности сами являются нормированиями, им эквивалентными, за исключением случая, когда нормирование v комплексное. Для неархимедовых v нормализованное нормирование допускает следующее внутреннее описание: если $\pi \in K_v$ — униформизующий элемент, то $\|\pi\|_v = q^{-1}$, где q — число элементов поля вычетов k_v. Вернемся к предложению 6. Для архимедовых v положим $W_v = \left\{x \in K_v^* \,\middle|\, \|x - 1\|_v < \frac{1}{2}\right\}$ и покажем, что окрестность единицы $\Omega = \prod_{v \in V_\infty^K} W_v \times \prod_{v \in V_f^K} U_v$ обладает свойством $\Omega \cap K^* = \{1\}$. Если $a \in \Omega \cap K^*$ и $a \neq 1$, то для элемента $a - 1$ будем иметь $\prod_{v \in V^K} \|a - 1\|_v < \prod_{v \in V_\infty^K} \frac{1}{2} \cdot \prod_{v \in V_f^K} 1 < 1$, что противоречит формуле произведения.

С помощью нормализованных нормирований определяется непрерывный гомоморфизм $J_K \to \mathbb{R}^{>0}$, $(x_v) \mapsto \prod_N \|x_v\|_v$, ядро J_K^1 которого называется *группой специальных иделей* (отметим, что в силу формулы произведения $J_K^1 \supset K^*$). Поскольку K дискретно в A_K, а K^* — в J_K, то естественно возникает задача по-

строения теории приведения, т. е. указания конструкции фундаментальных областей для K в A_K и для K^* в J_K. Мы не будем подробно заниматься здесь этими вопросами (см., например, Ленг [2], АТЧ), ибо позднее рассмотрим их в полной общности, применительно к произвольным алгебраическим группам. Отметим только, что факторпространство A_K/K компактно, а факторпространство J_K/K^* некомпактно, но компактно факторпространство J_K^1/K^*.

Остановимся еще на важном для нас в методологическом плане изоморфизме факторгруппы $J_K/J_K(\infty)K^*$ с группой $\mathrm{Cl}(K)$ классов идеалов поля K. Описать его можно следующим образом. Вначале устанавливается биекция между множеством V_f^K неархимедовых нормирований K и множеством $\mathscr{P}$ ненулевых простых (= максимальных) идеалов кольца $\mathcal{O}$, которая нормированию v ставит в соответствие идеал $\mathfrak{p}(v)=\mathcal{O}\cap\mathfrak{p}_v$. Тогда иделю $x=(x_v)$ отвечает идеал $i(x)=\prod_{v\in V_f^K}\mathfrak{p}(v)^{v(x_v)}$. (Здесь следует отметить, что поскольку $x\in J_K$, то $v(x_v)=0$ для почти всех $v\in V_f^K$ и указанное произведение корректно определено.) При этом степень $\mathfrak{p}^\alpha$ при $\alpha<0$ определяется в смысле группы $\mathrm{Id}(K)$ дробных идеалов поля K (см. § I.1, п. 1). Используя теорему о том, что любой дробный идеал в K (равно как и любой ненулевой идеал в $\mathcal{O}$) однозначно разлагается в произведение степеней простых идеалов, легко видеть, что отображение i: $x\longmapsto i(x)$ является сюръективным гомоморфизмом J_K на $\mathrm{Id}(K)$, ядром которого служит группа $J_K(\infty)$ целых иделей. Учитывая, что образ $i(K^*)$ совпадает с группой главных дробных идеалов, получаем, что i индуцирует требуемый изоморфизм $J_K/J_K(\infty)K^*\simeq\mathrm{Cl}(K)$. В частности, индекс $[J_K:J_K(\infty)K^*]$ совпадает с числом h_K классов идеалов поля K. Это наблюдение лежит в основе определения чисел классов алгебраических групп (см. гл. VIII).

2. Сильная и слабая аппроксимация. Нам понадобятся «усеченные» кольца аделей $A_{K,S}$, где S — некоторое конечное подмножество в V^K, которые определяются как образ A_K при естественной проекции на прямое произведение $\prod_{v\notin S}K_v$. Для любого конечного подмножества $T\subset V^K$, содержащего S, образ кольца T-целых аделей $A_K(T)$ в $A_{K,S}$ будет обозначаться через $A_{K,S}(T)$. В целях упрощения обозначений мы будем писать A_S, $A_S(T)$ вместо $A_{K,S}$, $A_{K,S}(T)$, если из контекста ясно, о каком поле идет речь. В частности, для $S=V_\infty^K$ кольцо A_{K,V_∞^K} будет обозначаться через A_f и называться *кольцом конечных аделей*. Топология на A_S вводится очевидным образом: в качестве базы системы открытых множеств берутся множества вида $\prod_{v\in T}W_v\times$

$\times \prod_{v \notin S \cup T} \mathcal{O}_v$, где $T \subset V^K \setminus S$ — некоторое подмножество, и для каждого $v \in T$ $W_v \subset K_v$ — некоторое открытое подмножество. Имеем $A = K_S \times A_S$, где $K_S = \prod_{v \in S} K_v$. Кольцо K наделяется топологией прямого произведения, и тогда A является произведением топологических колец K_S и A_S. При этом диагональное вложение поля K в A является произведением диагональных вложений в K_S и A_S соответственно.

Замечательный факт состоит в том, что хотя образ диагонального вложения K в A дискретен, каждое из вложений $K \to K_S$, $K \to A_S$ является плотным.

Теорема 4 (о слабой аппроксимации). *Образ K при диагональном вложении плотен в K_S.*

Теорема 5 (о сильной аппроксимации). *Если $S \neq \varnothing$, то образ K при диагональном вложении плотен в A_S.*

Теорема 4 справедлива для любого поля K и любого конечного множества S его неэквивалентных нормирований. Напротив, теорема 5 (и все понятия, связанные с аделями) имеют смысл лишь для числовых (или, более общо, глобальных полей). Чтобы прояснить арифметический смысл теоремы 5, разберем подробно случай $K = \mathbb{Q}$, $S = \{\infty\}$. Так как для любого аделя $x \in A_f = A_{\mathbb{Q}, S}$ можно подобрать такое целое число m, что $mx \in A_f(\infty)$, то в действительности достаточно доказать, что $\mathbb{Z}$ плотно вкладывается в произведение $A_f(\infty) = \prod_p \mathbb{Z}_p$. Любое открытое подмножество в $A_f(\infty)$ содержит множество вида

$$W = \prod_{i=1}^{r} \left(a_i + p_i^{\alpha_i} \mathbb{Z}_{p_i}\right) \times \prod_{p \neq p_i} \mathbb{Z}_p,$$

где $\{p_1, \ldots, p_r\}$ — некоторый конечный набор простых чисел, α_i — целые > 0 и $a_i \in \mathbb{Z}$. Поэтому вопрос о непустоте пересечения $\mathbb{Z} \cap W$ эквивалентен вопросу о разрешимости системы сравнений $x \equiv a_i \pmod{p_i^{\alpha_i}}$, $i = 1, 2, \ldots r$, который положительно решается классической китайской теоремой об остатках. Таким образом, в данной ситуации теорема о сильной аппроксимации эквивалентна китайской теореме об остатках. Отметим, что в гл. VII мы исследуем сильную и слабую аппроксимацию для алгебраических групп.

3. Локально-глобальный принцип. Исследование арифметических вопросов над локальными полями значительно проще исходных задач над числовыми полями. Поэтому естественно возникает вопрос, лежащий в основе так называемого локально-глобального метода: когда из выполнимости какого-либо свойства над всеми пополнениями K_v некоторого числового поля K

вытекает его выполнимость над полем K? Одним из первых результатов такого типа явилась классическая

Теорема 6 (Минковский — Хассе). Пусть $f = f(x_1, \ldots, x_n)$ — невырожденная квадратичная форма над полем алгебраических чисел K. Тогда если f представляет нуль *) над всеми пополнениями K_v, то f представляет нуль и над K.

Сейчас утверждения о возможности перехода «от локального к глобальному» принято называть утверждениями о справедливости в данной ситуации *локально-глобального принципа*, или *принципа Хассе*. Локально-глобальный принцип пронизывает всю арифметическую теорию алгебраических групп, и с его различными аспектами мы будем постоянно иметь дело в этой книге.

Не следует, однако, думать, что локально-глобальный принцип для представимости чисел формами выполняется всегда, и мы хотим закончить данный параграф указанием на классический пример.

Предварительно укажем на некоторые аспекты связи между кольцом аделей A_K поля K и кольцом аделей A_L его конечного расширения L. Оказывается, что существует естественный изоморфизм в алгебраическом и топологическом смыслах $A_K \otimes L \simeq A_L$. Этот изоморфизм получается из локальных изоморфизмов $K_v \otimes_K L \simeq \prod_{w \mid v} L_w$ (см. (2) § 1.1), и надо только заметить, что для почти всех $v \in V_f^K$ эти изоморфизмы осуществляют изоморфизм $\mathcal{O}_v \otimes \mathcal{O}_L \simeq \prod_{w \mid v} \mathcal{O}_{L_w}$. Далее, формулы (3) § 1.1 показывают, что отображения нормы и следа $\mathrm{N}_{L/K}$ и $\mathrm{Tr}_{L/K}$ продолжаются до отображений $\mathrm{N}_{L/K}\colon A_L \to A_K$ и $\mathrm{Tr}_{L/K}\colon A_L \to A_K$ по формулам

$$\mathrm{N}_{L/K}((x_w)) = \Big(\Big(\prod_{w \mid v} \mathrm{N}_{L_w/K_v}(x_w)\Big)_v\Big),$$

$$\mathrm{Tr}_{L/K}((x_w)) = \Big(\Big(\sum_{w \mid v} \mathrm{Tr}_{L_w/K_v}(x_w)\Big)_v\Big).$$

Легко проверить, что таким образом определенное норменное отображение $\mathrm{N}_{L/K}$ индуцирует непрерывный гомоморфизм групп иделей $\mathrm{N}_{L/K}\colon J_L \to J_K$. Говорят, что для расширения L/K выполняется норменный принцип Хассе, если $\mathrm{N}_{L/K}(J_L) \cap K^* = \mathrm{N}_{L/K}(L^*)$. Так как любой элемент $a \in K^*$ принадлежит U_v для почти всех $v \in V_f^K$ и для почти всех $v \in V_f^K$ расширение L_w/K_v неразветвлено, то в силу предложения 2 условие $a \in \mathrm{N}_{L/K}(J_L)$ в действительности эквивалентно тому, что $a \in \mathrm{N}_{L/K}\Big(\prod_{w \mid v} L_w^*\Big) = \mathrm{N}_{L/K}((L \otimes_K K_v)^*)$ для всех $v \in V_f^K$. На языке алгебраической геометрии последнее означает, что уравнение

*) То есть уравнение $f(x_1, \ldots, x_n) = 0$ имеет ненулевое решение.

$f(x_1, \ldots, x_n) = a$, где f — однородный многочлен степени n от координат $x_1, \ldots, x_n$ элемента $x \in L$ в некотором базисе расширения L/K, задающий норму, имеет решение над всеми полями K_v, $v \in V^K$, а справедливость принципа Хассе в данной ситуации сводится к существованию решения над K. (Было бы неправильно формулировать норменный принцип в виде $a \in \mathrm{N}_{L/K}(L^*) \Leftrightarrow a \in \mathrm{N}_{L_w/K_v}(L_w^*)$ для всех v и всех $w|v$, ибо если L/K не является расширением Галуа, то, вообще говоря, $\mathrm{N}_{L/K}(L^*) \not\subset \mathrm{N}_{L_w/K_v}(L_w^*)$.)

Классическая теорема Хассе о нормах (см. Хассе [1], а также следствия из теоремы 6.11) утверждает справедливость норменного принципа для циклических расширений Галуа. Однако уже для $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{13}, \sqrt{17})$, т. е. когда L/K является абелевым расширением Галуа с группой Галуа типа (2,2), норменный принцип не выполняется. Более точно, при помощи простых вычислений с символами Гильберта (см. [АТЧ], упр. 5.3) можно показать, что число 5^2 всюду является локальной нормой, но глобальной нормой не является. (К норменному принципу Хассе мы вернемся в гл. VI, см. § 6.3.)

§ 1.3. Когомологии

1. Основные понятия. В целом когомологический формализм используется в книге в сравнительно небольшом объеме. Исключение составляют лишь когомологии Галуа алгебраических групп над локальными и глобальными полями, которым посвящена специальная гл. VI. Эти вопросы, как правило, не затрагиваются в обычных курсах гомологической алгебры, ибо в основе их лежат так называемые некоммутативные когомологии, определения и основные свойства которых мы обсудим ниже. А пока укажем на необходимые нам свойства обычных (коммутативных) когомологий, доказательство которых можно найти в книгах Картан, Эйленберг [1], Серр [2], Браун [1], и также в гл. IV книги [АТЧ].

Итак, пусть A — абелева группа, на которой автоморфизмами действует некоторая группа G (так называемая G-группа)*). Тогда определено семейство $\{H^i(G, A)\}_{i \geqslant 0}$ абелевых групп, называемых *группами когомологий* G с коэффициентами в A. А именно, полагают $H^0(G, A) = A^G$ — подгруппа неподвижных относительно G элементов, а для определения высших групп рассматривают группы $C^i(G, A)$, состоящие из всех функ-

*) Часто используется также термин G-модуль, ибо задание на A структуры G-группы эквивалентно заданию на A структуры модуля над целочисленным групповым кольцом $\mathbb{Z}[G]$.

ций f: $G^i \to A$, называемых коцепями (при этом $C^0(G, A) = A$), и так называемые *кограничные операторы* d_i: $C^i(G, A) \to C^{i+1}(G, A)$, задаваемые формулой

$$(d_i f)(g_1, \ldots, g_{i+1}) = g_1 f(g_2, \ldots, g_{i+1}) + \\ + \sum_{j=1}^{i} (-1)^j f(g_1, \ldots, g_j g_{j+1}, \ldots, g_{i+1}) + (-1)^{i+1} f(g_1, \ldots, g_i).$$

Тогда $H^i(G, A) = \operatorname{Ker} d_i / \operatorname{Im} d_{i-1}$, причем элементы из $\operatorname{Ker} d_i = Z^i(G, A)$ называются коциклами, а из $\operatorname{Im} d_{i-1} = B^i(G, A)$ — кограницами. Основное свойство групп когомологий состоит в том, что они образуют когомологическое расширение функтора неподвижных точек $F(A) = H^0(G, A)$. А именно, это означает, что если $0 \to A \to B \to C \to 0$ — точная последовательность G-групп и G-гомоморфизмов (т. е. гомоморфизмов, перестановочных с действием G), то существуют такие связывающие гомоморфизмы δ_i: $H^i(G, C) \to H^{i+1}(G, A)$, что точна последовательность

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \xrightarrow{\delta_0} H^1(G, A) \to \ldots \\ \ldots \to H^i(G, A) \to H^i(G, B) \to H^i(G, C) \xrightarrow{\delta_i} H^{i+1}(G, A) \to \ldots \quad (1)$$

(остальные гомоморфизмы естественным образом индуцируются гомоморфизмами из последовательности $0 \to A \to B \to C \to 0$).

Группы когомологий малых размерностей имеют простые интерпретации. Так, $H^1(G, A)$ есть факторгруппа группы так называемых *скрещенных гомоморфизмов* f: $G \to A$, подчиняющихся условию $f(g_1 g_2) = f(g_1) + g_1 f(g_2)$, по подгруппе, состоящей из отображений вида $f(g) = ga - a$ для некоторого $a \in A$. Так, если G действует на A тривиально, то $H^1(G, A) = \operatorname{Hom}(G, A)$. С другой стороны, если $G = \langle \sigma \rangle$ — циклическая группа порядка n, то для любой G-группы A имеем $H^1(G, A) = A_0/A_1$, где A_0 — ядро оператора следа $\operatorname{Tr} a = a + \sigma a + \ldots + \sigma^{n-1} a$, A_1 — подгруппа, состоящая из элементов вида $\sigma a - a$.

Группа $H^2(G, A)$ есть факторгруппа группы так называемых *систем факторов* f: $G \times G \to A$, удовлетворяющих соотношению

$$g_1 f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2) = 0,$$

по подгруппе тривиальных систем факторов, состоящей из функций вида $f(g_1, g_2) = \varphi(g_1 g_2) - \varphi(g_1) - g_1 \varphi(g_2)$ для подходящей функции φ: $G \to A$. Системы факторов встречаются в теории расширений групп при изучении расширений E группы G при помощи A, т. е. точных последовательностей $1 \to A \to E \to G \to 1$. С их помощью устанавливается, что элементы группы $H^2(G, A)$ находятся во взаимно однозначном соответствии с классами изоморфизма таких расширений, индуцирующих заданное

действие G на A. В частности, если G действует на A тривиально, то $H^2(G, A)$ параметризует центральные расширения G при помощи A. В гл. IX мы встретимся с группами $H^2(G, \mathbf{J})$, где $\mathbf{J} = \mathbb{Q}/\mathbb{Z}$, которые совпадают с известными мультипликаторами Шура. В связи с этим укажем на несколько несложных утверждений.

Лемма 1. 1) *Пусть* $1 \to \mathbf{J} \to E \xrightarrow{\rho} G \to 1$ — *некоторое центральное расширение. Тогда для любых двух поэлементно перестановочных подгрупп* A, $B \subset G$ *отображение* φ: $A \times B \to \mathbf{J}$, $\varphi(a, b) = [\tilde{a}, \tilde{b}]$, *где* $\tilde{a} \in \rho^{-1}(a)$, $\tilde{b} \in \rho^{-1}(b)$, $[x, y] = xyx^{-1}y^{-1}$, *является корректно определенным и бимультипликативным.*

2) *Если* G — *конечнопорожденная абелева группа, то расширение* $1 \to \mathbf{J} \to E \to G \to 1$ *тривиально в том и только в том случае, если группа* E *абелева. В частности, если группа* G *циклическая, то* $H^2(G, \mathbf{J}) = 0$.

Утверждение 1) доказывается прямым вычислением. Доказательство 2) использует делимость группы $\mathbf{J}$ и тот факт, что факторгруппа абстрактной группы по центру не может быть нетривиальной циклической группой.

Нам понадобится также вычисление $H^2(S_n, \mathbf{J})$ для симметрической группы S_n.

Лемма 2. 1) *Если* $n \leqslant 3$, *то для любой подгруппы* $H \subset S_n$ *имеем* $H^2(H, \mathbf{J}) = 0$; 2) *если* $n \geqslant 4$, *то* $H^2(S_n, \mathbf{J})$ *имеет порядок 2, и для подгруппы* $C \subset S_n$, *порожденной двумя независимыми транспозициями, отображение ограничения* $H^2(S_n, \mathbf{J}) \to H^2(C, \mathbf{J})$ *(см. ниже) является изоморфизмом.*

Доказательство. Для любой конечной группы G и простого p, делящего порядок G, p-часть группы $H^i(G, A)$ изоморфна $H^i(G_p, A)$ для любого $i \geqslant 1$, где G_p — силовская p-подгруппа в G (см. [АТЧ], гл. IV, § 6). Поэтому утверждение 1) вытекает из пункта 2) леммы 1 и того факта, что при $n \leqslant 3$ группа S_n имеет лишь циклические силовские подгруппы. Тот факт, что $H^2(S_n, \mathbf{J})$ при $n \geqslant 4$ имеет порядок 2, был обнаружен еще Шуром [1] (см. также Хупперт [1]). Ясно также, что $H^2(C, \mathbf{J})$ также имеет порядок 2. Поэтому нам достаточно найти коцикл $\alpha \in H^2(S_n, \mathbf{J})$, ограничение которого на C нетривиально. Построить его можно следующим образом. Рассмотрим абстрактную группу $\tilde{S}_n$ с образующими σ, τ_i $(i = 1, \ldots, n-1)$ и соотношениями

$$\begin{gathered} \sigma^2 = \tau_i^2 = [\tau_i, \sigma] = 1, \quad i = 1, \ldots, n-1, \\ (\tau_i \tau_{i+1})^3 = 1, \quad i = 1, \ldots, n-2, \\ [\tau_i, \tau_j] = \sigma, \quad i + 1 < j. \end{gathered} \tag{2}$$

Поскольку группа S_n порождается транспозициями $(i, i+1)$, $i = 1, \ldots, n-1$, причем определяющее множество соотношений

имеет вид

$$(i,\ i+1)^2=1,\quad i=1,\ \ldots,\ n-1,$$
$$((i,\ i+1)(i+1,\ i+2))^3=1,\quad i=1,\ \ldots,\ n-2, \tag{3}$$
$$[(i,\ i+1),\ (j,\ j+1)]=1,\quad i+1<j$$

(см. Хупперт [1]), то существует единственный гомоморфизм $\tilde{S}_n \xrightarrow{\theta} S_n$ такой, что $\theta(\sigma)=1$, $\theta(\tau_i)=(i, i+1)$. Из (2), (3) вытекает, что $\operatorname{Ker}\theta$ лежит в центре $\tilde{S}_n$ и совпадает с циклической группой второго порядка, порожденной σ. Отождествляя ее с группой, порожденной элементом $\frac{1}{2}+\mathbb{Z}$ в $\mathbb{Q}/\mathbb{Z}$, обозначим через α коцикл в $H^2(S_n, \mathbf{J})$, отвечающий расширению $\tilde{S}_n \xrightarrow{\theta} S_n$. Другими словами, рассмотрим произвольное сечение φ: $S_n \to \tilde{S}_n$ и положим

$$\alpha(g,\ h)=\varphi(g)\,\varphi(h)\,\varphi(gh)^{-1}.$$

Заменяя группу C на сопряженную, можно считать, что C порождается транспозициями (1,2) и (3,4). Если предположить, что ограничение α на C тривиально, то в силу утверждения 2) леммы 1 группа $\theta^{-1}(C)$ должна быть абелевой. Однако $[\varphi((1,2)),\ \varphi((3,4))]=[\tau_1, \tau_2]=\sigma\neq 1$. Лемма доказана.

Из высших групп когомологий нам встретятся лишь группы $H^3(G, \mathbb{Z})$, где G — конечная группа, тривиально действующая на $\mathbb{Z}$, возникающая при изучении препятствий к принципу Хассе (см. § 6.3). Однако, как показывает следующий результат, их вычисление сводится к вычислению $H^2(G, \mathbf{J})$.

Лемма 3. *Пусть G — конечная группа. Тогда существует естественный изоморфизм $H^3(G, \mathbb{Z})\simeq H^2(G, \mathbf{J})$ групп когомологий относительно тривиального действия группы G.*

Действительно, известно (см. [АТЧ], гл. IV, § 6), что группы когомологий $H^i(G, A)$ конечной группы G аннулируются умножением на $[G]$. Так как аддитивная группа $\mathbb{Q}$ однозначно делима, то отсюда вытекает, что $H^i(G, \mathbb{Q})=0$ для всех $i\geqslant 1$. Тогда из точной последовательности $0\to\mathbb{Z}\to\mathbb{Q}\to\mathbf{J}\to 0$ получаем точную последовательность $0=H^2(G, \mathbb{Q})\to H^2(G, \mathbf{J})\to$ $\to H^3(G, \mathbb{Z})\to H^3(G, \mathbb{Q})=0$, из которой и следует требуемое.

Функториальность $H^i(G, A)$ по второму аргументу очевидна: любому G-гомоморфизму абелевых G-групп f: $A\to B$ отвечает гомоморфизм групп когомологий f^*: $H^i(G, A)\to H^i(G, B)$. Обсудим некоторые аспекты функториальности по первому аргументу. Если H — подгруппа в G, то ограничивая коциклы на H, получаем *гомоморфизм ограничения* Res: $H^i(G, A)\to H^i(H, A)$. Если N — нормальный делитель в G, а A — некоторая абелева G-группа, то группа неподвижных точек A^N является (G/N)-группой, и канонический гомоморфизм $G\to G/N$ индуцирует *гомоморфизм инфляции* Inf: $H^i(G/N, A^N)\to H^i(G, A)$. Кроме того, здесь можно определить действие факторгруппы G/N на

$H^i(N, A)$; при этом оказывается, что образ гомоморфизма ограничения Res: $H^i(G, A) \to H^i(N, A)$ лежит в группе неподвижных точек $H^i(N, A)^{G/N}$. Наконец, можно определить гомоморфизм Tra: $H^1(N, A)^{G/N} \to H^2(G, A^N)$, называемый *трансгрессией*, так, что имеет место точная последовательность

$$0 \to H^1(G/N, A^N) \xrightarrow{\text{Inf}} H^1(G, A) \xrightarrow{\text{Res}} H^1(N, A)^{G/N} \to$$
$$\xrightarrow{\text{Tra}} H^2(G/N, A^N) \xrightarrow{\text{Inf}} H^2(G, A), \quad (4)$$

которая представляет собой начальный отрезок *спектральной последовательности Хохшильда — Серра*, отвечающей расширению

$$1 \to N \to G \to G/N \to 1$$

(основные моменты построения последовательности (4), которые мы опускаем, читатель сможет найти в книге Коха [1]).

Существует прием, позволяющий заменить когомологии подгруппы $H \subset G$ когомологиями всей группы G. Для этого с произвольным H-модулем A связывается так называемый индуцированный G-модуль $\text{Ind}_G^H(A)$, который состоит из таких отображений f: $G \to A$, что $f(hg) = hf(g)$ $(h \in H, g \in G)$, причем действие G на $\text{Ind}_G^H(A)$ определяется формулой $(gf)(x) = f(xg)$. Сопоставляя каждому элементу $f \in \text{Ind}_G^H(A)$ его значение в единице, получаем гомоморфизм $\text{Ind}_G^H(A) \to A$, который определяет гомоморфизм

$$H^i(G, \text{Ind}_G^H(A)) \to H^i(H, A). \quad (5)$$

Оказывается, что гомоморфизм (5) является изоморфизмом («лемма Шапиро»). Предположим теперь, что H имеет конечный индекс в G и A является G-группой. Тогда можно определить сюръективный G-гомоморфизм π: $\text{Ind}_G^H(A) \to A$, полагая $\pi(f) = \sum_{x \in G/H} xf(x^{-1})$ (легко видеть, что эта сумма не зависит от выбора представителей). Тогда, переходя к когомологиям, получим *гомоморфизм коограничения* Cor: $H^i(H, A) \simeq H^i(G, \text{Ind}_G^H(A)) \to H^i(G, A)$, где $\simeq$ обозначает изоморфизм, обратный к (5). Отметим, что в размерности нуль гомоморфизм Cor: $A^H \to A^G$ совпадает с отображением следа $\text{Tr}(a) = \sum_{g \in G/H} g(a)$ (или, в мультипликативных обозначениях, — нормы).

Иногда приходится рассматривать непрерывные когомологии топологической группы G с коэффициентами в топологической абелевой G-группе A такой, что действие G на A непрерывно. Их определение получается, если вместо обычных коцепей рассматривать непрерывные. В этой книге (за исключением некоторых мест в § 9.5, где рассматриваются когомологии групп

аделей) мы будем работать исключительно с непрерывными когомологиями проконечной (т. е. компактной вполне несвязной) группы G с коэффициентами в дискретной группе A; при этом непрерывность действия G на A означает, что $A = \bigcup_U A^U$, где объединение берется по всем открытым нормальным делителям $U \subset G$. Для проконечной группы G имеет место представление в виде проективного предела $G = \varprojlim G/U$, где U пробегает некоторую фундаментальную систему окрестностей единицы, состоящую из нормальных делителей (основные факты о проконечных группах мы напоминаем в § 3.2); тогда группа когомологий $H^i(G, A)$ дискретной G-группы A представляется в виде индуктивного предела $\varinjlim H^i(G/U, A^U)$ относительно отображений инфляции $H^i(G/U, A^U) \to H^i(G/V, A^V)$ при $U \supset V$. Один из основных примеров связан с рассмотрением абсолютной группы Галуа $\mathcal{G} = \mathrm{Gal}(\bar{K}/K)$ некоторого совершенного поля K и ее естественного действия, скажем, на аддитивной или мультипликативной группе поля $\bar{K}$ или на некотором другом объекте A с K-структурой (см. § 2.2). Тогда соответствующие когомологии $H^i(\mathcal{G}, A)$ называются *когомологиями Галуа* и обозначаются $H^i(K, A)$.

Легко проверяется, что когомологии проконечной группы G с коэффициентами в дискретной группе A обладают всеми основными свойствами обычных когомологий. В частности, точной последовательности дискретных G-групп и G-гомоморфизмов $0 \to A \to B \to C \to 0$ отвечает точная когомологическая последовательность (1), а расширению $1 \to N \to G \to G/N \to 1$ проконечных групп — отрезок спектральной последовательности Хохшильда — Серра (4).

2. Неабелевы когомологии. При работе с алгебраическими группами возникают коциклы, принимающие значения в группе точек над некоторым (конечным или бесконечным) расширением Галуа поля определения, т. е. область значений коциклов является, вообще говоря, некоммутативной группой. С подобной ситуацией мы сталкиваемся и в других случаях, например, при изучении скрещенных произведений некоммутативных алгебр с некоторой конечной группой. Тем самым некоммутативные когомологии вполне заслуживают самостоятельного изучения; им посвящена книга Жиро [1], к которой мы и отсылаем заинтересованного читателя. В настоящем пункте мы напомним основные понятия, связанные с некоммутативными когомологиями, которые понадобятся нам при изучении когомологий Галуа алгебраических групп (см. Серр [2]).

Пусть G — некоторая группа (дискретная или проконечная), действующая на некотором множестве A, которое в топологическом случае предполагается дискретным, а действие G на

A — непрерывным. В этом случае A называется G-множеством. Если A — группа, а G действует на A автоморфизмами, то A называется G-группой. Для G-множества A определим $H^0(G, A)$ как множество G-инвариантных элементов A^G. Если A является G-группой, то $H^0(G, A)$ является группой.

Для G-группы A отображение f: $G \to A$ (непрерывное в топологической ситуации) называется *одномерным коциклом* или 1-*коциклом* со значениями в A, если для любых $s, t \in G$ выполняется соотношение $f(st) = f(s)s(f(t))$. Часто бывает удобно трактовать 1-коциклы как семейства, индексированные элементами группы G, и писать $f = \{f_s | s \in G\}$, имея в виду, что $f_s = f(s)$. Действие G на A бывает удобно записывать в экспоненциальной форме, т. е. писать ${}^s a$ вместо $s(a)$. С учетом этих соглашений условие на 1-коцикл записывается в виде $f_{st} = f_s {}^s f_t$. Множество всех коциклов будем обозначать через $Z^1(G, A)$. Множество $Z^1(G, A)$ непусто — оно всегда содержит единичный коцикл, определенный условием: $f_s = e$ — единичный элемент A для всех $s \in G$. Два коцикла (a_s) и (b_s) называются эквивалентными, если найдется элемент $c \in A$ такой, что $b_s = c^{-1} a_s {}^s c$ для всех $s \in G$. (Легко проверяется, что таким образом определенное отношение между коциклами действительно является отношением эквивалентности на множестве $Z^1(G, A)$.) Множество классов эквивалентности называется *множеством одномерных когомологий группы с коэффициентами в* A и обозначается $H^1(G, A)$. Если A — абелева группа, то это определение H^1 эквивалентно приведенному в п. 1, в частности, в этом случае $H^1(G, A)$ является абелевой группой. В общем случае $H^1(G, A)$ не несет никакой естественной групповой структуры и является лишь множеством с отмеченным элементом, которым служит класс эквивалентности единичного коцикла. Как и выше, если G — проконечная группа и $G = \varprojlim G/U$ то $H^1(G, A) = \varinjlim H^1(G/U, A^U)$ — индуктивный предел множеств с отмеченным элементом относительно очевидным образом определяемых отображений инфляции $H^1(G/U, A^U) \to H^1(G/V, A^V)$ для $U \supset V$, которые сохраняют отмеченные элементы. Вообще, если f: $A \to B$ — гомоморфизм G-группы A в H-группу B, совместный с гомоморфизмом g: $H \to G$, т. е. $f({}^{g(s)}a) = {}^s f(a)$ для всех $s \in H$, $a \in A$, то можно определить отображение $Z^1(G, A) \to Z^1(H, B)$, переводящее (a_s) в $(b_s = f(a_{g(s)}))$, которое индуцирует отображение множеств с отмеченными элементами (морфизм)

$$H^1(G, A) \to H^1(H, A).$$

Будем говорить, что последовательность множеств когомологий *точна*, если она точна как последовательность множеств с отмеченными элементами, т. е. прообраз отмеченного элемента

равен образу предыдущего отображения. (Отмеченным элементом во множестве нулевых когомологий $H^0(G, A)$ считается единичный элемент группы A.) Укажем на основные типы используемых нами точных последовательностей. Пусть A — подгруппа G-группы B, инвариантная относительно действия группы G. Тогда на множестве B/A левых смежных классов можно определить естественное действие группы G, так что B/A является G-множеством, и определено множество $H^0(G, B/A)$, которое обладает отмеченным элементом — классом A. Для любого элемента из $H^0(G, B/A) = (B/A)^G$ выберем представитель $b \in B$ и для $s \in G$ положим $a_s = b^{-1s}b$. Несложно проверить, что $a_s \in A$ и $(a_s) \in Z^1(G, A)$. При этом класс эквивалентности последнего коцикла не зависит от выбора представителя b, и мы получаем отображение δ: $H^0(G, B/A) \to H^1(G, A)$.

Прямое вычисление показывает, что имеет место точная последовательность множеств с отмеченными элементами:

$$1 \to H^0(G, A) \to H^0(G, B) \to H^0(G, B/A) \xrightarrow{\delta} H^1(G, A) \xrightarrow{\alpha} H^1(G, B), \tag{6}$$

где α индуцировано вложением $A \hookrightarrow B$. Кроме того, если c_1, $c_2 \in H^0(G, B/A)$, то $\delta(c_1) = \delta(c_2)$ в том и только том случае, когда существует $b \in B^G$ со свойством $c_2 = bc_1$. Отсюда следует, что элементы ядра отображения $H^1(G, A) \to H^1(G, B)$ находятся во взаимно однозначном соответствии с орбитами действия B^G на $(B/A)^G$. Если A — нормальный делитель в B, то последовательность (6) продолжается еще на один член:

$$\ldots \to H^0(G, B/A) \xrightarrow{\delta} H^1(G, A) \xrightarrow{\alpha} H^1(G, B) \xrightarrow{\beta} H^1(G, B/A). \tag{7}$$

Особого рассмотрения заслуживает случай, когда A — центральная подгруппа группы B (именно с такой ситуацией мы сталкиваемся, рассматривая универсальные накрытия алгебраических групп). Положим $C = B/A$ и обозначим через φ: $B \to C$ — канонический гомоморфизм. Тогда $H^1(G, A)$ является группой и отображение δ: $H^0(G, C) = C^G \to H^1(G, A)$ является гомоморфизмом групп; в дальнейшем мы будем называть его *кограничным гомоморфизмом*. Используя центральность A, можно определить естественное действие группы $H^1(G, A)$ на множестве $H^1(G, B)$: если $a = (a_s) \in Z^1(G, A)$, $b = (b_s) \in Z^1(G, B)$, то $a \cdot b = (a_s b_s) \in Z^1(G, B)$. Тогда оказывается, что орбиты этого действия совпадают со слоями морфизма β: $H^1(G, B) \to H^1(G, C)$. Далее, в силу коммутативности A определена группа $H^2(G, A)$, и как мы сейчас покажем, существует отображение ∂: $H^1(G, C) \to H^2(G, A)$, расширяющее последовательность (7) до точной последовательности

$$\ldots \to H^1(G, B) \xrightarrow{\beta} H^1(G, C) \xrightarrow{\partial} H^2(G, A). \tag{8}$$

Пусть $c=(c_s)\in Z^1(G, C)$; для каждого $s\in G$ мы можем найти такой элемент $b_s\in B$, что $\varphi(b_s)=c_s$. Положим тогда $a_{s,t}=b_s^s b_t b_{st}^{-1}$. Легко проверяется, что $a_{s,t}\in A$ и отображение $G\times G\to A$, $(s,t)\to a_{s,t}$ является 2-коциклом (т. е. элементом из $Z^2(G, A)$). Оказывается, что класс, определяемый коциклом a, не зависит ни от выбора элементов b_s, ни от выбора коцикла c в соответствующем классе эквивалентности в $H^1(G, C)$, и таким образом мы получаем корректно определенный кограничный морфизм ∂: $H^1(G, C)\to H^2(G, A)$. Непосредственно проверяется, что соответствующая последовательность (8) точна. Отметим, что в некоммутативном случае морфизм ∂ не связан ни с какой групповой структурой; более того, его образ в $H^2(G, A)$, вообще говоря, не является подгруппой.

В некоммутативной ситуации указанные точные последовательности несут существенно меньше информации, чем в коммутативном случае, ибо, скажем, знание ядра некоторого отображения множеств с отмеченными элементами, вообще говоря, не позволяет сделать выводы о всех его слоях. Частично эту трудность можно преодолеть при помощи одного приема, основанного на понятии *скручивания* (см. Серр [2], гл. I, § 5). Напомним основные определения. Пусть A — некоторая G-группа и F — некоторое G-множество с заданным действием группы A, причем это действие перестановочно с действием G, т. е. $s(a\cdot f)=s(a)\cdot s(f)$ для любых $s\in G$, $a\in A$, $f\in F$. Тогда с помощью произвольного коцикла $a=(a_s)\in Z^1(G, A)$ можно определить новое действие G на F по формуле

$$\bar{s}(f)=a_s(s(f)),\quad s\in G.$$

Множество F с этим действием обозначается через ${}_aF$. При этом говорят, что ${}_aF$ получено из F скручиванием при помощи коцикла a. Легко видеть, что множество ${}_aF$ функториально зависит от F (относительно A-морфизмов $F\to F'$) и что конструкция скручивания перестановочна с прямыми произведениями. Для эквивалентных в $Z^1(G, A)$ коциклов a и b G-множества ${}_aF$ и ${}_bF$ изоморфны. Кроме того, если F обладает некоторой структурой (например группы), а элементы A сохраняют эту структуру, то ${}_aF$ также наделяется этой структурой. Целый ряд примеров скручивания будет рассмотрен в § 2.3, а пока мы ограничимся одним примером, который возникает при работе с точными последовательностями. А именно, рассмотрим случай, когда $A=F$ действует на себе внутренними автоморфизмами. Тогда для любого коцикла $a\in Z^1(G, A)$ определена скрученная группа ${}_aA$, причем множества одномерных когомологий групп A и $A'={}_aA$ связаны между собой следующим образом:

Лемма 4. *Для произвольного коцикла $x=(x_s)\in Z^1(G, A')$ семейство $y=(x_s a_s)$ является коциклом в $Z^1(G, A)$, причем со-*

ответствие $x \mapsto y$ задает биекцию t_a: $Z^1(G, A') \to Z^1(G, A)$. При переходе к когомологиям t_a индуцирует биекцию τ_a: $H^1(G, A') \to H^1(G, A)$, которая переводит отмеченный элемент из $H^1(G, A')$ в класс коцикла a.

Тем самым мы получаем возможность перемножать коциклы, правда, переходя при этом к скрученной группе. При помощи этого приема, заменяя группы в последовательностях (6)—(8) на соответствующие скрученные группы (как мы будем говорить в дальнейшем, скручивая эти последовательности), можно получить описание слоев всех отображений в исходных последовательностях. Пусть, например, в ситуации, описанной при построении последовательности (6), $a \in Z^1(G, A)$ и мы желаем получить описание слоя $\alpha^{-1}(\alpha(a))$ (мы обозначаем той же буквой a соответствующий класс эквивалентности в $H^1(G, A)$). Для этого следует перейти к скрученным группам $A' = {}_aA$ и $B' = {}_aB$ и рассмотреть для них аналог точной последовательности (6)

$$1 \to H^0(G, A') \to H^0(G, B') \to H^0(G, B'/A') \xrightarrow{\delta}$$
$$\xrightarrow{\delta} H^1(G, A') \xrightarrow{\alpha'} H^1(G, B'). \quad (6')$$

Тогда биекция τ_a из леммы 4 устанавливает биекцию между элементами $\operatorname{Ker}\alpha'$ и элементами слоя $\alpha^{-1}(\alpha(a))$. С другой стороны, как следует из (6′), элементы $\operatorname{Ker}\alpha'$ находятся в биективном соответствии с орбитами действия $(B')^G$ на $(B'/A')^G$. Приведем также критерий того, когда класс некоторого коцикла $b \in Z^1(G, B)$ лежит в образе отображения α. Для этого условимся рассматривать действие B на множестве смежных классов (однородном пространстве) B/A посредством сдвигов; тем самым для любого $b \in Z^1(G, B)$ определено скрученное пространство ${}_b(B/A)$.

Лемма 5. $b \in \operatorname{Im}\alpha \Leftrightarrow H^0(G, {}_b(B/A)) \neq \varnothing$.

Аналогичным образом вычисляются слои отображения ∂ в последовательности (8). А именно, пусть $c = (c_s) \in Z^1(G, C)$. Так как A — центральная подгруппа в B, то группа C действует внутренними автоморфизмами на B, причем эти автоморфизмы тривиальны на A. Скрутив с помощью c точную последовательность $1 \to A \to B \to C \to 1$, мы получим точную последовательность $1 \to A \to {}_cB \to {}_cC \to 1$, из которой возникает новый кограничный морфизм ∂_c: $H^1(G, {}_cC) \to H^2(G, A)$. Прямое вычисление показывает, что этот морфизм связан с биекцией τ_c: $H^1(G, {}_cC) \to H^1(G, C)$ из леммы 4 следующим образом: $\partial(\tau_c(x)) = \partial_c(x)\,\partial(c)$ в смысле умножения в группе $H^2(G, A)$. Отсюда следует, что элементы слоя $\partial^{-1}(\partial(c))$ находятся в биективном соответствии с элементами $\operatorname{Ker}\partial_c$, которые, в свою очередь, биективно соответствуют элементам фактормножества $H^1(G, {}_cB)$ относительно действия группы $H^1(G, A)$.

Если H — нормальный делитель в G (замкнутый в топологической ситуации), то, как и в коммутативном случае, фактор-группа G/H действует на A^H, так что можно определить $H^1(G/H, A^H)$ и отображение инфляции $H^1(G/H, A^H) \to H^1(G, A)$. Тогда если $H^1(G, A) \to H^1(H, A)$ — отображение ограничения, то точна последовательность

$$1 \to H^1(G/H,\ A^H) \to H^1(G,\ A) \to H^1(H,\ A),$$

которую можно рассматривать как некоммутативный аналог последовательности Хохшильда — Серра (4).

Нам осталось рассмотреть индуцированные множества и некоммутативный вариант леммы Шапиро. Остановимся на этих вопросах более подробно, ибо они не вошли в книгу Серра [1]. Пусть H — подгруппа в G, предполагаемая замкнутой в топологической ситуации. Тогда для любого H-множества (соответственно H-группы) B можно определить G-множество (соответственно G-группу) $A = \mathrm{Ind}_G^H(B)$, которая состоит из всех непрерывных отображений a: $G \to B$, удовлетворяющих условию $a(ts) = {}^t a(s)$ для всех $t \in H$, $s \in G$, причем действие G на A задается формулой ${}^r a(s) = a(sr)$ для $r \in G$. G-множество (соответственно G-группа) A или любое G-множество (G-группа), изоморфное A, называются G — H-индуцированными. Отображение $A \to B$, $a \mapsto a(1)$, согласовано с включением $H \subset G$, и поэтому для $i = 0$, 1 индуцирует морфизмы

$$\varphi_i\colon\ H^i(G,\ A) \to H^i(H,\ B).$$

Предложение 7 (лемма Шапиро; некоммутативный вариант). *Отображения φ_i биективны.*

Доказательство. Рассмотрим отдельно случаи $i = 0$ и $i = 1$. Пусть вначале $i = 0$. Если $a \in H^0(G, A)$, то a есть отображение $G \to B$, инвариантное относительно действия G, т. е. $a = {}^r a$ для всех $r \in G$. Вспоминая определение действия G на A, мы видим, что последнее равенство эквивалентно соотношению $a(s) = a(sr)$ для всех s, $r \in G$. Полагая $s = 1$, получим, что a является постоянным отображением. По определению $\varphi_0(a) = a(1) \in B^H = H^0(H, B)$, откуда следует, что соотношение $\varphi_0(a) = \varphi_0(b)$ для a, $b \in H^0(G, A)$ влечет $a = b$, т. е. φ_0 инъективно. С другой стороны, для любого $c \in H^0(H, B)$ постоянное отображение a: $G \to B$, $a(s) = c$, лежит в A, причем легко проверяется, что $a \in H^0(G, A)$ и $\varphi_0(a) = c$.

Пусть теперь $i = 1$. Для доказательства инъективности φ_1 предположим, что классы коциклов $a = (a_r)$ и $b = (b_r) \in Z^1(G, A)$ переходят при отображении φ_1 в один и тот же элемент. Тогда для подходящего элемента $c \in B$ имеем $a_r(1) = c^{-1} b_r(1)\, {}^r c$ для всех $r \in H$. Легко видеть, что существует такой элемент $d \in A$, что $d(1) = c$. Тогда, заменяя коцикл b на

эквивалентный коцикл $b' = (d^{-1} b_r {}^r d)$, можно предполагать, что

$$a_r(1) = b_r(1) \text{ для всех } r \in H. \tag{9}$$

Из определения коцикла для всех r, s, $t \in G$ получаем соотношения

$$a_{rs}(t) = a_r(t)\, {}^r a_s(t) = a_r(t)\, a_s(tr),$$
$$b_{rs}(t) = b_r(t)\, {}^r b_s(t) = b_r(t)\, b_s(tr).$$

Полагая $r = t^{-1}$, из (9) находим, что

$$a_{t^{-1}s}(t)\, b_{t^{-1}s}(t)^{-1} = a_{t^{-1}}(t)\, b_{t^{-1}}(t)^{-1} \tag{10}$$

для всех $s \in H$. Определим функцию c: $G \to B$ равенством

$$c(t) = b_{t^{-1}}(t)\, a_{t^{-1}}(t)^{-1}.$$

Тогда из (10) для $s \in H$ получаем

$$c(st) = b_{t^{-1}s^{-1}}(st)\, a_{t^{-1}s^{-1}}(st)^{-1} =$$
$$= s\left(b_{t^{-1}s^{-1}}(t)\, a_{t^{-1}s^{-1}}(t)^{-1}\right) = s\left(b_{t^{-1}}(t)\, a_{t^{-1}}(t)\right) = s(c(t)),$$

т. е. $c \in A$. С другой стороны, непосредственно проверяется, что $a_r = c^{-1} b_r {}^r c$ для всех $r \in G$, и, значит, коциклы a и b эквивалентны. Инъективность φ_1 доказана.

Для доказательства сюръективности φ_1 рассмотрим произвольный коцикл $b = (b_r) \in Z^1(H, B)$. Пусть v: $G/H \to G$ — некоторое сечение, предполагаемое непрерывным в топологической ситуации и такое, что $v(H) = 1$. Тогда для $s \in G$ положим $w(s) = sv(Hs)^{-1} \in H$. Для каждого $s \in G$ определим функцию a_s: $G \to B$ формулой $a_s(t) = {}^{w(t)} b_{w(v(t)s)}$. Прямое вычисление показывает, что $a_s \in A$ и семейство $a = (a_s)$ образует коцикл в $Z^1(G, A)$, причем $\varphi_1(a) = b$. Предложение полностью доказано.

В приложениях оказывается полезным следующее простое утверждение:

Лемма 6. *Пусть H имеет конечный индекс в G. Тогда G-группа A является G — H-индуцированной в том и только том случае, если существует H-подгруппа $B \subset A$ такая, что A является прямым произведением групп ${}^s B$, где s пробегает некоторую систему представителей смежных классов G/H.*

Например, если L — конечное расширение Галуа поля алгебраических чисел K с группой Галуа $\mathscr{G}$, $v \in V^K$, u — некоторое продолжение нормирования v на L и $\mathscr{H} = \mathscr{G}(u)$ — соответствующая группа разложения, то, как показывает разложение (2) § 1.1, $\mathscr{G}$-модуль $L \otimes_K K_v$ изоморфен $\mathrm{Ind}_{\mathscr{H}}^{\mathscr{G}(u)}(L_u)$.

§ 1.4. Простые алгебры над локальными полями

1. Простые алгебры и группы Брауэра. Пусть A — конечномерная простая центральная алгебра над полем K (центральность означает, что центр A совпадает с K). Тогда A является полной матричной алгеброй $M_n(D)$ над некоторой центральной алгеброй с делением (телом) D над K и $\dim_K A = n^2 \dim_K D$. В свою очередь, размерность $\dim_K D$ является квадратом некоторого натурального числа d, называемого *индексом* тела D и соответственно алгебры A. Известно, что если K конечно или алгебраически замкнуто, то необходимо $d=1$, т. е. некоммутативных конечномерных центральных алгебр с делением над K нет. Если $K=\mathbb{R}$ и $d>1$, то D изоморфно телу обычных гамильтоновых кватернионов $\mathbb{H}$. Над неархимедовыми локальными полями или полями алгебраических чисел существуют тела произвольного индекса. Для их описания нам понадобятся некоторые факты из теории простых алгебр (см., например, Херстейн [1], Пирс [1]).

Один из таких фактов — это *теорема Сколема — Нётер*, утверждающая, что произвольный изоморфизм σ: $B_1 \to B_2$ двух простых подалгебр B_1, B_2 конечномерной центральной простой K-алгебры A, тривиальный на K, продолжается до внутреннего автоморфизма A. Важную роль при исследовании алгебры с делением D играют *максимальные подполя* $P \subset D$. Они обязательно содержат поле K и имеют над ним степень d; при этом $D \otimes_K P \simeq M_d(P)$. Обратно, если P — расширение K степени d и $D \otimes_K P \simeq M_d(P)$ (т. е. P — *поле разложения* D), то P изоморфно максимальному подполю в D. Рассмотрим произвольное поле разложения P простой алгебры A (можно, например, в качестве P выбрать алгебраическое замыкание $\bar{K}$) и зафиксируем соответствующий изоморфизм φ: $A \otimes_K P \simeq M_r(P)$. Тогда отображение $\mathrm{Nrd}_{A/K}(x) = \det \varphi(x \otimes 1)$, называемое *приведенной нормой*, является мультипликативным, не зависит ни от P, ни от φ и задается однородным многочленом степени r с коэффициентами из K от координат элемента x в некотором базисе A над K; в частности, $\mathrm{Nrd}_{A/K}(A^*) \subset K^*$. Часто используемое нами свойство приведенной нормы состоит в том, что для $x \in D$ приведенная норма $\mathrm{Nrd}_{D/K}(x)$ совпадает с обычной нормой $N_{P/K}(x)$ из максимального подполя $P \subset D$, содержащего x. Изучение мультипликативной группы A^* в существенной степени сводится к изучению образа приведенной нормы $\mathrm{Nrd}_{A/K}(A^*)$ и соответствующей специальной линейной группы $SL_1(A) = \{x \in A^* \mid \mathrm{Nrd}_{A/K}(x) = 1\}$. В свою очередь, строение группы $SL_1(A)$ (особенно в случае, когда $A = M_n(D)$, $n > 1$, см. § 7.2) зависит от того, совпадает группа $SL_1(A)$ с коммутантом $[A^*, A^*]$ или нет (отметим, что включение $[A^*, A^*] \subset SL_1(A)$ вытекает из мультипликативности приведенной нормы). Этот вопрос, по-

ставленный Таннакой и Артином в 1943 г., в терминах алгебраической K-теории эквивалентен вопросу о тривиальности так называемой *приведенной группы Уайтхеда* $SK_1(A) = SL_1(A)/[A^*, A^*]$. О связи этих проблем с известной в теории алгебраических групп *гипотезой Кнезера — Титса* см. § 7.2. Проблема Таннаки — Артина была отрицательно решена В. П. Платоновым в 1975 г. В работах [13] — [16] им была развита *приведенная K-теория*, позволяющая во многих случаях вычислять группу $SK_1(A)$ и устанавливать ее связь с другими арифметическими вопросами (см. гл. VII). Тем не менее, в интересующих нас случаях локальных и глобальных полей группа $SK_1(A)$ всегда тривиальна (для локальных полей этот результат был впервые получен Накаямой — Мацусимой [1] в 1943 г., а для полей алгебраических чисел — Вангом [1] в 1950 г.). Так как этот факт неоднократно будет использоваться в книге, ниже мы приведем его доказательство, которое существенно отличается от оригинального и является более коротким и концептуальным.

Введем на множестве конечномерных центральных простых алгебр над полем K отношение эквивалентности, считая, что $A_1 = M_{n_1}(D_1) \sim A_2 = M_{n_2}(D_2)$, если тела D_1 и D_2 изоморфны, и определим произведение классов эквивалентности формулой $[A_1] \cdot [A_2] = [A_1 \otimes_K A_2]$ (отметим, что тензорное произведение над K двух простых K-алгебр, одна из которых центральна, также является простой K-алгеброй). Эта операция превращает множество классов эквивалентности конечномерных центральных простых K-алгебр в абелеву группу (обратным к классу $[A]$ является класс противоположной алгебры A^0, которая получается из A заданием нового произведения по формуле $a \circ b = ba$, где справа стоит произведение в алгебре A), которая называется *группой Брауэра* поля K и обозначается $\mathrm{Br}(K)$. Для любого расширения L/K классы эквивалентности таких центральных простых K-алгебр A, для которых L является полем разложения, образуют подгруппу в $\mathrm{Br}(K)$, которая обозначается через $\mathrm{Br}(L/K)$. Порядок элемента $[A]$ в $\mathrm{Br}(K)$ всегда конечен; он называется *экспонентой* алгебры A. Отметим, что экспонента алгебры A делит ее индекс и в общем случае отлична от него. Одним из глубоких результатов теории алгебр является совпадение экспоненты и индекса над локальными и глобальными полями (в связи с этим укажем на гипотезу о том, что так называемые C_2-поля также обладают этим свойством (см. М. Артин [1])). Отметим, что группа Брауэра $\mathrm{Br}(K)$ имеет когомологическую интерпретацию. А именно, сопоставление простой алгебре соответствующей системы факторов (см. Ван дер Варден [1]) определяет изоморфизм

$$\mathrm{Br}(K) \simeq H^2(K, \bar{K}^*),$$

2. Простые алгебры над локальными полями. Пусть D — тело индекса n над (неархимедовым) локальным полем K. Всюду в этом параграфе через v будет обозначаться нормирование поля K, через $\mathcal{O}$ — кольцо нормирования с идеалом нормирования $\mathfrak{p}$ и через $U=\mathcal{O}^*$ — соответствующая группа единиц. Нормирование v единственным образом продолжается на D при помощи формулы

$$\tilde{v}(x)=\frac{1}{n}v(\mathrm{Nrd}_{D/K}(x)),\quad x\in D, \tag{1}$$

причем D полно в топологии, определяемой этим нормированием (для тел нормирования определяются так же, как и для полей, см. Пирс [1]). Пусть $\mathcal{O}_D=\{x\in D\mid \tilde{v}(x)\geqslant 0\}$ и $\mathfrak{P}_D=\{x\in D\mid \tilde{v}(x)>0\}$ — соответственно кольцо целых и идеал нормирования $\tilde{v}$. Легко видеть, что $\mathfrak{P}_D$ является максимальным двусторонним идеалом в $\mathcal{O}_D$, так что определено тело вычетов $\bar{D}$. Пусть $f=[\bar{D}:k]$ — степень тела вычетов (k — поле вычетов для K) и $e=[\tilde{\Gamma}:\Gamma]$ (где $\Gamma=v(K^*)$, $\tilde{\Gamma}=\tilde{v}(D^*)$ — группы значений нормирований v и $\tilde{v}$) — соответствующий индекс ветвления. Тогда, как и в коммутативном случае (см. § 1.1, п. 2), $ef=\dim_K D=n^2$. С другой стороны, $\bar{D}$, будучи конечным телом, коммутативно, и, следовательно, $\bar{D}=k(\alpha)$ для подходящего $\alpha\in\bar{D}$. Пусть $\beta\in\mathcal{O}_D$ — такой элемент, что вычет $\bar{\beta}$ совпадает с α (в дальнейшем черта всюду будет обозначать образ в поле или теле вычетов). Тогда для поля $L=K(\beta)$ и соответствующего поля вычетов l имеем

$$f=[\bar{D}:\bar{K}]=[l:k]\leqslant[L:K]=n.$$

Из формулы (1) вытекает, что умножение на n индуцирует изоморфизм $\tilde{\Gamma}$ в Γ и поскольку $\Gamma\simeq\mathbb{Z}$, то $e=[\tilde{\Gamma}:\Gamma]\leqslant n$. Отсюда следует, что в действительности $e=f=n$ и тело вычетов $\bar{D}$ совпадает с полем вычетов l подходящего подполя $L\subset D$, которое автоматически является максимальным подполем в D и неразветвлено над K. Группа значений $\tilde{\Gamma}$ является бесконечной циклической, так что существует элемент $\Pi\in D^*$, называемый *униформизующим*, со свойством $\tilde{v}(\Pi)=1/n$. Имеем $\mathfrak{P}_D=\Pi\mathcal{O}_D=\mathcal{O}_D\Pi$, причем любой другой униформизующий элемент $\Pi'\in\mathcal{O}_D$ имеет вид $\Pi'=\Pi u$, $u\in U_D=\mathcal{O}_D^*$. Аналогично, для любого $i\geqslant 1$ имеем $\mathfrak{P}_D^i=\Pi^i\mathcal{O}_D=\mathcal{O}_D\Pi^i$.

Зафиксируем максимальное неразветвленное подполе $L\subset D$ (отметим, что любое другое максимальное неразветвленное подполе $L'\subset D$ изоморфно L над K и поэтому в силу теоремы Сколема — Нётер сопряжено L). Расширение L/K является циклическим расширением Галуа и группа Галуа $\mathrm{Gal}(L/K)$ порождается автоморфизмом Фробениуса φ (см. § 1.1, п. 3). По

теореме Сколема — Нётер существует такой элемент $g \in D^*$, что

$$\varphi(x) = gxg^{-1} \quad \forall x \in L. \tag{2}$$

Тогда образ элемента $\tilde{v}(g) \in \frac{1}{n}\mathbb{Z}$ в группе $\mathbb{Q}/\mathbb{Z}$ определен корректно, называется *инвариантом* тела D и обозначается $\mathrm{inv}_K(D)$. *Инвариантом* $\mathrm{inv}(A)$ *простой алгебры* $A = M_n(D)$ называется инвариант тела D.

Теорема 7. *Отображение* $A \mapsto \mathrm{inv}_K A$ *определяет изоморфизм* $\mathrm{Br}(K) \simeq \mathbb{Q}/\mathbb{Z}$. *При этом если* P/K — *конечное расширение степени* m, *то коммутативна следующая диаграмма*:

$$\begin{tikzcd} \mathrm{Br}(K) \arrow[r, "\mathrm{inv}_K"] \arrow[d, "{[A]}", "{[A \otimes_K P]}"'] & \mathbb{Q}/\mathbb{Z} \arrow[d, "{[m]}"] \\ \mathrm{Br}(P) \arrow[r, "\mathrm{inv}_P"] & \mathbb{Q}/\mathbb{Z} \end{tikzcd} \tag{3}$$

где $[m]$ *означает умножение на* m.

Из коммутативности (3) вытекает, что если D — тело индекса n над K, то для любого расширения P/K степени n имеем $D \otimes_K P \simeq M_n(P)$, следовательно, P изоморфно максимальному подполю в D. Еще одно важное наблюдение состоит в следующем: над полем K экспонента любого тела совпадает с его индексом. В самом деле, нужно показать, что если $\tilde{v}(g) = a/n$, то $(a, n) = 1$. Для доказательства заметим, что в силу (1) $\mathcal{O}_D$ и $\mathfrak{P}_D$ инвариантны относительно сопряжения в D, и поэтому *любой* элемент $h \in D^*$ индуцирует автоморфизм σ_h: $\bar{x} \mapsto \overline{hxh^{-1}}$ тела $\bar{D}$ над k. Положим $\sigma = \sigma_\Pi$. Из коммутативности $\bar{D}$ вытекает, что для $u \in U_D$ имеем $\sigma_u = \mathrm{id}$, так что σ не зависит от выбора униформизующего Π. Мы видели, что $\bar{D}$ совпадает с полем вычетов l максимального неразветвленного подполя $L \subset D$, так что в действительности $\sigma \in \mathrm{Gal}(l/k)$. Имеем $g = \Pi^a u$, $u \in U_D$, и поэтому $\varphi = \sigma^a$ (мы обозначаем одной и той же буквой автоморфизм Фробениуса расширений L/K и l/k). Так как φ порождает $\mathrm{Gal}(l/k)$, то необходимо $(a, n) = 1$. Одновременно мы показали, что $\sigma = \sigma_\Pi$ порождает $\mathrm{Gal}(l/k)$, что будет использовано ниже.

Изложенные факты о строении тел над полями p-адических чисел восходят к Хассе [1], Витту [1]. Отметим, что недавно были получены структурные теоремы для широкого класса тел над произвольными гензелевыми полями (см. Платонов, Янчевский [3], [4]).

3. Мультипликативная структура тел над локальными полями. Прежде всего установим, что для конечномерного центрального тела D над полем K имеем $\mathrm{Nrd}_{D/K}(D^*) = K^*$ и группа $SL_1(D)$ совпадает с коммутантом $[D^*, D^*]$ (более тщательное

исследование группы D^* при помощи фильтрации, определяемой конгруэнц-подгруппами, мы проведем в следующем пункте).

Мы уже видели, что существует максимальное неразветвленное подполе $L \subset D$, и поэтому группа единиц U лежит в $N_{L/K}(L^*) \subset \mathrm{Nrd}_{D/K}(D^*)$ (см. предложение 2). Остается показать, что $\mathrm{Nrd}_{D/K}(D^*)$ содержит униформизующий элемент π поля K. Для этого заметим, что многочлен $t^n + (-1)^n \pi$ (n — индекс D) является многочленом Эйзенштейна (см. п. 3 § 1.1) и поэтому определяет некоторое расширение P/K степени n, причем $\pi \in N_{P/K}(P^*)$. Но, как мы отмечали, P изоморфно максимальному подполю в D, и поэтому $N_{P/K}(P^*) \subset \mathrm{Nrd}_{D/K}(D^*)$, т. е. $\pi \in \mathrm{Nrd}_{D/K}(D^*)$. Таким образом, равенство $\mathrm{Nrd}_{D/K}(D^*) = K^*$ доказано.

Доказательство утверждения о том, что группа $SL_1(D)$, которую мы в дальнейшем будем для краткости обозначать $D^{(1)}$, совпадает с коммутантом $[D^*, D^*]$, является несколько более сложным. Во-первых, заметим, что группа $L^{(1)} = L \cap D^{(1)}$ содержится в $[D^*, D^*]$. Действительно, по «теореме 90» Гильберта (см. Ленг [3], гл. VIII) любой элемент $x \in L^{(1)} = \{t \in L^* \mid N_{L/K}(t) = 1\}$ имеет вид $x = \varphi(y) y^{-1}$ для подходящего $y \in L^*$. Тогда $x = gyg^{-1}y^{-1} \in [D^*, D^*]$ в силу (2). Поэтому требуемый факт вытекает из следующего утверждения.

Теорема 8 (Платонов, Янчевский [2]). *Нормальный делитель в $D^{(1)}$, порожденный группой $L^{(1)}$, совпадает с $D^{(1)}$.*

Доказательство. Пусть $x \in D^{(1)}$, тогда вычет $\bar{x}$ лежит в группе $l^{(1)} = \{a \in l^* \mid N_{l/k}(a) = 1\}$. Действительно, x можно представить в виде $x = ab$, где a принадлежит группе единиц U_L поля L, а $b \in 1 + \mathfrak{P}_D$. Тогда $\bar{x} = \bar{a}$. С другой стороны, $N_{L/K}(a) = \mathrm{Nrd}_{D/K}(a) = \mathrm{Nrd}_{D/K}(b^{-1}) = N_{M/K}(b)^{-1}$ для максимального подполя $M \subset D$, содержащего b. Но $b \in (1 + \mathfrak{P}_D) \cap M = 1 + \mathfrak{P}_M$, так что, согласно предложению 3, $N_{M/K}(b^{-1}) \in 1 + \mathfrak{p}$, где $\mathfrak{p}$ — идеал нормирования в K. Поэтому $N_{l/k}(\bar{a}) = \prod_{i=0}^{n-1} \varphi^i(\bar{a}) = \overline{\prod_{i=0}^{n-1} \varphi^i(a)} = \overline{N_{L/K}(a)} = 1$. Поскольку группа $l^{(1)}$ циклическая, существует такой элемент $z \in l^{(1)}$, что элемент $\bar{x}z$ является образующим $l^{(1)}$, и, следовательно, $l = k(\bar{x}z)$. Утверждается, что $z = \bar{y}$ для подходящего $y \in L^{(1)}$. Действительно, согласно теореме 90 Гильберта, $z = \varphi(s)/s$ для подходящего $s \in l^*$. Тогда если $u \in U_L$ обладает свойством $\bar{u} = s$, то элемент $y = \varphi(u)/u$ является искомым. Далее, заметим, что расширение $P = K(xy)$ является максимальным неразветвленным подполем в D, ибо

$$n \geqslant [P : K] \geqslant [k(\overline{xy}) : k] = [l : k] = n,$$

откуда $[P : K] = [k(\overline{xy}) : k] = n$, что и требовалось. Таким образом, $P \simeq L$ над K, и, следовательно, по теореме Сколема —

Нётер $P = sLs^{-1}$ для подходящего $s \in D^*$. Учитывая, что $N_{L/K}(L^*) = UK^{*n}$ (предложение 2) и тот факт, что для элемента g в (2) выполняется условие $v(\mathrm{Nrd}_{D/K}(g), n) = 1$ (см. п. 2), мы видим, что для подходящих $i \in \mathbb{Z}$, $c \in L$ выполняется равенство $\mathrm{Nrd}_{D/K}(s) = \mathrm{Nrd}_{D/K}(g^i c)$. Полагая $t = s(g^i c)^{-1}$, будем иметь $P = tg^i cLc^{-1}g^{-i}t^{-1} = tLt^{-1}$ и $\mathrm{Nrd}_{D/K}(t) = 1$. Окончательно, $x \in P^{(1)}y^{-1} \subset t^{-1}L^{(1)}tL^{(1)}$ и доказательство теоремы 8 завершено.

Заметим, что из доказательства теоремы 8 вытекает, что любой элемент из $D^{(1)}$ является произведением не более двух коммутаторов. Неизвестно, можно ли понизить эту оценку до одного коммутатора.

4. Фильтрации в D^* и $D^{(1)}$ (см. Рим [1]). Материал этого пункта не будет использоваться нигде, кроме § 9.5, поэтому его можно опустить при первом чтении.

Пусть по-прежнему D — тело индекса n над локальным полем K. Сохраним обозначения, введенные в п. 2,3. Положим также $U_i = 1 + \mathfrak{P}_D^i$, $C_i = U_i \cap D^{(1)}$ $(i \geqslant 1)$, считая, что $U_0 = U_D = \mathcal{O}_D^*$ и $C_0 = D^{(1)}$. Из формулы (1) вытекает, что группы U_i и C_i являются нормальными в D^* (они называются *конгруэнц-подгруппами* уровня $\mathfrak{P}_D^i$, или просто уровня i, соответственно в D и $D^{(1)}$). Так как группы U_D и $D^{(1)}$, очевидно, компактны, а группы U_i и C_i открыты в U_D и $D^{(1)}$ соответственно (более того, образуют базу окрестностей единицы), то индексы $[U : U_i]$ и $[D^{(1)} : C_i]$ конечны. Определим структуру последовательных факторов U_i/U_{i+1} и C_i/C_{i+1}.

Предложение 8. *Существуют естественные изоморфизмы*

$$\rho_0\colon U_0/U_1 \to l^*,$$

$$\rho_i\colon U_i/U_{i+1} \to l^+,\ i \geqslant 1 \ (\textit{аддитивная группа поля } l).$$

При этом $\rho_0(C_0) = l^{(1)} = \{x \in l^* \mid N_{l/k}(x) = 1\}$, *а* $\rho_i(C_i) = l$, *если* $i \not\equiv 0 \pmod n$ *и* $\rho_i(C_i) = l^{(0)} = \{x \in l \mid \mathrm{Tr}_{l/k}(x) = 0\}$, *если* $i \equiv 0 \pmod n$.

Доказательство. Как и выше, для элемента $a \in \mathcal{O}_D$ будем обозначать через $\bar{a}$ его образ в $l = \mathcal{O}_D/\mathfrak{P}_D$. Тогда ρ_0 индуцируется отображением $a \mapsto \bar{a}$, а $\rho_i (i \geqslant 1)$ — отображением $1 + a\Pi^i \mapsto \bar{a}$ (заметим, что ρ_i зависит от выбора униформизующего элемента Π). Образ $\rho_0(C_0)$ мы уже вычислили при доказательстве теоремы 8. Для вычисления $\rho_i(C_i)$ $(i \geqslant 1)$ нам понадобится

Лемма 7. $\mathrm{Nrd}_{D/K}(1 + \mathfrak{P}_D^i) = 1 + \mathfrak{p}^j$, *где* j — *минимальное целое число* $\geqslant i/n$.

Доказательство легко получается из предложения 3.

Пусть теперь $x \in l$ и $a \in \mathcal{O}_D$ — такой элемент, что $\bar{a} = x$. Рассмотрим $z = 1 + a\Pi^i$. Тогда $t = \mathrm{Nrd}_{D/K}(z) \in 1 + \mathfrak{p}^j$, где j —

минимальное целое $\geqslant i/n$. Если $i \not\equiv 0 \pmod n$, то $j \geqslant (i+1)/n$, и по лемме 7 найдется $y \in U_{j-1}$ со свойством $\mathrm{Nrd}_{D/K}(y) = t$. Полагая $z_1 = zy^{-1}$, получим, что $\mathrm{Nrd}_{D/K}(z_1) = 1$, т. е. $z_1 \in C_i$, и $\rho_i(z_1) = x$. Таким образом, $\rho_i(C_i) = l$ при $i \not\equiv 0 \pmod n$. Пусть теперь $i = jn$. Поскольку $\mathcal{O}_D = \mathcal{O}_L + \mathfrak{P}_D$, то $\mathfrak{P}_D^i = \mathcal{O}_L \pi^j + \mathfrak{P}_D \pi^j = \mathfrak{P}_L^j + \mathfrak{P}_D^{j+1}$ (где $\mathcal{O}_L$, $\mathfrak{P}_L$ — соответственно кольцо целых и идеал нормирования в L; отметим, что $\mathfrak{P}_L = \mathcal{O}_L \pi$ для униформизующего элемента $\pi \in K$, ибо L/K неразветвлено). Отсюда следует, что $U_i = (U_i \cap L^*) U_{i+1}$ и $U_i \cap L^* = 1 + \mathfrak{P}_L^j$. Поэтому если $z \in U_i$ и $z = st$, где $s \in U_i \cap L^*$, $t \in U_{i+1}$, то $N_{L/K}(s) = \mathrm{Nrd}_{D/K}(t)^{-1} \in 1 + \mathfrak{P}^{i+1}$. С другой стороны, если $s = 1 + r\pi^j$, $r \in \mathcal{O}_L$, то

$$N_{L/K}(s) = \prod_{m=0}^{n-1} \varphi^m (1 + r\pi^j) \equiv 1 + \mathrm{Tr}_{L/K}(r)\, \pi^j \pmod{\mathfrak{p}^{j+1}}.$$

Таким образом, $\mathrm{Tr}_{L/K}(r) \equiv 0 \pmod{\mathfrak{p}}$, откуда $\mathrm{Tr}_{l/k}(\bar{r}) = 0$ и $\rho_i(C_i) \subset l^{(0)}$. Обратно, если $\mathrm{Tr}_{L/K}(r) \equiv 0 \pmod{\mathfrak{p}}$, то для $s = 1 + r\pi^j$ имеем $N_{L/K}(s) \in 1 + \mathfrak{p}^{j+1}$, так что найдется $t \in 1 + \mathfrak{P}_L^{j+1}$ со свойством $N_{L/K}(s) = N_{L/K}(t)$ и элемент $z = st^{-1} \in L^{(1)} \cap (1 + \mathfrak{P}_L^j)$ обладает свойством $\rho_i(z) = r$. Предложение доказано.

Следствие. *Для любого $i \geqslant 0$ факторы U_0/U_i и C_0/C_i являются конечными разрешимыми группами. Следовательно, группы U_0 и C_0 проразрешимы.*

Действительно, разрешимость факторгрупп U_0/U_i и C_0/C_i непосредственно вытекает из предложения. Как мы отмечали выше, группы U_i и C_i образуют базу окрестностей единицы в группах U_0 и C_0 соответственно, поэтому $U_0 = \varprojlim U_0/U_i$, $C_0 = \varprojlim C_0/C_i$ — проразрешимые группы (см. § 3.3).

Теперь, следуя Риму [1], определим взаимные коммутанты $[C_0, C_i]$ и $[C_1, C_i]$ $(i \geqslant 1)$. Для этого нам понадобится одно вычисление.

Лемма 8. *Пусть $x = 1 + a\Pi^i$, $y = 1 + b\Pi^j$, где $a, b \in \mathcal{O}_D$, $i, j \geqslant 1$. Тогда коммутатор $[x, y] = xyx^{-1}y^{-1}$ имеет вид $1 + c\Pi^{i+j}$, где $\bar{c} = \bar{a}\sigma^i(\bar{b}) - \sigma^j(\bar{a})\bar{b}$ (здесь σ, как и п. 2, автоморфизм l над k, задаваемый соответствием $\bar{d} \to \overline{\Pi d \Pi^{-1}}$). В частности, $[U_i, U_j] \subset U_{i+j}$.*

Доказательство. Положим $(s, t) = st - ts$. Тогда легко проверяется, что $[x, y] = 1 + (x-1, y-1)x^{-1}y^{-1}$, откуда $[x, y] = 1 + (a\Pi^i b\Pi^j - b\Pi^j a\Pi^i)x^{-1}y^{-1} = 1 + c\Pi^{i+j}$, где $c = (a\Pi^i b\Pi^{-i} - b\Pi^j a\Pi^{-j})(\Pi^{i+j}x^{-1}y^{-1}\Pi^{-(i+j)})$. Переходя к вычетам и учитывая, что $\bar{x} = \bar{y} = 1$, получим требуемое.

Теорема 9. *Пусть $n > 2$. Тогда*

1) $[C_1, C_i] = C_{i+1}$ *для любого* $i \geqslant 1$;

2) $[C_0, C_i] = \begin{cases} C_i, & \text{если } i \not\equiv 0 \pmod n, \\ C_{i+1}, & \text{если } i \equiv 0 \pmod n. \end{cases}$

В частности, $[C_0, C_0] = C_1$.

Доказательство. Покажем вначале, что $\rho_{i+1}([C_1, C_i]) = \rho_{i+1}(C_{i+1})$. Из леммы 8 и предложения 8 вытекает, что образ $\rho_i([C_1, C_i])$ порождается как абелева группа элементами вида $\alpha\sigma(\beta) - \sigma^i(\alpha)\beta$, где $\alpha \in l$, $\beta \in l$ или $l^{(0)}$ в зависимости от того, делится i на n или нет. Мы оставляем читателю в качестве упражнения показать, что эти элементы порождают соответственно l или $l^{(0)}$, т. е. $\rho_{i+1}(C_{i+1})$. Итак, для любого i

$$[C_1, C_i] C_{i+2} = C_{i+1}. \tag{4}$$

Покажем теперь, что на самом деле $[C_1, C_i] = C_{i+1}$. Воспользуемся устанавливаемым в гл. III фактом (см. теорему 3 гл. III), из которого, в частности вытекает, что любой нецентральный нормальный делитель в $D^{(1)}$ является открытым (излишне говорить, что доказательство теоремы 3 гл. III не использует самой теоремы 9). Тогда для подходящего j имеем $[C_1, C_i] \supset C_j$, причем можно предполагать, что j — минимальное число с таким свойством. Предположим, что $j > i + 1$, тогда $j - 2 \geqslant i$, так что в силу (4) получаем

$$[C_1, C_i] \supset [C_1, C_{j-2}] C_j = C_{j-1},$$

что противоречит определению j. Итак, $j = i + 1$ и утверждение 1) доказано. (Отметим, что Рим [1] устанавливает справедливость равенства $[C_1, C_i] = C_{i+1}$ непосредственно.)

Из 1) вытекает, что $[C_0, C_i] \supset [C_1, C_i] = C_{i+1}$, так что для доказательства 2) достаточно показать, что

$$\rho_i([C_0, C_i]) = \begin{cases} l, & \text{если } i \not\equiv 0 \pmod n, \\ 0, & \text{если } i \equiv 0 \pmod n. \end{cases} \tag{5}$$

Прямое вычисление показывает, что для $x \in U_D$, $i \geqslant 1$, $y = 1 + a\Pi^i$ имеем $\rho_i([x, y]) = (\bar{x}\sigma^i(\bar{x})^{-1} - 1)\bar{a}$. Если $i \equiv 0 \pmod n$, то отсюда непосредственно получаем, что $\rho_i([x, y]) = 0$. Если же $i \not\equiv 0 \pmod n$, то из свойств конечных полей легко установить существование такого $\alpha \in l^{(1)}$, что $\sigma^i(\alpha) \neq \alpha$. Тогда, беря в качестве x такой элемент из $D^{(1)}$, что $\bar{x} = \alpha$, мы получим первое утверждение в (5). Для завершения доказательства теоремы 9 остается заметить, что всегда $[C_0, C_0] \subset C_1 = [C_0, C_1]$, следовательно, $[C_0, C_0] = C_1$.

Замечание. Некоторое уточнение приведенных выше рассуждений позволяет рассмотреть и случай $n = 2$. Результаты здесь выглядят следующим образом (см. Рим [1]):

если $p = \operatorname{char} k \neq 2$, то остаются в силе утверждения теоремы 9; в случае $n = p = 2$ аналог утверждения 1) принимает

вид

$$[C_1, C_{2i+1}] = C_{2i+2}, \quad \text{если либо } [k] > 2, \text{ либо } i \geqslant 1;$$
$$[C_1, C_{2i}] = C_{2(i+1)} \text{ для всех } i.$$

Если $[k] = 2$, то $[C_1, C_1]$ содержит C_4, но не содержит C_3. Утверждение 2) теоремы 9, в частности, равенство $[C_0, C_0] = C_1$ выполняется всегда.

Следствие. $C_0 = L^{(1)}[C_0, C_0]$, *где* L — *максимальное неразветвленное подполе в* D.

При $n > 2$ (соответственно, $n = 2$) это вытекает из теоремы 9 и предложения 8 (соответственно, из сделанного замечания и предложения 8). Другое доказательство, не различающее случаи $n > 2$ и $n = 2$, моментально получается из теоремы 8.

В § 9.5 нам понадобится знание структуры группы $F(i) = C_i/C_{i+1}$ $(i \geqslant 1)$ как модуля над группой $\Delta = C_0/C_1$, которая определяется действием группы C_0 сопряжениями (отметим, что в силу леммы 6 группа C_1 действует на $F(i)$ тривиально). Используя отображения ρ_0 и ρ_i из предложения 8, отождествим Δ и $F(i)$ соответственно с $l^{(1)}$ и $l^{(0)}$ в зависимости от того, делится i на n или нет. Тогда простое вычисление показывает, что структура Δ-модуля на $F(i)$ определяется формулой

$$\delta \cdot x = \delta\sigma^i(\delta)^{-1}x, \quad \delta \in \Delta, \quad x \in F(i) \tag{6}$$

(справа в (6) стоит произведение в l).

Предложение 9. *Если* $i \not\equiv 0 \pmod n$, *то* $F(i)$ *является простым* Δ-*модулем, за исключением случая, когда расширение* l/k *есть* F_9/F_3, *либо* F_{64}/F_4 (F_q — *конечное поле из* q *элементов*). *В последнем случае* Δ-*подмодули в* $F(i) \simeq F_{64}$ *соответствуют векторным подпространствам в* F_{64} *над полем* F_8.

Доказательство. Обозначим через m подполе в l, порожденное над простым подполем элементами вида $\delta(\sigma^i(\delta))^{-1}$, $\delta \in l^{(1)}$. Тогда наше утверждение, очевидно, эквивалентно тому, что $m = l$, если l/k отлично от F_9/F_3, F_{64}/F_4, и $m = F_8$, если l/k есть F_{64}/F_4. Доказательство этих фактов элементарно, и мы оставляем его читателю.

Используя предложение 9, Рим получает полное описание нормальных подгрупп в C_0. Так как в дальнейшем эти результаты нам не понадобятся, мы приведем только формулировку основной теоремы без разбора возникающих здесь исключительных случаев. Для этого положим $E_r = (K^* \cap C_0)C_r$ и будем говорить, что нормальный делитель $N \subset C_0$ имеет *уровень* r, если $N \subset E_r$, но $N \not\subset E_{r+1}$. Поскольку $\bigcap_r E_r = K^* \cap C_0$, то любой нецентральный нормальный делитель в C_0 обладает некоторым уровнем.

Теорема 10. *Предположим, что D не является алгеброй кватернионов над конечным расширением поля $\mathbb{Q}_2$. Тогда если $N \subset C_0$ — нормальный делитель уровня r, то*

$$C_{r+1} \subset N \subset E_r.$$

Если $n \not\mid r$ и Δ-модуль $F(r)$ прост, то выполняется более сильное условие $C_r \subset N \subset E_r$.

Отметим, что включение $C_r \subset N \subset E_r$ означает, что N может отличаться от конгруэнц-подгруппы лишь на центральную подгруппу, и тем самым мы имеем неулучшаемое описание нормальных подгрупп.

Мы используем предложение 9 для других целей. А именно, с его помощью мы опишем модуль $B = B(F(1), F(r))$ билинейных Δ-инвариантных отображений b: $F(1) \times F(r) \to F_p = \mathbb{Z}/p\mathbb{Z}$, где $p = \operatorname{char} k$ и Δ действует на F_p тривиально.

Теорема 11 (Прасад, Рагунатан [4]). 1) *Если $r \not\equiv -1 \pmod n$, то $B = 0$; 2) если $r \equiv -1 \pmod n$, $n > 2$, то B состоит в точности из всех отображений вида*

$$b(\lambda)(x, y) = \operatorname{Tr}_{l/F_p}(\lambda x \sigma(y)), \tag{7}$$

где $\lambda \in l$ в случае, если расширение l/k отлично от F_{64}/F_4, и из отображений вида

$$b(\lambda, \mu)(x, y) = \operatorname{Tr}_{l/F_p}(\lambda x \sigma(y) + \mu x \sigma(y)^8), \tag{8}$$

где $\lambda, \mu \in l$, в противном случае.

(Отметим, что появление оператора следа в формулах (7), (8) не случайно, ибо для любого конечного сепарабельного расширения полей P/M формула $f(x, y) = \operatorname{Tr}_{P/M}(xy)$ определяет невырожденное M-линейное спаривание P с самим собой, так что любой M-линейный функционал φ: $P \to M$ имеет вид $\varphi(x) = \operatorname{Tr}_{P/M}(ax)$ для подходящего $a \in P$.)

Доказательство. Пусть $r, s > 0$ и $s + r \equiv 0 \pmod n$. Тогда для любого $\lambda \in l$ билинейное отображение $F(r) \times F(s) \to F_p$, определяемое формулой

$$b_r(\lambda)(x, y) = \operatorname{Tr}_{l/F_p}(\lambda x \sigma^r(y)), \tag{9}$$

является Δ-инвариантным. В самом деле, для любого $\delta \in \Delta$ в силу формулы (6) имеем

$$b_r(\lambda)(\delta \cdot x, \delta \cdot y) = \operatorname{Tr}_{l/F_p}\left(\lambda\left(\delta\sigma^r(\delta)^{-1}\right) x \sigma^r\left(\delta\sigma^s(\delta)^{-1} y\right)\right) =$$

$$= \operatorname{Tr}_{l/F_p}\left(\lambda\left(\delta\sigma^{r+s}(\delta)^{-1}\right) x \sigma^r(y)\right) = b_r(\lambda)(x, y),$$

ибо $r + s \equiv 0 \pmod n$. Если при этом $r \not\equiv 0 \pmod n$, то $F(r) \simeq l$ и $F(s) \simeq l$, откуда следует, что $b_r(1)$ задает невырожденное спаривание $F(r) \times F(s) \to F_p$, т. е. определяет изоморфизм $F(r)$

с двойственным модулем $\widehat{F(s)} = \mathrm{Hom}(F(s), F_p)$. Если же $r \equiv s \pmod n$, то $F(r)$ и $F(s)$ одновременно являются тривиальными Δ-модулями, и поэтому здесь также $F(r) \simeq F(s)$. Поскольку, очевидно, $B(F(r), F(s)) = \mathrm{Hom}_\Delta(F(r), \widehat{F(s)})$, то для доказательства первого утверждения теоремы достаточно установить, что $\mathrm{Hom}_\Delta(F(r), F(s)) = 0$, если $r \not\equiv s \pmod n$.

Пусть $\varphi \in \mathrm{Hom}_\Delta(F(r), F(s))$, $\varphi \not\equiv 0$. Тогда для любого $a \in F(r)$ и любого $\delta \in \Delta$ имеем

$$\varphi\left(\delta\left(\sigma^r(\delta)\right)^{-1} a\right) = \delta\left(\sigma^s(\delta)\right)^{-1} \varphi(a). \tag{10}$$

Обозначим через $\mathscr{F}_1$ и $\mathscr{F}_2$ аддитивные подгруппы в l, порожденные элементами вида $\delta(\sigma^r(\delta))^{-1}$ и $\delta(\sigma^s(\delta))^{-1}$ соответственно. Выбирая $a \in F(r)$ таким образом, чтобы $\varphi(a) \neq 0$, из (10) получим, что если $\delta_i \in \Delta$ и $\sum \delta_i (\sigma^r(\delta_i))^{-1} = 0$, то $\sum \delta_i (\sigma^s(\delta_i))^{-1} = 0$ и тем самым отображение ψ: $\delta(\sigma^r(\delta))^{-1} \mapsto \delta(\sigma^s(\delta))^{-1}$ продолжается до аддитивного гомоморфизма $\mathscr{F}_1$ на $\mathscr{F}_2$. Более того, $\mathscr{F}_1$ и $\mathscr{F}_2$, очевидно, замкнуты относительно умножения, т. е. являются конечными полями, причем продолжение ψ является на самом деле изоморфизмом полей $\mathscr{F}_1$ и $\mathscr{F}_2$. Отсюда следует, что $\psi(x) = x^{p^l}$ для подходящего целого l. Таким образом,

$$\left(\delta\left(\sigma^r(\delta)\right)^{-1}\right)^{p^l} = \delta\left(\sigma^s(\delta)\right)^{-1} \tag{11}$$

для любого $\delta \in \Delta$. Пусть $k = F_{p^a}$. Тогда $\Delta = \{x^{p^a-1} \mid x \in l^*\}$ и $\sigma(x) = x^{p^{ab}}$ для подходящего целого b, так что из (11) получаем, что

$$x^{-p^l(p^{abr}-1)(p^a-1)} = x^{-(p^{abs}-1)}$$

для всех $x \in l^*$, откуда $p^l(p^{abr}-1)(p^a-1) \equiv p^{abs}-1 \pmod{p^{an}-1}$. Но из последнего сравнения вытекает (см. Прасад, Рагунатан [2], добавление к § 7), что $br \equiv bs \pmod n$, и, значит, $r \equiv s \pmod n$, ибо $(b, n) = 1$, и первое утверждение теоремы доказано.

При доказательстве второго утверждения предположим вначале, что расширение l/k отлично от расширения F_{64}/F_4, т. е. $F(r)$ является простым Δ-модулем. Пусть $b = b(x, y) \in B$. Тогда отображение $x \mapsto b(x, 1)$ является F_p-линейным отображением l в F_p, и поэтому $b(x, 1) = \mathrm{Tr}_{l/F_p}(\lambda x)$ для подходящего $\lambda \in l$. Рассмотрим разность $b_0 = b - b_1(\lambda)$, где $b_1(\lambda)$ определяется формулой (9). В силу инвариантности b и $b_1(\lambda)$ для любого $x \in F(1)$ множество $x^\perp = \{y \in F(r) \mid b_0(x, y) = 0\}$ является Δ-инвариантным содержащим 1 подмодулем в $F(r)$, откуда $x^\perp = F(r)$ и $b_0 = 0$, т. е. $b = b_1(\lambda)$, что и требовалось.

Нам осталось рассмотреть случай $l = F_{64}$, $k = F_4$. Здесь неприводимые A-подмодули в $F(r)$ отвечают векторным подпро-

странствам в l над полем F_8, причем единственный нетривиальный автоморфизм F_{64}/F_8 имеет вид $x \mapsto x^8$. Пусть $z \in l/F_8$. Тогда, рассуждая как и выше, установим существование таких $\theta, \omega \in l$, что

$$b(x, 1) = \mathrm{Tr}_{l/F_p}(\theta x),$$

$$b(x, z) = \mathrm{Tr}_{l/F_p}(\omega x)$$

для всех $x \in l$. Так как $z^8 \neq z$, то найдутся $\lambda, \mu \in l$, удовлетворяющие системе

$$\lambda + \mu = \theta,$$

$$\lambda\sigma(z) + \mu\sigma(z)^8 = \omega.$$

Поскольку в нашей ситуации $\delta(\sigma^r(\delta))^{-1} \in F_8$ для всех $\delta \in l^{(1)}$, то билинейное отображение $b(\lambda, \mu)$ (см. (8)) является Δ-инвариантным. Тогда отображение $b_0 = b - b(\lambda, \mu)$ также Δ-инвариантно. Отсюда следует, что для любого $x \in F(1)$ пространство $x^\perp$ является Δ-подмодулем в $F(r)$, содержащим $1, z$, и поэтому $x^\perp = F(r)$. Таким образом, $b_0 = 0$ и $b = b(\lambda, \mu)$. Теорема 11 доказана.

§ 1.5. Простые алгебры над полями алгебраических чисел

1. Группа Брауэра. Пусть A — простая центральная алгебра над полем алгебраических чисел K. Тогда для любого $v \in V^K$ алгебра $A_v = A \otimes_K K_v$ также является простой, и отображение $[A] \to [A_v]$ в обозначениях п. 1 § 1.4 определяет гомоморфизм групп Брауэра $\mathrm{Br}(K) \xrightarrow{\theta_v} \mathrm{Br}(K_v)$. Чтобы получить описание группы $\mathrm{Br}(K)$, следует рассмотреть произведение

$$\theta = \prod_{v \in V^K} \theta_v : \mathrm{Br}(K) \to \prod_{v \in V^K} \mathrm{Br}(K_v).$$

В п. 2 § 1.4 мы видели, что для $v \in V_f^K$ имеет место изоморфизм inv_{K_v}: $\mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$. Чтобы унифицированно рассматривать все нормирования, условимся считать инвариантом тела кватернионов над $K_v = \mathbb{R}$ класс в $\mathbb{Q}/\mathbb{Z}$, содержащий $1/2$. Тогда отображение inv_{K_v}: $\mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$ определено для всех v и является вложением.

Теорема 12 (Хассе, Брауэр, Нётер). *Отображение θ инъективно, и его образ состоит из таких $a = (a_v) \in \prod_v \mathrm{Br}(K_v)$, что $a_v = 0$ для почти всех v и $\sum_v \mathrm{inv}_{K_v}(a_v) = 0$.*

Таким образом, любая конечномерная центральная алгебра с делением D над K с точностью до изоморфизма определяется заданием инвариантов $\mathrm{inv}_{K_v}[D_v]$ алгебр $D_v = D \otimes_K K_v$, которые мы будем для краткости обозначать через $\mathrm{inv}_v D$. Обратно,

для любого набора инвариантов, почти все из которых равны нулю и сумма которых также равна нулю, найдется алгебра с делением над K, имеющая данные инварианты.

Из инъективности θ вытекает ряд следствий. Прежде всего из п. 1 § 1.4 получаем, что расширение P поля K степени n, равной индексу тела D, изоморфно максимальному подполю в D в том и только том случае, если $D_v \otimes_{K_v} P_w$ есть матричная алгебра для всех $v \in V^K$ и всех $w|v$ (последнее условие равносильно тому, что для всех $v \in V^K$ и всех $w|v$ локальные степени $[P_w : K_v]$ делятся на индекс алгебры D_v). Тогда, применяя теорему Грюнвальда — Ванга из теории полей классов (см., например, Артин, Тэйт [1]), получаем, что D содержит максимальное подполе $L \subset D$, являющееся циклическим расширением K. Учитывая структуру тел над локальными полями, естественно задать более тонкий вопрос: всегда ли существует максимальное подполе $L \subset D$, являющееся циклическим расширением поля K и такое, что все расширения L_v/K_v неразветвлены для тех $v \in V_f^K$, что алгебра D_v является телом? К сожалению, это не всегда так (контрпримеры существуют уже над полем $\mathbb{Q}$), однако выполнение этого условия можно обеспечить, наложив на тело D некоторые ограничения, что использовалось в работе Платонова, Рапинчука [4]. Применение теоремы Грюнвальда — Ванга в сочетании с теоремой 12 позволяет установить, что над полями алгебраических чисел, как и над локальными полями, экспонента простой алгебры совпадает с ее индексом, и, в частности, тела экспоненты 2 исчерпываются телами (обобщенных) кватернионов.

2. Мультипликативная структура. Пусть D — центральное тело индекса n над полем алгебраических чисел K. Мы опишем образ приведенной нормы $\mathrm{Nrd}_{D/K}(D^*)$ и покажем, что группа $SL_1(D)$ совпадает с коммутантом $[D^*, D^*]$ мультипликативной группы D^*.

Теорема 13 (Эйхлер). *Группа* $\mathrm{Nrd}_{D/K}(D^*)$ *совпадает со множеством тех элементов из* K^*, *которые положительны по всем вещественным нормированиям* $v \in V_\infty^K$ *таким, что* $D_v \not\simeq M_n(K_v)$.

Доказательство — см. Вейль [7], с. 279—284 (см. также § 6.7).

Теорема 14 (Ванг). *Группа* $SL_1(D)$ *совпадает с коммутантом* $[D^*, D^*]$.

Оригинальное доказательство Ванга [1] этой теоремы является весьма сложным и использует глубокие результаты теории чисел. Мы изложим модифицированное рассуждение (см. Платонов [15], Янчевский [1]), которое основывается исключительно на теореме Эйхлера.

Сначала получим редукцию доказательства теоремы 14 к телам примарного индекса. Нам понадобятся некоторые сведения

об определителе Дьедонне (см. Артин [1], Дьедонне [2]). Пусть $GL_m(D)$ — группа обратимых элементов матричной алгебры $A = M_m(D)$. Тогда существует сюръективный гомоморфизм $GL_m(D) \xrightarrow{\delta} D^*/[D^*, D^*]$, называемый *определителем Дьедонне*, ядро которого содержит коммутант $[GL_m(D), GL_m(D)]$, причем $\delta\left(\begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_m \end{pmatrix}\right) = a_1 \ldots a_m [D^*, D^*]$. Известно также, что во всех случаях, кроме одного исключительного: $m = 2$, $D = F_2$ — поле из двух элементов, $\operatorname{Ker} \delta$ совпадает с $[GL_m(D), GL_m(D)]$. В частности, δ индуцирует изоморфизм $SK_1(A) \simeq SK_1(D)$, и поэтому для любого поля P, отличного от F_2 при $m = 2$, группа $SL_m(P)$ совпадает с коммутантом $GL_m(P)$.

Лемма 9. *Пусть $a \in SL_1(D)$ и $a \in [(D \otimes_K B)^*, (D \otimes_K B)^*]$, где B — ассоциативная K-алгебра с единицей размерности m над K. Тогда $a^m \in [D^*, D^*]$.*

Доказательство. Регулярное представление $B \hookrightarrow M_m(K)$ является точным и индуцирует вложение $D \otimes B \to M_m(D)$. При этом элементу $a \in D$ отвечает матрица $\begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix}$. Если теперь $a \in SL_1(D)$ и $a \in [(D \otimes_K B)^*, (D \otimes_K B)^*]$, то, очевидно, $\begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix} \in [GL_m(D), GL_m(D)]$, так что, вычисляя определитель Дьедонне, получим $a^m \in [D^*, D^*]$, что и требовалось.

Из леммы 9 получаем

Следствие 1. *Группа $SK_1(D)$ тела D индекса n является группой экспоненты n.*

Действительно, если $L \subset D$ — некоторое максимальное подполе, то $[L : K] = n$ и $D \otimes_K L = M_n(L)$. Поэтому, применяя лемму 9 к $B = L$ и учитывая тот факт, что $SL_n(L) = [GL_n(L), GL_n(L)]$, получаем наше утверждение.

Далее, известно, что если $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, то $D = D_1 \otimes_K \ldots \otimes_K D_r$, где D_i — тело индекса $p_i^{\alpha_i}$. В этих обозначениях имеет место

Следствие 2. *Если $SK_1(D_i) = 1$ для всех $i = 1, \ldots, r$, то $SK_1(D) = 1$.*

Для доказательства обозначим через B_i тензорное произведение $\bigotimes_{j \neq i} D_j^0$ соответствующих противоположных алгебр. Тогда B_i

является K-алгеброй размерности n_i^2, где $n_i = n/p_i^{\alpha_i}$, причем $D \otimes_K B_i \simeq M_{n_i^2}(D_i)$ для всех $i = 1, \ldots, r$. Из свойств определителя Дьедонне и равенства $SK_1(D_i) = 1$ вытекает, что $SL_{n_i^2}(D_i) = \left[GL_{n_i^2}(D_i), GL_{n_i^2}(D_i)\right]$, так что для любого $a \in SL_1(D)$ в силу леммы 9 имеем включение $a^{n_i^2} \in [D^*, D^*]$. Но все числа n_i^2 взаимно просты в совокупности, поэтому $u_1 n_1^2 + \ldots + u_r n_r^2 = 1$ для подходящих целых u_i, откуда $a = \left(a^{n_1^2}\right)^{u_1} \ldots \left(a^{n_r^2}\right)^{u_r} \in [D^*, D^*]$, что и требовалось.

Итак, достаточно доказать теорему 14 для тела D индекса p^α, где p — некоторое простое число, $\alpha \geqslant 0$. Доказательство будем вести индукцией по α, заметив, что в начальном случае $\alpha = 0$ требуемое утверждение, очевидно, выполняется. Итак, предположим, что для произвольного тела Δ индекса $p^{\alpha-1}$ над некоторым полем алгебраических чисел имеем $SK_1(\Delta) = 1$, и покажем, что тогда для тела D индекса p^α также $SK_1(D) = 1$. Пусть $a \in SL_1(D)$. Нам достаточно найти такое расширение F/K степени, взаимно простой с p, что $a \in [(D \otimes_K F)^*, (D \otimes_K F)^*]$, ибо в этом случае $a^{[F:K]} \in [D^*, D^*]$ согласно лемме 9 и одновременно $a^{p^\alpha} \in [D^*, D^*]$ в силу следствия 1. Тогда поскольку p и $[F:K]$ взаимно просты, существуют $s, t \in \mathbb{Z}$ со свойством $s[F:K] + tp^\alpha = 1$, и, следовательно, $a = (a^{[F:K]})^s \left(a^{p^\alpha}\right)^t \in [D^*, D^*]$, что и требовалось. Для построения F рассмотрим максимальное подполе $L \subset D$, содержащее a. Пусть P — нормальное замыкание поля L над K и $\mathscr{G} = \mathrm{Gal}(P/K)$ — соответствующая группа Галуа. Рассмотрим силовскую p-подгруппу $\mathscr{G}_p \subset \mathscr{G}$ и возьмем в качестве F отвечающее ей неподвижное поле $F = P^{\mathscr{G}_p}$. Тогда, очевидно, степень $[F:K]$ взаимно проста с p. Покажем, что $a \in [(D \otimes_K F)^*, (D \otimes_K F)^*]$.

Группа Галуа $\mathrm{Gal}(P/F)$ есть $\mathscr{G}_p$, и пусть $\mathscr{H} \subset \mathscr{G}_p$ — подгруппа, отвечающая подполю $LF \subset P$. Из свойств p-групп вытекает существование нормальной подгруппы $\mathscr{N} \subset \mathscr{G}_p$ индекса p, содержащей $\mathscr{H}$. Тогда соответствующее неподвижное поле $M = P^{\mathscr{N}}$ является циклическим расширением поля F степени p, содержащимся в LF. Если $\alpha = 1$, то $M = LF$ — циклическое расширение F степени p. Тогда поскольку $a \in SL_1(D)$, имеем $N_{M/F}(a) = 1$, так что по теореме 90 Гильберта $a = \sigma(b)/b$ для подходящего $b \in LF$, где σ — образующая группы Галуа $\mathrm{Gal}(M/F)$. Но в силу теоремы Сколема — Нётер найдется такой элемент $g \in (D \otimes_K F)^*$, что $\sigma(b) = gbg^{-1}$ (мы отождествляем LF с $L \otimes_K F \subset D \otimes_K F$), и тогда $a = gbg^{-1}b^{-1} \in [(D \otimes_K F)^*, (D \otimes_K F)^*]$, что и требовалось. (Заметим, что мы пока не использовали предположение о том, что K — поле ал-

гебраических чисел, и, таким образом, $SK_1(D)=1$ для тела D индекса p над произвольным полем K.) В случае $\alpha>1$ обозначим через Δ централизатор M в $D\otimes_K F$. Тогда Δ является телом индекса $p^{\alpha-1}$ с центром M (теорема о двойном централизаторе, см. Пирс [1]). Очевидно, $a\in\Delta$, причем

$$1=\mathrm{Nrd}_{(D\otimes_K F)/F}(a)=N_{LF/F}(a)=$$
$$=N_{M/F}(N_{LF/M}(a))=N_{M/F}(\mathrm{Nrd}_{\Delta/M}(a)).$$

Поэтому $t=\mathrm{Nrd}_{\Delta/M}(a)$ имеет вид

$$t=\sigma(s)/s \tag{1}$$

для некоторого $s\in M$, где σ — образующая $\mathrm{Gal}(M/F)$. По теореме Сколема — Нётер найдется $g\in(D\otimes_K F)^*$ со свойством $\sigma(b)=gbg^{-1}$ для всех $b\in M$. Тогда автоматически $g\Delta g^{-1}=\Delta$, ибо Δ — централизатор M и $\mathrm{Nrd}_{\Delta/M}(gxg^{-1})=g\,\mathrm{Nrd}_{\Delta/M}(x)\,g^{-1}$ для любого $x\in\Delta$. Предположим теперь, что нам удалось выбрать элемент s в (1) из образа приведенной нормы $\mathrm{Nrd}_{\Delta/M}(\Delta^*)$ (элемент s в (1) определен с точностью до элемента из F^*). Тогда если $s=\mathrm{Nrd}_{\Delta/M}(z)$, где $z\in\Delta$, то $\mathrm{Nrd}_{\Delta/M}(gzg^{-1}z^{-1})=$ $=\sigma(s)/s=\mathrm{Nrd}_{\Delta/M}(a)$, так что $a'=a(gzg^{-1}z^{-1})^{-1}\in SL_1(\Delta)$. По предположению индукции $SL_1(\Delta)=[\Delta^*,\Delta^*]\subset([D\otimes_K F)^*,$ $(D\otimes_K F)^*]$, откуда $a\in[(D\otimes_K F)^*,\ (D\otimes_K F)^*]$, и теорема доказана.

Итак, осталось показать, что элемент s в (1) можно всегда выбрать из $\mathrm{Nrd}_{\Delta/M}(\Delta^*)$. Для этого воспользуемся теоремой 13. Тогда, если p нечетно, то $\Delta_w=\Delta\otimes_M M_w$ является полной матричной алгеброй для всех $w\in V_\infty^M$, следовательно, $\mathrm{Nrd}_{\Delta/M}(\Delta^*)=$ $=M^*$ и доказывать нечего. Пусть теперь $p=2$. В этом случае M является квадратичным расширением F и $\mathrm{Nrd}_{\Delta/M}(\Delta^*)$ совпадает с подгруппой в M, состоящей из тех m, которые положительны относительно всех вещественных $w\in V_\infty^M$ таких, что алгебра Δ_w не является полной матричной алгеброй; обозначим множество всех таких w через S. Пусть S_0 состоит из ограничений нормирований $w\in S$ на F. Тогда над каждым $v\in S_0$ лежат два нормирования w', $w''\in S$ (т. е. w' и w'' являются продолжениями v) и $M_{w'}=M_{w''}=F_v$, причем $w''=w'\sigma$. Если s — произвольный элемент, удовлетворяющий (1), то в силу условия $t=\sigma(s)/s\in\mathrm{Nrd}_{\Delta/M}(\Delta^*)$ s имеет одинаковые знаки относительно w' и w''. Поэтому найдется такой $f_v\in K_v$, что элемент sf_v положителен относительно w' и w''. Используя теорему 4 о слабой аппроксимации, выберем элемент $f\in K$ таким образом, чтобы f и f_v имели одинаковые знаки в K_v для всех $v\in S_0$. Тогда, полагая $s_1=sf$, получим, что $t=\sigma(s)/s=\sigma(s_1)/s_1$ и $s_1\in\mathrm{Nrd}_{\Delta/M}(\Delta^*)$. Доказательство теоремы 14 завершено.

3. Решетки и порядки. Пусть K — поле алгебраических чисел с кольцом целых чисел O. *Решеткой* (или, точнее, O-решеткой) в конечномерном векторном пространстве V над полем

K называется конечнопорожденный $\mathcal{O}$-подмодуль $L \subset V$, содержащий некоторый базис V над K (обычно в качестве V мы будем рассматривать стандартное n-мерное пространство $V = K^n$). Решетка $L \subset V$ называется *свободной*, если $\mathcal{O}$-модуль L свободен, т. е. обладает базисом. Если $\mathcal{O}$ — кольцо главных идеалов или, эквивалентно, число классов идеалов поля K равно единице, то любая решетка свободна. В общем случае любая решетка $L \subset V$ обладает так называемым *псевдобазисом*, т. е. если $\dim_K V = n$, то существуют такие $x_1, \ldots, x_n \in V$, что $L = \mathcal{O}x_1 \oplus \ldots \oplus \mathcal{O}x_{n-1} \oplus \mathfrak{a}x_n$, где $\mathfrak{a} \subset \mathcal{O}$ — некоторый идеал (см. О'Мира [1]).

Порядком в конечномерной K-алгебре A называется подкольцо $B \subset A$, содержащее единицу алгебры A и являющееся $\mathcal{O}$-решеткой. Порядок называется *максимальным*, если он не содержится ни в каком большем порядке.

Изучение решеток и порядков в существенной степени сводится к изучению соответствующих локальных конструкций. А именно (*локальной*) *решеткой* в конечномерном векторном пространстве V_{K_v} над полем K_v, где $v \in V_f^K$, называется конечнопорожденный $\mathcal{O}_v$-подмодуль $L_v \subset V_{K_v}$, содержащий базис V_{K_v}. Поскольку $\mathcal{O}_v$ — кольцо главных идеалов, то любая решетка обладает $\mathcal{O}_v$-базисом. Определение порядка и максимального порядка в конечномерной K_v-алгебре формулируется теперь очевидным образом. Ясно, что если L — некоторая решетка в конечномерном векторном пространстве V над K (соответственно B — некоторый порядок в конечномерной K-алгебре), то $L_v = L \otimes_{\mathcal{O}} \mathcal{O}_v$ (соответственно $B_v = B \otimes_{\mathcal{O}} \mathcal{O}_v$) является решеткой в пространстве $V_{K_v} = V \otimes_K K_v$ (соответственно порядком в алгебре $A_{K_v} = A \otimes_K K_v$). Таким образом, каждой решетке $L \subset V$ отвечает набор локализаций $\{L_v \subset V_{K_v} \mid v \in V_f^K\}$. Возникает вопрос, в какой степени решетка L определяется своими локализациями L_v.

Теорема 15. 1) $L = \bigcap_v (V \cap L_v)$, *в частности решетка, определяется своими локализациями однозначно*;

2) *для любых двух решеток* $L, M \subset V$ *имеем* $L_v = M_v$ *для почти всех* v;

3) *если* $L \subset V$ — *некоторая решетка и* $\{N_v \subset V_{K_v}\}$ — *произвольный набор локальных решеток, причем* $N_v = L_v$ *для почти всех* v, *то существует такая решетка* $M \subset V$, *что* $M_v = N_v$ *для всех* v.

Доказательство. Пусть L, M — две решетки, $x_1, \ldots, x_n$ — содержащийся в L базис пространства V и $y_1, \ldots, y_r$ — конечная система образующих M как $\mathcal{O}$-модуля. Тогда $y_i = \sum_{j=1}^{n} a_{ij}x_j$

для подходящих $a_{ij} \in K$. Выбирая целое число m таким образом, чтобы $ma_{ij} \in K$ для всех i, j, получим, что $mM \subset L$. Меняя L и M местами, установим существование такого $l \in \mathbb{Z}$, что $lL \subset M$, т. е. $L \subset \frac{1}{l} M$. Тогда если $v \notin V(lm)$ (обозначения см. п. 1 § 1.2), то $L_v = M_v$, и утверждение 2) доказано. При доказательстве утверждений 1), 2) удобно рассмотреть вложение V в соответствующее адельное пространство $V_{A_f} = V \otimes_K A_f$, где A_f — кольцо конечных аделей поля K. Из сильной аппроксимационной теоремы вытекает, что $L_{A_f(\infty)} = L \otimes_{\mathcal{O}} A_f(\infty) = \prod_{v \in V_f^K} L_v$ (где $A_f(\infty) = \prod_{v \in V_f^K} \mathcal{O}_v$ — кольцо целых конечных аделей) совпадает с замыканием L в V_{A_f}. Поэтому $L' = \bigcap_{v \in V_f^K} (V \cap L_v)$ совпадает с замыканием L в V в индуцированной топологии, и для доказательства 1) остается установить замкнутость L. Для этого снова рассмотрим некоторый базис $x_1, \ldots, x_n$ пространства V, содержащийся в L, и положим $M = \mathcal{O}x_1 + \ldots + \mathcal{O}x_n$. Из того, что $\mathcal{O} = \bigcap_{v \in V_f^K} (K \cap \mathcal{O}_v)$, вытекает, что M совпадает с $\bigcap_{v \in V_f^K} (V \cap M_v$.) Так как $\prod_v M_v$ наряду с $\prod_v L_v$ открыто в V_{A_f}, то отсюда следует открытость M, а следовательно, открытость и замкнутость $L \subset V$. Наконец, если набор локальных решеток $N_v \subset V_{K_v}$ удовлетворяет условию $N_v = L_v$ для почти всех v, то произведение $\prod_{v \in V_f^K} N_v$ является открытой компактной подгруппой в V_{A_f} и поэтому соизмеримо с $\prod_{v \in V_f^K} L_v$ (т. е. их пересечение имеет конечный индекс в каждой из них). Отсюда следует соизмеримость $M = \bigcap_{v \in V_f^K} (V \cap N_v)$ с $L = \bigcap_{v \in V_f^K} (V \cap L_v)$, и поэтому, очевидно, M является искомой решеткой.

Перейдем к изучению порядков в алгебрах. Мы ограничимся рассмотрением круга вопросов, связанных с существованием максимальных порядков и вложимостью произвольного порядка в максимальный, ибо именно эти вопросы возникают при рассмотрении максимальных арифметических и максимальных компактных подгрупп в алгебраических группах. Прежде всего заметим, что из теоремы 15 вытекает

Предложение 10. *Порядок $B \subset A$ является максимальным в том и только в том случае, если для каждого $v \in V_f^K$ максимален порядок $B_v \subset A_{K_v}$.*

Простые примеры (какие?) показывают, что произвольные алгебры могут не иметь максимальных порядков. Наша цель состоит в доказательстве того факта, что максимальные порядки всегда существуют в так называемых полупростых алгебрах. Напомним, что *полупростой* K-алгеброй называется прямая сумма конечного числа простых (не обязательно центральных) K-алгебр. Таким образом, полупростая алгебра имеет вид $A = \bigoplus_{i=1}^{r} M_{n_i}(D_i)$, где D_i — некоторая конечномерная алгебра с делением над K. В характеристике нуль условие полупростоты алгебры A эквивалентно тому, что $A \otimes_K \bar{K} = \bigoplus_{i=1}^{r} M_{m_i}(\bar{K})$ для подходящих целых m_i (см. Пирс [1]). Поэтому естественно вначале рассмотреть вопрос о максимальных порядках в матричной алгебре $A = M_n(K_v)$. Наши рассуждения будут основаны на изучении естественного действия A на пространстве $V = K_v^n$ и привлечении элементарных топологических соображений, связанных с понятием компактности. Для любой решетки $L \subset V$ положим $A^L = \{g \in M_n(K_v) \mid g(L) \subset L\}$ и будем называть A^L *стабилизатором* решетки L. Тогда A^L в базисе L совпадает с $M_n(\mathcal{O}_v)$ и, в частности, является порядком и открытым компактным подкольцом (в действительности эти понятия эквивалентны).

Предложение 11. 1) *Для любого компактного подкольца $B \subset A$ найдется такая решетка $L \subset V$, что $B \subset A^L$;*

2) *для любой решетки $L \subset V$ кольцо A^L является максимальным порядком в A;*

3) *любой порядок $B \subset A$ содержится в некотором максимальном порядке, причем таких максимальных порядков имеется лишь конечное число.*

Доказательство. Пусть $L_0 = \mathcal{O}_v^n$ — решетка, натянутая на стандартный базис пространства $V = K_v^n$. Тогда из открытости A^{L_0} и компактности B вытекает существование такого конечного набора $x_1, \ldots, x_r \in A$, что $B \subset \bigcup_{i=1}^{r} (x_i + A^{L_0})$. Отсюда следует, что $\mathcal{O}_v$-подмодуль $L \subset V$, порожденный множеством $B(L_0) = \bigcup_{x \in B} x(L_0)$, порождается на самом деле объединением $L_0 \cup x_1(L_0) \cup \ldots \cup x_r(L_0)$, т. е. является решеткой. При этом, очевидно, $B(L_0) \subset L_0$, что и доказывает 1). Далее, предположим, что A^L содержится в некотором порядке $B \subset A$. Так как любой порядок, очевидно, является открытым компактным подколь-

цом, то в силу 1) $B \subset A^M$ для подходящей решетки $M \subset V$. Таким образом, $A^L \subset A^M$ и наша цель — показать, что $A^L = A^M$. Заменяя решетку M на решетку вида αM, $\alpha \in \mathcal{O}_v \setminus \{0\}$, что не изменяет кольца A^M, можно предполагать, что $M \subset L$, но $M \not\subset \pi L$, где π — униформизующий элемент в K_v. Тогда можно выбрать такой базис $e_1, \ldots, e_n$ решетки L, что для подходящих целых неотрицательных $\alpha_2, \ldots, \alpha_n$ элементы $e_1, \pi^{\alpha_2}e_2, \ldots, \pi^{\alpha_n}e_n$ образуют базис M. Рассмотрим преобразование $g_i \in A^L$, которое векторы e_1 и e_i меняют местами, оставляя на месте все e_j для $j \neq 1, i$. В силу включения $A^L \subset A^M$ имеем $g_i \in A^M$, откуда $g_i(e_1) = e_i \in M$ и $\alpha_i = 0$. Окончательно получаем, что $L = M$, $A^L = A^M$, и утверждение 2) доказано. Из пунктов 1), 2) вытекает, что любой порядок $B \subset A$ содержится в некотором максимальном порядке $C = A^L$, так что остается установить конечность множества $\{C_l\}$ максимальных порядков в A, содержащих B. Имеем $C_l = A^{M_l}$, $B \supset \pi^\alpha C$ для подходящих решеток $M_l \subset V$ и некоторого целого неотрицательного α. Тогда для любого l имеем $C_l \supset B \supset \pi^\alpha C$. Покажем, что одновременно $\pi^\alpha C_l \subset C$. Как и при доказательстве 2), можно без ограничения считать, что решетки L и M_l обладают базисами вида $e_1, e_2, \ldots, e_n$ и $e_1, \pi^{\alpha_2}e_2, \ldots, \pi^{\alpha_n}e_n$ $(\alpha_i \geqslant 0)$. Так как $C_l \supset \pi^\alpha C$, то $C(M_l) \subset \subset \pi^{-\alpha}C_l(M_l) = \pi^{-\alpha}M_l$. Снова, используя введенные выше преобразования $g_i \in C$, получим, что $\alpha_i \leqslant \alpha$, т. е. $\pi^\alpha L \subset M_l$. Тогда $\pi^\alpha C_l(L) \subset C_l(M_l) = M_l \subset L$, т. е. $\pi^\alpha C_l \subset C$. Итак, $\pi^\alpha C \subset C_l \subset \subset \pi^{-\alpha}C$, откуда в силу конечности индекса $[\pi^{-\alpha}C : \pi^\alpha C]$ вытекает конечность числа различных C_l. Предложение доказано.

Замечание. Из описания максимальных порядков в $A = M_n(K_v)$ как стабилизаторов решеток $L \subset V$ вытекает их сопряженность в A.

Из предложения легко выводятся аналогичные утверждения о максимальных компактных подгруппах в $G = GL_n(K_v)$. Для произвольной решетки $L \subset V$ обозначим через G^L группу автоморфизмов L, т. е. $G^L = \{g \in G \mid g(L) = L\}$ (вообще, для произвольной подгруппы $\Gamma \subset G$ положим $\Gamma^L = \{g \in \Gamma \mid g(L) = L\}$ и будем называть Γ^L стабилизатором решетки L в группе Γ). Ясно, что $G^L = (\Lambda^L)^*$ отождествляется с группой $GL_n(\mathcal{O}_v)$ в базисе решетки L, так что G^L является открытой компактной подгруппой в G и $\det g \in U_v$ для любого $g \in G^L$.

Предложение 12. 1) *Для любой компактной подгруппы $B \subset G$ найдется такая решетка $L \subset V$, что $B \subset G^L$;*

2) *для любой решетки $L \subset V$ группа G^L является максимальной компактной подгруппой в G, в частности, любая компактная подгруппа содержится в некоторой максимальной компактной подгруппе;*

3) *все максимальные компактные подгруппы в G сопряжены между собой.*

Доказательство легко получается из предложения 11.

Из предложения 11 легко выводится также основная теорема о порядках в полупростых алгебрах над локальным полем.

Теорема 16. *Пусть A — полупростая алгебра над полем K_v. Тогда любой порядок $B \subset A$ содержится в некотором максимальном порядке, причем содержащих B максимальных порядков имеется лишь конечное число.*

Доказательство. Используя разложение A в прямую сумму простых алгебр, легко получить редукцию к случаю простой алгебры A. Пусть F — центр A, $\mathcal{O}_F$ — соответствующее кольцо целых. Тогда для любого $\mathcal{O}_v$-порядка $B \subset A$ произведение $\mathcal{O}_F B$ является одновременно $\mathcal{O}_v$- и $\mathcal{O}_F$-порядком в A. Из этого замечания вытекает, что достаточно рассмотреть случай $F = K_v$. Ясно, что для доказательства теоремы нам достаточно показать, что множество $\{B_i\}$ всех порядков в A, содержащих B, конечно. С этой целью выберем такое конечное расширение P поля K_v, что $A \otimes_{K_v} P \simeq M_n(P)$, и положим $\tilde{B} = B \otimes_{\mathcal{O}_v} \mathcal{O}_P$, $\tilde{B}_i = B_i \otimes \otimes_{\mathcal{O}_v} \mathcal{O}_P$. Тогда $\tilde{B}$ и $\tilde{B}_i$ являются порядками в $M_n(P)$, причем $\tilde{B} \subset \tilde{B}_i$. Но из предложения 11 вытекает, что среди порядков $\tilde{B}_i$ различных имеется лишь конечное число, поэтому остается показать, что $\tilde{B}_i = \tilde{B}_j$, только если $B_i = B_j$. Для этого выберем $\mathcal{O}_v$-базисы $x_1, \ldots, x_{n^2}$ и $y_1, \ldots, y_{n^2}$ порядков B_i и B_j соответственно. Тогда $x_l = \sum_{m=1}^{n^2} a_{lm} y_m$ и $y_l = \sum_{m=1}^{n^2} b_{lm} x_m$ для подходящих $a_{lm}, b_{lm} \in K_v$. Но поскольку $x_1, \ldots, x_{n^2}$ и $y_1, \ldots, y_{n^2}$ являются также $\mathcal{O}_P$-базисами порядков $\tilde{B}_i$ и $\tilde{B}_j$ и $\tilde{B}_i = \tilde{B}_j$, то в действительности $a_{lm}, b_{lm} \in \mathcal{O}_P \cap K_v = \mathcal{O}_v$, откуда $B_i = B_j$. Теорема 16 доказана.

Объединяя предложение 11 с теоремой 16, получаем существование максимальных порядков в полупростых алгебрах над полем алгебраических чисел.

Теорема 17. *Пусть A — полупростая алгебра над полем алгебраических чисел K. Тогда любой порядок $B \subset A$ содержится в некотором максимальном порядке.*

Доказательство, как и выше, редуцируется к случаю простой центральной K-алгебры A. Достаточно показать, что множество $\{B_i\}$ порядков алгебры A, содержащих B, конечно. Вначале это утверждение доказывается для матричной алгебры $A = M_n(K)$. Здесь, очевидно, A обладает максимальным порядком $C = M_n(\mathcal{O})$. Тогда из утверждения 2) теоремы 15 вытекает, что $B_v = C_v$ для почти всех $v \in V_f^K$ — максимальный порядок в $A_{K_v} = M_n(K_v)$. При этом для остальных v число порядков в A_{K_v}, содержащих B_v, конечно. Отсюда и из утверждения 1) теоремы 15 вытекает требуемое. Для сведения общего случая

к только что рассмотренному выберем конечное расширение P/K со свойством $A \otimes_K P \simeq M_n(P)$ и порядкам B, B_i сопоставим порядки $\tilde{B} = B \otimes_{\mathcal{O}} \mathcal{O}_P$, $\tilde{B}_i = B_i \otimes_{\mathcal{O}} \mathcal{O}_P$ в $M_n(P)$. Тогда среди $\tilde{B}_i$ имеется лишь конечное число различных, поэтому это же верно и для B_i. Теорема доказана.

Замечание. Можно показать, что над полем K_v все максимальные порядки сопряжены, однако над полем K, вообще говоря, имеются и несопряженные максимальные порядки.

ГЛАВА II

АЛГЕБРАИЧЕСКИЕ ГРУППЫ

Настоящая глава, как и первая, имеет вводный характер. В § 2.1 излагаются (как правило, без доказательства) основные структурные результаты об алгебраических группах, включая классификацию полупростых групп как над алгебраически замкнутым, так и над произвольным полем. В § 2.2 разбираются некоторые аспекты классификации K-групп при помощи когомологий Галуа. Используя эту технику, мы в § 2.3 даем явную классификацию групп классических типов. Кроме того, в § 2.3 содержится некоторый дополнительный материал, связанный с классическими группами, в частности, теорема Витта в относительном и абсолютном вариантах. Наконец, в § 2.4 излагаются необходимые сведения из алгебраической геометрии, включая конструкцию некоторых нужных нам алгебраических многообразий.

§ 2.1. Структурные свойства алгебраических групп

В этом параграфе собраны основные определения и результаты об алгебраических группах как над алгебраически замкнутым, так и над произвольным полем, которые будут постоянно использоваться в книге. Здесь мы не приводим фактически никаких доказательств, ибо наша основная цель — унифицировать терминологию и обозначения, а также указать точные ссылки относительно доказательств основных фактов. В качестве основных источников мы рекомендуем книги Борель [8], Хамфри [1] (случай алгебраически замкнутого основного поля) и статью Борель, Титс [1] (случай произвольного поля). Формально для понимания книги достаточно знакомства с перечисленными ниже результатами, однако в действительности желательно предварительное систематическое изучение указанных источников, а также основ алгебраической геометрии, теории алгебр Ли и систем корней, например, по книгам Шафаревич [1] и Бурбаки [4].

1. Алгебраические группы. В большинстве случаев мы довольствуемся «наивным» определением линейной алгебраической группы как замкнутой в топологии Зарисского подгруппы полной линейной группы $GL_n(\Omega)$, где Ω — так называемая «универсальная область» (алгебраически замкнутое поле беско-

нечной степени трансцендентности над простым подполем). Так, например, обстоит дело при построении теории приведения в гл. IV, где вообще можно считать, что $\Omega = \mathbb{C}$. Однако в ряде мест, особенно при работе с аделями или группами точек над различными пополнениями естественно иметь в виду более фундаментальный подход, при котором алгебраическая группа G рассматривается как алгебраическое многообразие вместе с морфизмами

$$\begin{aligned} G \times G &\xrightarrow{\mu} G, \quad (x, y) \longmapsto xy, \\ G &\xrightarrow{i} G, \qquad x \longmapsto x^{-1}, \end{aligned} \tag{1}$$

которые удовлетворяют обычным групповым аксиомам. В принципе, работая с группами точек над различными кольцами, иногда удобно использовать и схемную точку зрения, однако мы стремились ею не злоупотреблять. Отметим, что эти разные подходы приводят, фактически, к одному и тому же классу объектов, ибо аффинная алгебраическая группа в смысле второго определения является линейной, т. е. изоморфна замкнутой по Зарисскому подгруппе подходящей группы $GL_n(\Omega)$ (под морфизмом алгебраических групп понимается морфизм алгебраических многообразий, являющийся одновременно групповым гомоморфизмом; изоморфизм есть морфизм, для которого существует обратный морфизм). Так как более общие алгебраические группы, чем линейные, в данной книге не рассматриваются, то слово «линейный» будет зачастую опускаться.

В ряде случаев удобно рассматривать алгебраическую группу G как подмножество, замкнутое по Зарисскому не только в $GL_n(\Omega)$, но и в матричной алгебре $M_n(\Omega)$. Этого всегда можно добиться, увеличив число n (называемое *степенью группы* G) на единицу. Действительно, достаточно реализовать саму группу $GL_n(\Omega)$ как замкнутое подмножество в $M_{n+1}(\Omega)$. Искомое замкнутое вложение задается формулой

$$g \longmapsto \begin{pmatrix} & & 0 \\ & & 0 \\ & g & \vdots \\ 0 & 0 \ \dots & (\det g)^{-1} \end{pmatrix},$$

а его образ определяется следующими уравнениями на элементы матрицы $y = (y_{ij}) \in M_{n+1}(\Omega)$:

$$\begin{gathered} y_{i\,n+1} = y_{n+1\,i} = 0, \quad i = 1, \dots, n, \\ y_{n+1\,n+1} \cdot \det\left((y_{ij})_{i,\,j=1,\,\dots,\,n}\right) - 1 = 0. \end{gathered}$$

Отсюда следует, что кольцо регулярных функций на $GL_n(\Omega)$ есть $A = \Omega[x_{11}, x_{12}, \dots, x_{nn}, \det(x_{ij})^{-1}]$, а кольцо регулярных

функций на алгебраической группе $G \subset GL_n(\Omega)$ есть $A/\mathfrak{a}$, где $\mathfrak{a}$ — идеал функций из A, обращающихся в нуль на G (отметим, что некоторые часто используемые алгебро-геометрические понятия мы обсуждаем в § 2.4). В частности, если $f\colon G \to H$ — морфизм двух алгебраических групп $G \subset GL_n(\Omega)$, $H \subset GL_m(\Omega)$, то существуют такие полиномы

$$f_{kl} = f_{kl}(x_{11}, \ldots, x_{nn}, \det(x_{ij})^{-1}), \quad k, l = 1, \ldots, m, \tag{2}$$

что

$$f(g) = (f_{kl}(g))_{k, l = 1, \ldots, m}.$$

В этой книге будут рассматриваться алгебраические группы, определенные над некоторым подполем $K \subset \Omega$, в качестве которого будет обычно выступать либо поле алгебраических чисел, либо его пополнение. В связи с этим напомним, что алгебраическая группа $G \subset GL_n(\Omega)$ называется *K-определенной* (или, короче, *K-группой*), если рассмотренный выше идеал $\mathfrak{a} \subset A$ кольца A регулярных функций на $GL_n(\Omega)$, состоящий из функций, обращающихся в нуль на G, порождается пересечением $\mathfrak{a}_K = \mathfrak{a} \cap A_K$, где $A = K[x_{11}, \ldots, x_{nn}, \det(x_{ij})^{-1}]$. (Символы A_K, $\mathfrak{a}_K$ и аналогичные им будут систематически использоваться для обозначения «K-элементов» и в дальнейшем, причем в самых разнообразных ситуациях. Так для алгебраической K-группы $G \subset GL_n(\Omega)$ через G_K всюду будет обозначаться группа K-точек, т. е. пересечение $G \cap GL_n(K)$.) Морфизм $f\colon G \to H$ двух K-групп $G \subset GL_n(\Omega)$, $H \subset GL_m(\Omega)$ *определен над K* (другими словами, является *K-морфизмом*), если задающие его полиномы (2) можно выбрать из A_K.

В этой книге мы будем иметь дело исключительно с группами над совершенными полями. Поэтому ниже, если не оговорено противное, K будет обозначать некоторое совершенное поле (более того, в контексте излагаемой теории можно считать, что K либо конечно, либо является полем характеристики нуль). В этом случае критерий Галуа K-определенности, который мы рассмотрим в § 2.4 применительно к произвольным многообразиям, приобретает наиболее простой вид. Отметим также, что имеется и абстрактное определение K-группы как алгебраического K-многообразия с двумя K-морфизмами (1), которые удовлетворяют аксиомам группы. Можно, однако, показать (см. Борель [8]), что аффинная K-группа в смысле этого определения K-изоморфна K-определенной линейной алгебраической группе.

2. Конструкция ограничения основного поля. Пусть $G \subset GL_n(\Omega)$ — алгебраическая группа, определенная над конечным (сепарабельным) расширением L поля K степени d. Мы хотим построить такую алгебраическую K-группу G', группа K-точек G'_K которой была бы некоторым естественным образом

изоморфна группе L-точек G_L. Эту задачу решает группа, получаемая из G конструкцией ограничения основного поля с L до K, которая обозначается через $\mathbf{R}_{L/K}(G)$. Для построения $G' = \mathbf{R}_{L/K}(G)$ следует выбрать некоторый базис $\omega_1, \ldots, \omega_d$ поля L над K и рассмотреть соответствующее регулярное представление $\rho\colon L \to M_d(K)$, которое есть не что иное, как сопоставление элементу $x \in L$ матрицы правого сдвига $y \mapsto xy$ в данном базисе. Пусть

$$F_k(y^{\alpha\beta}) = 0, \quad \alpha, \beta = 1, \ldots, d; \quad k = 1, \ldots, z,$$

— система линейных уравнений относительно коэффициентов матрицы $y = (y^{\alpha\beta}) \in M_d(K)$, определяющая образ $\rho(L) \subset M_d(K)$. Пусть, далее, $P_l(x_{ij})$, $l = 1, \ldots, m$, — конечная система образующих идеала $\mathfrak{a}_L$, состоящая из полиномов от x_{ij}, где $\mathfrak{a} \subset \Omega[x_{11}, \ldots, x_{nn}, \det(x_{ij})^{-1}]$ — идеал функций, обращающихся в нуль на G. Используя стандартное отождествление $M_n(M_d(K)) = M_{nd}(K)$, поставим в соответствие полиному $P_l(x_{ij}) = \sum a_{\gamma_{11} \ldots \gamma_{nn}} x_{11}^{\gamma_{11}} \ldots x_{nn}^{\gamma_{nn}}$ «матричный» полином $\widetilde{P}_l(y_{ij}^{\alpha\beta}) = \sum \rho(a_{\gamma_{11} \ldots \gamma_{nn}}) (y_{11}^{\alpha\beta})^{\gamma_{11}} \ldots (y_{nn}^{\alpha\beta})^{\gamma_{nn}} \in M_d(K[y_{ij}^{\alpha\beta}])$ относительно n^2d^2 переменных $y_{ij}^{\alpha\beta}$ где $\alpha, \beta = 1, \ldots, d$; $i, j = 1, \ldots, n$. Тогда образ G'_L в $M_{nd}(K)$ при отображении, индуцируемом ρ, определяется уравнениями

$$\begin{aligned} &F_k(y_{ij}^{\alpha\beta}) = 0 \quad \forall i, j = 1, \ldots, n; \quad k = 1, \ldots, r, \\ &\widetilde{P}_l(y_{ij}^{\alpha\beta}) = 0 \qquad l = 1, \ldots, m \end{aligned} \tag{3}$$

(в последнем уравнении 0 обозначает матричный нуль в $M_d(K)$). Обозначим через G' множество решений системы (3) в $GL_{nd}(\Omega)$. Тогда G' и будет искомой алгебраической K-группой. Отметим, что при другом выборе базиса L/K группа $G' = \mathbf{R}_{L/K}(G)$ изменится на K-изоморфную.

Система уравнений (3), определяющая группу G', показывает, что группу G' можно интерпретировать как группу точек G в $\overline{K}$-алгебре $L \otimes_K \overline{K}$. Так как $L \otimes_K \overline{K} \simeq \overline{K}^d$, причем вложение L в $\overline{K}^d$ осуществляется по формуле $x \mapsto (\sigma_1(x), \ldots, \sigma_d(x))$, где $\sigma_1, \ldots, \sigma_d$ — различные вложения L в $\overline{K}$ над K, то отсюда вытекает существование $\overline{K}$-изоморфизма

$$G' \simeq G^{\sigma_1} \times \ldots \times G^{\sigma_d}, \tag{4}$$

где G^{σ_i}-подгруппа в $GL_n(\Omega)$, определяемая уравнениями из идеала $\mathfrak{a}_L^{\sigma_i}$, получаемого из $\mathfrak{a}_L$ путем применения ко всем многочленам вложения σ_i.

Любому L-определенному морфизму $f\colon G \to H$ алгебраических L-групп G, H соответствует K-определенный морфизм $\tilde{f} = \mathbf{R}_{L/K}(f)\colon \mathbf{R}_{L/K}(G) \to \mathbf{R}_{L/K}(H)$ (он строится аналогично тому, как по полиномам P строились полиномы $\tilde{P}$). Тем самым $\mathbf{R}_{L/K}$ является функтором из категории L-групп и L-гомоморфизмов в категорию K-групп и K-гомоморфизмов. Отметим, что не всякий K-морфизм $\tilde{f}\colon \mathbf{R}_{L/K}(G) \to \mathbf{R}_{L/K}(H)$ имеет вид $\tilde{f} = \mathbf{R}_{L/K}(f)$ для некоторого L-определенного морфизма $f\colon G \to H$ (например, если L/K — расширение Галуа, то у группы $R_{L/K}(G)$ имеются K-определенные автоморфизмы, индуцируемые автоморфизмами L/K, которые не представляются в виде $\mathbf{R}_{L/K}(f)$), однако, используя разложение (4), несложно показать (см. Борель [1], предложение 1.6), что имеет место совпадение групп рациональных характеров: $\mathbf{X}(\mathbf{R}_{L/K}(G))_K = \mathbf{X}(G)_L$ (определение характеров см. в п. 7).

Отметим два арифметических свойства конструкции ограничения основного поля. Пусть L/K — расширение полей алгебраических чисел и $v \in V^K$. Тогда, проводя отождествления $L \otimes_K K_v = \bigoplus_{w \mid v} L_w$ (см. § 1.1), для любой L-группы G будем иметь

$$\mathbf{R}_{L/K}(G)_{K_v} \simeq \prod_{w \mid v} G_{L_w}.$$

Пусть теперь $K = \mathbb{Q}$ и $\omega_1, \ldots, \omega_d$ — некоторый базис $\mathcal{O}/\mathbb{Z}$, где $\mathcal{O} = \mathcal{O}_L$ — кольцо целых поля L. Тогда, рассматривая регулярное представление ρ в этом базисе, мы придем к изоморфизмам $\mathbf{R}_{L/K}(G)_{\mathbb{Z}} \simeq G_{\mathcal{O}_L}$, и $\mathbf{R}_{L/K}(G)_{\mathbb{Z}_p} \simeq \prod_{v \mid p} G_{\mathcal{O}_v}$ для любого простого p.

3. Алгебра Ли алгебраической группы. Многообразие алгебраической группы G является однородным, а именно, для любых двух точек $g_1, g_2 \in G$ сдвиг $x \mapsto hx$ на элемент $h = g_2 g_1^{-1}$ является морфизмом алгебраического многообразия G, переводящим g_1 в g_2. Так как на многообразии всегда существует простая точка, то в действительности все точки G являются простыми, т. е. многообразие G гладко (относительно понятий, связанных с простыми точками и касательными пространствами, см. § 2.4 и 3.1). Алгеброй Ли $L(G)$ алгебраической группы G называется касательное пространство $T_e(G)$ к многообразию G в единице; ясно, что $\dim L(G) = \dim G$. Если $G \subset GL_n(\Omega)$, то $L(G) \subset M_n(\Omega) = L(GL_n(\Omega))$, причем скобка Ли задается стандартной формулой

$$[X, Y] = XY - YX.$$

Если подгруппа $G \subset GL_n(\Omega)$ определена над K, то $L(G)$ является алгеброй с K-структурой, а именно, для $L(G)_K = L(G) \cap M_n(K)$ выполняется $L(G)_K \otimes_K \Omega = L(G)$. При практическом

отыскании алгебры Ли следует пользоваться методом двойных чисел (см. Борель [8], Хамфри [1]).

Если $G \subset GL_n(\Omega)$, то для любого $g \in G$ имеем $gL(G)g^{-1} = L(G)$, так что возникает морфизм алгебраических групп $G \to GL(L(G))$, $g \mapsto \varphi_g$, где $\varphi_g(X) = gXg^{-1}$ для $X \in L(G)$, который называется присоединенным представлением группы G и обозначается Ad. Далее, рассмотрим отображение ad: $L(G) \to \mathrm{End}(L(G))$; $\mathrm{ad}\, X(Y) = [X, Y]$, называемое присоединенным представлением алгебры Ли $L(G)$. Используя двойные числа (см. Борель [8]), легко показать, что ad является дифференциалом в единице представления Ad. Введем симметричную билинейную форму f на $L(G)$, определяемую формулой

$$f(X, Y) = \mathrm{Tr}(\mathrm{ad}\, X\, \mathrm{ad}\, Y), \quad X, Y \in L(G),$$

где Tr обозначает след в матричной алгебре $\mathrm{End}(L(G))$, и называемую *формой Киллинга*; тогда f инвариантна относительно присоединенного действия группы G.

4. Связная компонента. Поскольку многообразие G является гладким, его неприводимые компоненты совпадают со связными. Связная компонента единицы G^0 является открыто-замкнутым нормальным делителем в G конечного индекса. При этом $\dim G = \dim G^0$ и $L(G) = L(G^0)$. Если группа G определена над K, то группа G^0 также определена над K. Отметим, что большинство групп, рассматриваемых в книге, являются связными. В частности, все редуктивные или полупростые группы предполагаются связными.

5. Разложение Жордана. Пусть $g \in GL_n(\Omega)$; тогда g можно единственным образом представить в виде $g = g_s g_u$, где g_s — полупростая матрица (т. е. g_s можно сопряжением привести к диагональному виду), а g_u — унипотентная (т. е. все собственные значения g_u равны 1) и $g_s g_u = g_u g_s$. Разложение $g = g_s g_u$ называется *разложением Жордана*. Если $g \in G$, где $G \subset GL_n(\Omega)$ — некоторая алгебраическая группа, то $g_s, g_u \in G$. При этом если f: $G \to H$ — морфизм алгебраических групп, то $f(g)_s = f(g_s)$ и $f(g)_u = f(g_u)$. В этом смысле разложение Жордана не зависит от матричной реализации G. Кроме того, если $g \in G_K$, то $g_s, g_u \in G_K$ (напоминаем, что поле K предполагается совершенным). Аналогично, любую матрицу $X \in M_n(\Omega)$ можно представить в виде $X = X_s + X_n$, где X_s, X_n — соответственно полупростая и нильпотентная матрицы такие, что $X_s X_n = X_n X_s$, причем это разложение, называемое *аддитивным разложением Жордана*, определено однозначно. Если $X \in L(G)$, то $X_s, X_n \in L(G)$, причем компоненты X_s, X_n ведут себя функториально при дифференциалах морфизмов алгебраических групп. При этом для $X \in L(G)_K$ имеем $X_s, X_n \in L(G)_K$.

6. Фактормногообразия. Если G — K-определенная группа, $H \subset G$ — ее K-определенная подгруппа, то множество G/H

смежных классов наделяется структурой алгебраического K-многообразия (в общем случае квазипроективного) такой, что факторотображение $G \to G/H$ является K-определенным морфизмом алгебраических многообразий (см. подробнее § 2.4). В случае когда H является нормальным делителем в G, многообразие G/H оказывается аффинным, причем структура многообразия на G/H согласована с естественной групповой операцией, так что G/H становится алгебраической K-группой, а отображение $G \to G/H$ — K-определенным морфизмом алгебраических групп.

7. Диагонализируемые группы и алгебраические торы. Алгебраическая группа G называется диагонализируемой, если для некоторого точного представления $f\colon G \to GL_m(\Omega)$ группа $f(G)$ диагонализируема, т. е. сопряжена подгруппе группы D_n диагональных матриц. В этом случае образ любого представления $h\colon G \to GL_m(\Omega)$ также диагонализируем. Можно показать, что класс диагонализируемых групп совпадает с классом коммутативных алгебраических групп, состоящих из полупростых элементов. Среди диагонализируемых групп особую роль занимают связные диагонализируемые группы, которые обычно называются *алгебраическими торами*. Алгебраические торы можно также определить как такие алгебраические группы G, для которых существует изоморфизм $G \simeq (\boldsymbol{G}_m)^d$, где $\boldsymbol{G}_m = GL_1(\Omega)$ — мультипликативная группа поля Ω, $d = \dim G$. *Характером алгебраической группы* G называется морфизм алгебраических групп $\chi\colon G \to \boldsymbol{G}_m$. Все характеры группы G образуют коммутативную группу относительно операции $(\chi_1 + \chi_2)(g) = \chi_1(g)\chi_2(g)$; эту группу мы будем обозначать через $\mathbf{X}(G)$. Легко видеть, что для d-мерного тора G группа $\mathbf{X}(G)$ изоморфна $\mathbb{Z}^d$, т. е. является конечнопорожденным $\mathbb{Z}$-модулем без кручения.

Для K-определенного тора G изоморфизм $G \simeq (\boldsymbol{G}_m)^d$, вообще говоря, нельзя выбрать K-определенным; в случае, когда это возможно, тор G называют *K-разложимым*. Оказывается, что следующие условия равносильны: 1) тор G является K-разложимым; 2) все его характеры определены над K; 3) для любого (эквивалентно, некоторого точного) K-определенного представления $f\colon G \to GL_n(\Omega)$ группа $f(G)$ диагонализируема над K, т. е. сопряжена подгруппе группы D_n при помощи матрицы из $GL_n(K)$. Отметим, что последние два условия имеют смысл и эквивалентны также для произвольной диагонализируемой K-группы и тем самым позволяют определить понятие K-диагонализируемой группы. В общем случае диагонализируемая K-группа G становится диагонализируемой над некоторым конечным расширением L поля K, называемым *полем разложения* G. Из условия 2) вытекает, что расширение L поля K будет полем разложения для G в том и только том случае, если $\mathbf{X}(G) = \mathbf{X}(G)_L$. На языке теории Галуа это означает, что если

рассмотреть естественное действие на $\mathbf{X}(G)$ группы Галуа $\mathscr{G} = \mathrm{Gal}(\bar{K}/K)$ (напомним, что поле K предполагается совершенным), что равносильно заданию на дискретной группе $\mathbf{X}(G)$ структуры непрерывного модуля над проконечной группой $\mathscr{G}$, то открытая подгруппа $\mathscr{H} \subset \mathscr{G}$, отвечающая L, действует на $\mathbf{X}(G)$ тривиально, т. е. $\mathbf{X}(G) = \mathbf{X}(G)^{\mathscr{H}}$. Отсюда, в частности, вытекает существование минимального поля разложения данной диагонализируемой K-группы G, которое автоматически является расширением Галуа поля K и содержится в любом другом поле разложения.

Итак, для K-разложимого тора G имеем $\mathbf{X}(G) = \mathbf{X}(G)_K$. Антиподами K-разложимых торов являются так называемые *K-анизотропные* торы, для которых $\mathbf{X}(G)_K = 0$. Известно, что в любом K-торе G существуют K-определенные подторы G_a и G_d, являющиеся соответственно K-разложимым и K-анизотропным торами, такие, что $G = G_a G_d$ и пересечение $G_a \cap G_d$ конечно (т. е. G является почти прямым произведением G_a и G_d).

Соответствие $G \xrightarrow{\Phi} \mathbf{X}(G)$ является контравариантным функтором из категории $\mathscr{A}$ K-определенных диагонализируемых групп, разложимых над конечным расширением Галуа L/K с группой Галуа $\mathscr{F}$, и K-определенных морфизмов, в категорию $\mathscr{B}$ конечнопорожденных модулей над групповым кольцом $\Gamma = \mathbb{Z}[\mathscr{F}]$ и Γ-гомоморфизмов таких модулей.

Теорема 1. *Соответствие Φ является контравариантной эквивалентностью категорий, при которой подкатегории $\mathscr{A}_0 \subset \mathscr{A}$, состоящей из K-определенных алгебраических торов, отвечает подкатегория $\mathscr{B}_0 \subset \mathscr{B}$, образованная Γ-модулями без $\mathbb{Z}$-кручения.*

Теорема 1 играет фундаментальную роль при исследовании алгебраических торов, которому посвящена книга Воскресенского [3]. Благодаря ей алгебраический тор можно задавать, указывая соответствующий модуль характеров. При этом, как показал Воскресенский, на этом языке могут быть описаны многие геометрические и арифметические свойства торов. В настоящей книге мы не будем касаться теории торов, отсылая читателя к книге Воскресенского, а ограничимся указанием на характерные примеры и нужные для дальнейшего конструкции.

Прежде всего отметим, что имеется также ковариантная эквивалентность между категориями $\mathscr{A}_0$ и $\mathscr{B}_0$, которая задается соответствием $G \xrightarrow{\Psi} \mathbf{X}_*(G)$, где $\mathbf{X}_*(G) = \mathrm{Hom}(\boldsymbol{G}_m, G)$ — группа кохарактеров, или однопараметрических подгрупп в G, естественным образом наделяемая структурой Γ-модуля. Имеется естественное спаривание $\mathbf{X}_*(G) \times \mathbf{X}(G) \to \mathbb{Z}$, определяемое следующим образом: если $\varphi \in \mathbf{X}_*(G)$, $\chi \in \mathbf{X}(G)$, то композиция $\chi \circ \varphi$ является морфизмом $\boldsymbol{G}_m$ в $\boldsymbol{G}_m$; поэтому $(\chi \circ \varphi)(t) = t^m$ для некоторого $m \in \mathbb{Z}$ $(t \in \Omega^*)$, и тогда полагаем $\langle \chi, \varphi \rangle = m$. Это

спаривание позволяет отождествить $\mathbf{X}_*(G)$ с Γ-модулем $\mathrm{Hom}_{\mathbb{Z}}(\mathbf{X}(G), \mathbb{Z})$, двойственным к $\mathbf{X}(G)$. Отсюда, в частности, вытекает что если тор G K-разложим, т. е. $\mathbf{X}(G) = \mathbf{X}(G)_K$, то и $\mathbf{X}_*(G) = \mathbf{X}_*(G)_K$. С другой стороны, если тор G K-анизотропен, то $\mathbf{X}_*(G) = 0$. Обратно, если $\mathbf{X}_*(G) = \mathbf{X}_*(G)_K$ (соответственно $\mathbf{X}_*(G) = 0$), то тор G K-разложим (соответственно K-анизотропен).

Пример. Пусть L/K — конечное расширение степени d. Положим $G = \mathbf{R}_{L/K}(\boldsymbol{G}_m)$. Тогда из результатов пункта 2 вытекает существование K-определенного изоморфизма $G \simeq (\boldsymbol{G}_m)^d$, т. е. G является d-мерным тором. Из явного описания конструкции ограничения основного поля вытекает, что G реализуется в качестве K-определенной подгруппы группы $GL_d(\Omega)$. Обозначим через φ ограничение на G обычного определителя. Тогда φ является K-определенным морфизмом G в $\boldsymbol{G}_m$, т. е. элементом из $\mathbf{X}(G)_K$. С точки зрения теории полей ограничение φ на $G_K = L^*$ совпадает с определителем регулярного представления L над K, т. е. с обычной нормой $N_{L/K}$: $L^* \to K^*$. Поэтому ядро φ, обычно обозначаемое $\mathbf{R}^{(1)}_{L/K}(\boldsymbol{G}_m)$, называется *норменным тором*, отвечающим расширению L/K. Минимальным полем разложения L является нормальное замыкание P поля L над K. Положим $\mathcal{F} = \mathrm{Gal}(P/K)$, $\mathcal{H} = \mathrm{Gal}(P/L)$. Тогда $\mathbf{X}(G)$, как модуль над $\Gamma = \mathbb{Z}[\mathcal{F}]$, изоморфен $\mathbb{Z}[\mathcal{F}/\mathcal{H}]$—свободному $\mathbb{Z}$-модулю, базис которого составляют смежные классы $g\mathcal{H}$, $g \in \mathcal{F}$, на которых $\mathcal{F}$ действует левыми сдвигами. Норменному отображению φ: $G \to \boldsymbol{G}_m$ соответствует гомоморфизм Γ-модулей $\mathbb{Z} \to \mathbb{Z}[\mathcal{F}/\mathcal{H}]$, где $z \mapsto z\sigma$, $\sigma = \sum g\mathcal{H}$, и сумма берется по всем смежным классам. Тогда модуль характеров $\mathbf{X}(H)$ норменного тора $H = \mathbf{R}^{(1)}_{L/K}(\boldsymbol{G}_m)$ совпадает с фактормодулем $\mathbb{Z}[\mathcal{F}/\mathcal{H}]/\mathbb{Z}\sigma$. Поскольку модуль неподвижных точек $\mathbb{Z}[\mathcal{F}/\mathcal{H}]^{\mathcal{F}}$ совпадает с $\mathbb{Z}\sigma$, то отсюда вытекает, что $\mathbf{X}(H)_K = 0$, т. е. тор H является K-анизотропным. Тот же результат можно получить, рассматривая вместо модулей характеров модули кохарактеров. Здесь также модуль $\mathbf{X}_*(G)$ изоморфен $\mathbb{Z}[\mathcal{F}/\mathcal{H}]$, а модуль $\mathbf{X}_*(H)$ есть ядро пополняющего гомоморфизма $\mathbb{Z}[\mathcal{F}/\mathcal{H}] \to \mathbb{Z}$, $\sum a_g g\mathcal{H} \mapsto \sum a_g$. Ясно, что $\mathbf{X}_*(H)^{\mathcal{F}} = \mathbf{X}_*(H) \cap \mathbb{Z}\sigma = (0)$, и снова получаем, что тор H K-анизотропен.

Предыдущий пример допускает следующее обобщение. Рассмотрим r конечных расширений $L_1, \ldots, L_r$ поля K, и для каждого $i = 1, \ldots, r$ построим соответствующее норменное отображение φ_i: $\mathbf{R}_{L_i/K}(\boldsymbol{G}_m) \to \boldsymbol{G}_m$. Тогда $T = \{(x_1, \ldots, x_r) \in \mathbf{R}_{L_1/K}(\boldsymbol{G}_m) \times \ldots \times \mathbf{R}_{L_r/K}(\boldsymbol{G}_m) \mid \varphi_1(x_1) \ldots \varphi_r(x_r) = 1\}$ является тором, который естественно называть *мультинорменным*.

Торы вида $\mathbf{R}_{L/K}(\boldsymbol{G}_m)$ и их конечные прямые произведения называются *квазиразложимыми* (над K). Им отвечают так на-

зываемые *пермутационные модули характеров*, т. е. $\mathbb{Z}$-свободные конечнопорожденные модули, обладающие базисом, элементы которого переставляются под действием абсолютной группы Галуа $\mathcal{G} = \mathrm{Gal}(\bar{K}/K)$. Квазиразложимые торы наиболее легко поддаются изучению, поэтому при изучении произвольных торов зачастую с успехом применяется прием, суть которого состоит в том, что рассматриваемый тор накрывается подходящим квазиразложимым тором. Приведем несколько примеров такого рода конструкций, которые понадобятся нам в дальнейшем.

Предложение 1. *Пусть F — диагонализируемая K-группа, разложимая над расширением P/K. Тогда F может быть вложена в точную последовательность*

$$1 \to F \to T \to S \to 1,$$

где T и S — K-торы, разложимые над P, причем тор T квазиразложим над K.

Доказательство. Обозначим через $\mathcal{H}$ ядро естественного действия группы Галуа $\mathcal{G} = \mathrm{Gal}(\bar{K}/K)$ на группе характеров $\mathbf{X}(F)$, и пусть $L = \bar{K}^{\mathcal{H}}$ — соответствующее неподвижное поле. Тогда L/K является конечным расширением Галуа поля K с группой Галуа $\mathcal{F} = \mathcal{G}/\mathcal{H}$, причем, очевидно, $L \subset P$. Рассмотрим теперь $\mathbf{X}(F)$ как модуль над групповым кольцом $\Gamma = \mathbb{Z}[\mathcal{F}]$ и представим его как фактормодуль некоторого свободного модуля Γ^l. Тогда имеет место точная последовательность вида

$$0 \to \Delta \to \Gamma^l \to \mathbf{X}(F) \to 0.$$

Переходя от модулей Δ и Γ^l к соответствующим торам, мы получим точную последовательность

$$1 \to F \to T \to S \to 1,$$

где T и S — K-торы, причем $T = \mathbf{R}_{L/K}(\mathbf{G}_m)^l$. Предложение доказано.

Если провести аналогичное рассуждение, предполагая F тором и используя вместо модуля характеров модуль кохарактеров, мы получим

Предложение 2. *Любой K-тор F может быть вложен в точную последовательность $1 \to S \to T \to F \to 1$, где S и T — K-торы и тор T квазиразложим.*

Нам понадобится также следующее

Предложение 3 (Оно [5]). *Для любого K-тора F существует такое целое число $m > 0$ и такой квазиразложимый тор T', что произведение $F^m \times T'$ изогенно некоторому квазиразложимому K-тору T.*

(Напомним, что *изогенией* алгебраических групп называется сюръективный гомоморфизм с конечным ядром; две группы называются *изогенными*, если между ними существует изогения.

Применительно к полупростым группам мы рассмотрим это понятие в п. 13. В случае торов свойства изогенности не такие как в полупростом случае; в частности, отношение изогенности является отношением эквивалентности. В терминах групп характеров это отношение выражается следующим образом: два тора T_1, T_2 из категории $\mathscr{A}_0$, описанной в теореме 1, изогенны в том и только том случае, если $\mathbb{Q}[\mathscr{F}]$-модули $\mathbf{X}(T_1)\otimes_{\mathbb{Z}}\mathbb{Q}$ и $\mathbf{X}(T_2)\otimes_{\mathbb{Z}}\mathbb{Q}$ изоморфны).

Доказательство предложения 3, которое мы опускаем (см. цитированную работу Оно, а также его статью в сборнике «Арифметические группы и автоморфные функции»), в действительности является переводом на язык торов теоремы Артина об индуцированных характерах.

8. Разрешимые и унипотентные группы. В этом пункте предполагается, что характеристика основного поля равна 0. Алгебраическая группа G называется *унипотентной*, если ее элементы унипотентны. Примером унипотентной группы может служить аддитивная группа поля

$$\boldsymbol{G}_a=\left\{g\in GL_2(\Omega)\mid g=\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\right\}.$$

Если $G\subset GL_n(\Omega)$ — унипотентная группа, то $(g-E_n)^n=0$, где E_n — единичная $n\times n$-матрица; тогда «усеченное» логарифмическое отображение

$$l\colon G\to M_n(\Omega),\quad l(g)=(g-E_n)-\frac{(g-E_n)^2}{2}+\ldots$$
$$\ldots+(-1)^{n-2}\frac{(g-E_n)^{n-1}}{n-1}$$

устанавливает полиномиальный изоморфизм многообразий группы G и ее алгебры Ли $L(G)$; обратное отображение доставляет «усеченное» экспоненциальное отображение $e\colon L(G)\to G$, $e(X)=E_n+X+\frac{X^2}{2!}+\ldots+\frac{X^{n-1}}{(n-1)!}$. В частности, группа G всегда связна. Пусть теперь $G\subset GL_n(\Omega)$ — K-определенная унипотентная подгруппа. Тогда G триангулируема над K, т. е. существует такая матрица $g\in GL_n(K)$, что группа gGg^{-1} содержится в группе $\boldsymbol{U}_n$ верхних унитреугольных матриц. Отсюда, в частности, следует, что группа G нильпотентна. Более того, можно показать, что в G существует центральный ряд

$$G=G_0\supset G_1\supset\ldots\supset G_n=\{e\}$$

такой, что $G_i/G_{i+1}\simeq\boldsymbol{G}_a$, $i=0,\ldots,n-1$. Отметим, что часть из приведенных выше фактов не переносится в положительную характеристику.

Нам понадобится одно техническое утверждение об унипотентных группах.

Лемма 1. *Пусть K-разложимый тор T действует автоморфизмами на унипотентной K-группе U. Тогда для любой T-инвариантной K-подгруппы $V \subset U$ найдется такое T-инвариантное K-определенное замкнутое по Зарисскому подмножество $P \subset U$, что морфизм-произведение индуцирует K-изоморфизмы многообразий $P \times V \xrightarrow{\sim} U$ и $V \times P \xrightarrow{\sim} U$. При этом если группа U абелева, то в качестве P можно выбрать подходящую K-подгруппу в U.*

Действительно, если U абелева, то введенное выше отображение l: $U \to L(U)$ является изоморфизмом групп, так что достаточно выбрать T-инвариантное K-определенное подпространство $W \subset L(U)$, дополнительное к $L(V)$, и положить $P = e(W)$. Общий случай разбирается при помощи индукции по $\dim U/V$, причем с помощью центрального ряда (1) все дело сводится к случаю $\dim U/V = 1$. Тогда опять можно положить $P = e(W)$, где W — одномерное T-инвариантное K-определенное дополнение в $L(U)$ к $L(V)$.

Пусть теперь $G \subset GL_n(\Omega)$ — связная разрешимая группа. Тогда G триангулируема (теорема Ли — Колчина). Отсюда получается структурная теорема для разрешимых групп: множество G_u унипотентных элементов связной разрешимой группы G образует нормальный делитель в G, а G является полупрямым произведением G_u и (произвольного) максимального тора $T \subset G$. Если G определена над K, то группа G_u также определена над K и существует максимальный K-определенный тор $T \subset G$, причем в этом случае разложение $G = TG_u$ в полупрямое произведение также определено над K. Над полем Ω существует композиционный ряд

$$G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\} \tag{5}$$

такой, что последовательные факторы G_i/G_{i+1} изоморфны $\boldsymbol{G}_m$ или $\boldsymbol{G}_a$. Если существует ряд (5), состоящий из K-определенных подгрупп, причем факторы G_i/G_{i+1} K-изоморфны $\boldsymbol{G}_m$ или $\boldsymbol{G}_a$, то группа G называется *K-разложимой*. В действительности это эквивалентно существованию максимального K-разложимого тора $T \subset G$, и тогда любой K-определенный тор в G разложим над K. В частности, любая унипотентная K-группа является K-разложимой, причем в этом случае все факторы соответствующего ряда (5) K-изоморфны $\boldsymbol{G}_a$.

9. Связные группы. При изучении связных групп G выделяют два класса подгрупп: максимальные торы $T \subset G$ и *подгруппы Бореля* $B \subset G$ (т. е. максимальные связные разрешимые подгруппы). Из соображений размерности вытекает, что максимальные торы и подгруппы Бореля всегда существуют. Далее, оказывается, что все максимальные торы в G (соответственно

подгруппы Бореля) сопряжены в G. (В частности, размерность $r = \dim T$ не зависит от выбора тора T, называется (*абсолютным*) *рангом* группы G и обозначается $\operatorname{rang} G$.) Известно также, что подгруппа Бореля совпадает со своим нормализатором в G. Отсюда следует, что если зафиксировать некоторый максимальный тор $T \subset G$ (соответственно подгруппу Бореля $B \subset G$), то множество всех максимальных торов в G (соответственно борелевских подгрупп) можно отождествить с множеством смежных классов G/N, где $N = N_G(T)$ — нормализатор T в G (соответственно G/B)). (См. также теорему 19 в § 2.4.) Содержащие B подгруппы $P \subset G$ называются *параболическими*. Они связны и характеризуются тем свойством, что фактормногообразие G/P (см. Борель [8]) является проективным.

Если группа G определена над K, то существует максимальный тор $T \subset G$, определенный над K. Напротив, определенной над K борелевской подгруппой группа G, как правило, не обладает; те же группы, для которых такая подгруппа существует, называются *квазиразложимыми* над K. Группа G называется K-разложимой, если существует максимальный K-тор $T \subset G$, разложимый над K (для связных разрешимых групп это понятие совпадает с определением предыдущего пункта).

Теорема 2. *Пусть G — связная алгебраическая группа над бесконечным совершенным полем K. Тогда G_K плотно в G в топологии Зарисского.*

Радикалом $R(G)$ группы G называется максимальный связный разрешимый нормальный делитель в G, а *унипотентным радикалом* $R_u(G)$ — максимальный связный унипотентный нормальный делитель (очевидно, что $R_u(G)$ совпадает с унипотентной частью $R(G)_u$ радикала $R(G)$). Связная группа G называется *редуктивной* (соответственно *полупростой*), если $R_u(G) = \{e\}$ (соответственно $R(G) = \{e\}$). Легко видеть, что для любой связной группы G факторгруппа $G/R(G)$ полупроста, а факторгруппа $G/R_u(G)$ редуктивна.

Если группа G определена над K, то оба радикала $R(G)$ и $R_u(G)$ также определены над K. Имеет место

Теорема 3 (Мостов [1]). *Пусть G — связная группа над полем K характеристики 0. Тогда существует такая редуктивная K-определенная подгруппа $H \subset G$, что $G = HR_u(G)$ — полупрямое произведение. При этом любая редуктивная K-определенная подгруппа $H' \subset G$ сопряжена при помощи элемента из $R_u(G)_K$ подгруппе группы H.*

Разложение $G = HR_u(G)$, существование которого утверждается теоремой, называется *разложением Леви*. С его помощью многие вопросы сводятся к редуктивным группам. Теорема 3 является аналогом теоремы для групп Ли, полученной Леви и Мальцевым (см. Мальцев [1, 2]).

10. Редуктивные группы. Используемые в дальнейшем свойства редуктивных групп заключены в следующей теореме.

Теорема 4. *Пусть G — редуктивная K-группа. Тогда*: 1) *радикал $R(G)$ совпадает со связной компонентой S центра $Z(G)$ и является тором*; 2) *коммутант $H = [G, G]$ является полупростой K-группой*; 3) *$G = HS$ — почти прямое произведение* (*т. е. пересечение $H \cap S$ конечно*); 4) *если* $\operatorname{char} K = 0$, *то любое алгебраическое представление f: $G \to GL_n(\Omega)$ является вполне приводимым.*

Более точный анализ структуры редуктивных и, в особенности, полупростых групп основан на понятии системы корней. Для ее определения рассмотрим редуктивную группу G и зафиксируем некоторый максимальный тор $T \subset G$. Пусть $\mathfrak{g} = L(G)$ — алгебра Ли группы G и Ad: $G \to GL(\mathfrak{g})$ — присоединенное представление. Тогда из п. 7 вытекает, что группа $\mathrm{Ad}\, T$ является диагонализируемой в $GL(\mathfrak{g})$. Этот факт нам удобно выразить в следующей форме. Для $\alpha \in \mathbf{X}(T)$ обозначим через $\mathfrak{g}_\alpha$ весовое пространство, отвечающее весу α, т. е. $\mathfrak{g}_\alpha = \{X \in \mathfrak{g} \mid \mathrm{Ad}(t)X = \alpha(t)X, \quad \forall t \in T\}$, и положим $R(T, G) = \{\alpha \in \mathbf{X}(T) \mid \alpha \neq 0 \text{ и } \mathfrak{g}_\alpha \neq 0\}$. Тогда $\mathfrak{g} = L(T) \oplus \left(\bigoplus_{\alpha \in R(T, G)} \mathfrak{g}_\alpha\right)$, где $L(T)$ — алгебра Ли тора T, совпадающая с весовым пространством веса 0. Замечательный факт состоит в том, что множество $R = R(T, G)$ образует абстрактную систему корней в пространстве $V = \mathbf{X}(T/S) \underset{\mathbb{Z}}{\otimes} \mathbb{R}$ (определение см. в книге Бурбаки [4], гл. VI), поэтому его естественно называть системой корней группы G относительно тора T. Отметим, что если группа G полупроста, то $S = \{e\}$, и мы получаем систему корней в пространстве $\mathbf{X}(T) \underset{\mathbb{Z}}{\otimes} \mathbb{R}$. Каждое пространство $\mathfrak{g}_\alpha$ одномерно, и ему соответствует одномерная унипотентная подгруппа $U_\alpha \subset G$ (*корневая подгруппа* такая, что $\mathfrak{g}_\alpha = L(U_\alpha)$). Подгруппа $G_\alpha \subset G$, порожденная U_α и $U_{-\alpha}$ (отметим, что если $\alpha \in R$, то и $-\alpha \in R$), является полупростой группой ранга 1, откуда следует, что в действительности $G_\alpha \simeq SL_2(\Omega)$ либо $PSL_2(\Omega)$. Укажем также на следующее эквивалентное описание группы G_α: G_α является коммутантом централизатора Z_α связной компоненты $(\operatorname{Ker} \alpha)^0$ ядра характера α.

Пусть $\Pi \subset R$ — некоторая система простых корней, R_+^Π — соответствующая система положительных корней (см. Бурбаки [4], гл. VI). Тогда группа $U(\Pi)$, порожденная всеми группами U_α для $\alpha \in R_+^\Pi$, нормализуется тором T, и полупрямое произведение $B(\Pi) = TU(\Pi)$ является подгруппой Бореля в G. При этом соответствие $\Pi \to B(\Pi)$ задает биекцию между множеством систем простых корней в R и множеством подгрупп Бореля в G, содержащих T. Таким образом, по заданной подгруппе

Бореля $B \subset G$, содержащей T, однозначно определяется некоторая система простых корней Π, и можно выбрать упорядочение V_+ на пространстве V такое, что $R_+^{\Pi} = R \cap V_+$.

С системой корней R связывается так называемая *группа Вейля* $W = W(R)$ (Бурбаки [4]). Системой её образующих является множество S, состоящее из отражений w_α относительно простых корней $\alpha \in \Pi$. При этом пара (W, S) является группой Кокстера (см. Бурбаки [4], гл. IV, VI). В W существует единственный элемент w максимальной длины (относительно системы образующих S). Он характеризуется тем свойством, что $w(R_+^{\Pi}) = -R_+^{\Pi}$, и его длина в действительности совпадает с числом положительных корней. Замечательно, что группа Вейля $W(R)$ может быть отождествлена с группой Вейля $W(T, G)$ группы G относительно тора T, которая определяется как факторгруппа $N_G(T)/T$, где $N_G(T)$ — нормализатор тора T. Напомним вкратце, как это делается. Действие $N_G(T)$ на T посредством сопряжений определяет гомоморфизм $W(T, G)$ в группу автоморфизмов $\mathrm{Aut}(R)$ системы корней R. Для любого $\alpha \in R$ группа Вейля $W(T_\alpha, G_\alpha)$, где $T_\alpha = T \cap G_\alpha$, имеет порядок 2, причем элемент $n_\alpha \in N_{G_\alpha} \setminus T_\alpha$ индуцирует на R отражение w_α. Отсюда следует, что образ $W(T, G)$ в $\mathrm{Aut}(R)$ содержит группу $W(R)$. Остается заметить, что группы $W(T, G)$ и $W(R)$ имеют одинаковые порядки, ибо первая однотранзитивно действует на множестве подгрупп Бореля, содержащих тор T, а вторая — на системах простых корней в R.

Группа Вейля $W = W(T, G)$ имеет еще одну содержательную интерпретацию, связанную с так называемым *разложением Брюа*. А именно, для каждого элемента $w \in W(T, G)$ выберем некоторый представитель $n_w \in N_G(T)$ и рассмотрим двойной смежный класс Bn_wB, где B — некоторая подгруппа Бореля в G, содержащая T.

Теорема 5 (разложение Брюа). *Для редуктивной группы G имеет место представление*

$$G = \bigcup_{w \in W} Bn_wB, \tag{6}$$

где справа стоит объединение непересекающихся двойных смежных классов.

Следствие. *Пересечение двух любых подгрупп Бореля группы G содержит максимальный тор.*

Действительно, рассмотрим произвольную подгруппу Бореля $B \subset G$, и пусть (6) — соответствующее разложение Брюа. По теореме сопряженности любая другая подгруппа Бореля имеет вид gBg^{-1}, $g \in G$. Пользуясь разложением Брюа, представим элемент g в виде $g = b_1nb_2$, где $b_i \in B$ $(i = 1, 2)$; n лежит в нормализаторе фиксированного максимального тора $T \subset B$. Тогда

$B \cap gBg^{-1} = b_1(B \cap nBn^{-1})b_1^{-1} \supset b_1Tb_1^{-1}$, так что тор $T_1 = b_1Tb_1^{-1}$ искомый.

Поскольку класс Bn_wB не зависит от выбора представителя n_w, то зачастую вместо Bn_wB пишут просто BwB, и тем самым группа Вейля W «параметризует» двойные смежные классы в разложении G по подгруппе Бореля B. Особо важную роль играет двойной смежный класс Bn_wB, отвечающий элементу максимальной длины $w \in W$ и называемый *«большой клеткой»*. А именно, пусть $B = B(\Pi)$, где $\Pi \subset R$ — система простых корней, и $w_0 \in W$ — элемент максимальной длины относительно систем образующих $S = \{w_\alpha | \alpha \in \Pi\}$. Тогда $w_0(R_+^\Pi) = -R_+^\Pi$ есть множество отрицательных корней в R и $w_0Bw_0^{-1} = B^-$, где $B^- = TU(-\Pi)$ и $U(-\Pi)$ есть подгруппа, порожденная U_α для всех отрицательных корней α. Положив для краткости $U = U(\Pi)$, $U^- = U(-\Pi)$, будем иметь $Bw_0B = UTU^-w_0$. Рассмотрим, далее, морфизм-произведение $U \times T \times U^- \xrightarrow{\varphi} G$. Вычисляя его дифференциал в единице и учитывая разложение $\mathfrak{g} = L(T) \oplus \left(\bigoplus_{\alpha \in R} \mathfrak{g}_\alpha\right)$, получим, что φ является доминантным, откуда следует, что «большая клетка» является открытым подмножеством в G. Более того, легко проверить, что морфизм φ инъективен, т. е. является бирациональным изоморфизмом, так что многообразие G рационально. Наконец, получаем, что $\dim G = \dim T + [R] = \dim T + 2l(w_0)$, где $l(w_0)$ — длина элемента w_0.

Пример. Пусть $G = GL_n(\Omega)$. Тогда $\mathfrak{g} = M_n(\Omega)$. В качестве максимального тора $T \subset G$ возьмем группу всех диагональных матриц. Обозначим через ε_i характер тора T, определяемый формулой ε_i: $t = \mathrm{diag}(t_1, \ldots, t_n) \longmapsto t_i$. Для любой матрицы $X = (x_{ij}) \in M_n(\Omega)$ и любого $t = \mathrm{diag}(t_1, \ldots, t_n) \in T$, очевидно, имеем $\mathrm{Ad}(t)(X) = (t_it_j^{-1}x_{ij})$, откуда следует, что $R(T, G) = \{\varepsilon_i - \varepsilon_j | i \neq j\}$. В качестве системы простых корней можно взять $\Pi = \{\varepsilon_i - \varepsilon_{i+1} | i = 1, \ldots, n-1\}$, и тогда $R_+^\Pi = \{\varepsilon_i - \varepsilon_j | i < j\}$. Легко проверить, что в этом случае борелевская подгруппа $B = B(\Pi)$ совпадает с группой всех верхних треугольных матриц. Нормализатор тора $N_G(T)$ есть группа мономиальных матриц, откуда следует, что группа Вейля $W(T, G)$ изоморфна симметрической группе S_n. В свою очередь, группа Вейля $W(R)$ также изоморфна S_n и действует на корни посредством перестановки индексов. Каноническая система образующих $W(R) = S_n$, отвечающая Π, состоит из транспозиций $(i, i+1)$, $i = 1, \ldots, n-1$. Элемент $w_0 \in W(R)$ максимальной длины преобразует i в $n - i + 1$. Группа $B^- = w_0Bw_0^{-1}$ есть группа всех нижних треугольных матриц, и произведение UTU^- состоит из матриц, у которых все главные миноры отличны от нуля.

11. Регулярные полупростые элементы. Пусть G — редуктивная алгебраическая группа, $T \subset G$ — ее максимальный тор и $R = R(T, G)$ — соответствующая система корней. Полупростой элемент $g \in G$ называется *регулярным*, если размерность $\dim Z_G(g)$ его централизатора совпадает с рангом группы G. В этом случае связная компонента $Z_G(g)^0$ является тором. Регулярные элементы существуют. Более того, элемент $t \in T$ регулярен в том и только том случае, если $\alpha(t) \neq 1$ для всех $\alpha \in R$, откуда следует, что регулярные элементы в T образуют открытое плотное подмножество $\Theta \subset T$. Рассматривая тогда морфизм $G \times \Theta \xrightarrow{\varphi} G$, $(g, \theta) \overset{\varphi}{\longmapsto} g\theta g^{-1}$, и проводя подсчет размерностей, получаем, что множество полупростых регулярных элементов является открытым в G. Кроме того, прямое вычисление показывает, что дифференциал φ в любой точке сюръективен. Полупростой элемент $X \in L(G)$ называется *регулярным*, если его централизатор является алгеброй Ли некоторого тора. Свойства полупростых регулярных элементов в алгебре Ли аналогичны соответствующим свойствам для элементов в группе. В частности, они образуют непустое открытое подмножество в $L(G)$.

12. Параболические подгруппы. Пусть в дополнение к обозначениям и соглашениям предыдущего пункта $\Pi \subset R$ — система простых корней и $B = B(\Pi)$ — соответствующая борелевская подгруппа. Тогда из разложения Брюа и свойств группы Вейля W вытекает, что любая подгруппа $P \subset G$, содержащая B, имеет вид $P_\Delta = BW_\Delta B$, где W_Δ — подгруппа W, порожденная отражениями w_α, $\alpha \in \Delta$, для некоторого подмножества $\Delta \subset \Pi$. При этом $L(P_\Delta) = L(T) \oplus \left(\bigoplus_{\alpha \in \Theta} \mathfrak{g}_\alpha\right)$, где Θ есть объединение множества положительных корней R_+^Π и тех отрицательных, которые являются линейными комбинациями корней из Δ. Подгруппы вида P_Δ называются *стандартными параболическими подгруппами*. Из сопряженности подгрупп Бореля вытекает, что любая параболическая подгруппа в G сопряжена некоторой стандартной параболической подгруппе.

13. Полупростые группы. При описании структуры полупростых групп удобно использовать понятие *изогении*. Так мы называем сюръективный морфизм $f\colon G \to H$ алгебраических групп с конечным ядром. (Отметим, что в случае характеристики $p > 0$ класс допустимых с точки зрения классификации полупростых групп изогений приходится несколько ограничивать, вводя так называемые центральные изогении, которые характеризуются тем свойством, что для любой Ω-алгебры A ядро индуцированного морфизма $f_A\colon G_A \to H_A$ групп A-точек лежит в центре G_A. Так как в основном для нас случае характеристики нуль любая изогения центральна, то мы в дальнейшем не будем

вдаваться в тонкости, возникающие в положительной характеристике.) Говорят, что группа G является *почти прямым произведением* своих подгрупп $G_1, \ldots, G_r$, если морфизм-произведение $G_1 \times \ldots \times G_r \to G$ является изогенией. Связную некоммутативную алгебраическую группу G будем называть (*абсолютно*) *простой*, если она не имеет связных нормальных делителей (здесь мы отходим от традиционного термина «почти простая группа»).

Предложение 4. *Пусть G — полупростая группа, $G_i (i \in I)$ — минимальные связные нормальные делители группы G. Тогда множество I конечно (скажем, $I = \{1, \ldots, r\}$) и G является почти прямым произведением групп $G_1, \ldots, G_r$. В частности, группа G является почти прямым произведением простых групп.*

В действительности группы $G_i (i = 1, \ldots, r)$ непосредственно связаны с разложением $R = \bigcup_{i=1}^{r} R_i$ системы корней R группы G на неприводимые компоненты (см. Бурбаки [4], гл. VI), а именно, группа G_i порождается U_α для $\alpha \in R_i$. В общем случае почти прямое произведение заменить на прямое нельзя, однако мы сейчас опишем два случая, когда это возможно. Группа G называется *односвязной*, если любая (центральная) изогения $f\colon H \to G$, где группа H связна, является изоморфизмом. Группа G называется *присоединенной*, если любая (центральная) изогения $f\colon G \to H$ является изоморфизмом.

Теорема 6. *Пусть G — полупростая группа.*

1) *Существуют односвязная группа $\tilde{G}$, присоединенная группа $\bar{G}$ и (центральные) изогении $\pi\colon \tilde{G} \to G$, $\varphi\colon G \to \bar{G}$.*

2) *Односвязная либо присоединенная группа G является прямым произведением своих минимальных связных нормальных делителей, которые при этом также соответственно односвязны или присоединенны.*

3) *Если $R = R(T, G)$ — система корней группы G, $\Pi \subset R$ — некоторая система простых корней, то группа G односвязна (соответственно присоединенна), если в $X(T)$ существует такой базис $\{\lambda_\alpha | \alpha \in \Pi\}$, что $w_\alpha \lambda_\beta = \lambda_\beta - \delta_{\alpha\beta}\alpha$, где $\delta_{\alpha\beta}$ — символ Кронекера (соответственно Π порождает $\mathbf{X}(T)$).*

Пример. Пусть $G = SL_n(\Omega)$. Как и в предыдущем примере, устанавливается, что для диагонального подтора $T \subset G$ система корней $R = R(T, G)$ состоит из $\varepsilon_i - \varepsilon_j$, где $\varepsilon_i\colon t = \operatorname{diag}(t_1, \ldots, t_n) \mapsto t_i$, $\Pi = \{\varepsilon_i - \varepsilon_{i+1} | i = 1, \ldots, n-1\}$. Положим $\lambda_j(t) = t_1 \ldots t_j (j = 1, \ldots, n-1)$. Тогда $w_{\alpha_i}(\lambda_j) = \lambda_j - \delta_{ij}\alpha_i$, и следовательно, группа G односвязна.

Изогения $\pi\colon \tilde{G} \to G$ в п. 1 теоремы 6 называется *универсальным накрытием*, а $F = \operatorname{Ker} \pi$ — *фундаментальной группой группы G*. Итак, любая полупростая группа обладает универсальной накрывающей, которая является произведением простых

односвязных групп. Поэтому завершает классификацию полупростых групп с точностью до изогении

Теорема 7. *Простая односвязная алгебраическая группа с точностью до изоморфизма однозначно определяется своей системой корней.*

Система корней простой группы является неприводимой и приведенной и поэтому относится либо к одной из четырех классических серий A_n, B_n, C_n, D_n, либо к одной из пяти исключительных систем E_6, E_7, E_8, F_4, G_2. Систему корней удобно задавать соответствующей *диаграммой Дынкина*, причем список возможных диаграмм выглядит следующим образом:

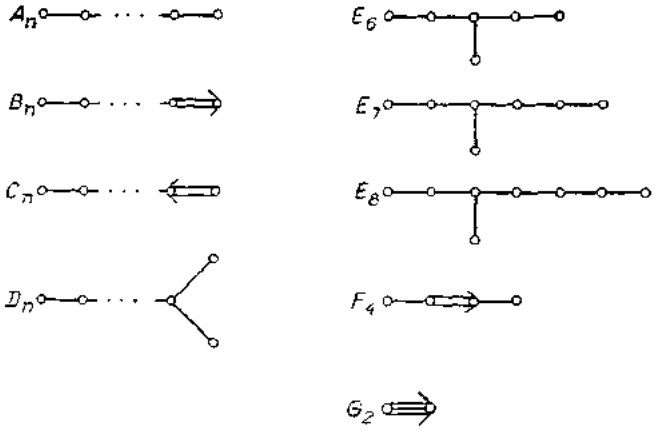


Диаграмма Дынкина полупростой группы является объединением диаграмм Дынкина простых компонент (пояснения см. в книге Бурбаки [4], гл. VI). Приведем также таблицу соответствующих односвязных групп для классических серий (см. подробнее § 2.3) и структуру центров простых групп, что дает полное описание простых групп.

Тип	Реализация	Структура центра
A_n	$\mathbf{SL}_{n+1}$	$\mathbb{Z}/(n+1)\mathbb{Z}$
B_n	$\mathbf{Spin}_{2n+1}$	$\mathbb{Z}/2\mathbb{Z}$
C_n	$\mathbf{Sp}_{2n}$	$\mathbb{Z}/2\mathbb{Z}$
D_n	$\mathbf{Spin}_{2n}$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, n четно $\mathbb{Z}/4\mathbb{Z}$, n нечетно
E_6	—	$\mathbb{Z}/3\mathbb{Z}$
E_7	—	$\mathbb{Z}/2\mathbb{Z}$
E_8	—	$\{e\}$
F_4	—	$\{e\}$
G_2	—	$\{e\}$

В алгебре Ли $\mathfrak{g} = L(G)$ полупростой группы G можно выбрать так называемый *базис Шевалле*. А именно, существуют такие элементы $X_\alpha \in \mathfrak{g}_\alpha$ для $\alpha \in R$ и такие элементы $H_\alpha \in L(T)$ для $\alpha \in \Pi$, что $\{X_\alpha\}_{\alpha \in R} \cup \{H_\alpha\}_{\alpha \in \Pi}$ — базис алгебры $\mathfrak{g}$ и выполняются следующие соотношения:

$$
\begin{aligned}
&[H_\alpha, H_\beta] = 0, && \alpha, \beta \in \Pi,\\
&[H_\alpha, X_\beta] = c_{\alpha\beta} X_\beta, && c_{\alpha\beta} \in \mathbb{Z}, \quad \alpha \in \Pi, \quad \beta \in R,\\
&[X_\alpha, X_{-\alpha}] = H_\alpha, && \alpha \in \Pi,\\
&[X_\alpha, X_\beta] = d_{\alpha\beta} X_{\alpha-\beta}, && d_{\alpha\beta} \in \mathbb{Z}, \quad \text{если} \quad \alpha + \beta \in R,\\
&[X_\alpha, X_\beta] = 0, && \text{если} \quad \beta \neq -\alpha \quad \text{и} \quad \alpha + \beta \notin R.
\end{aligned}
$$

Базис, удовлетворяющий этим свойствам (где $c_{\alpha\beta}$ и $d_{\alpha\beta}$ принимают значения, зависящие только от α, β и системы R, см. подробнее Стейнберг [2], теорема 1), определен однозначно с точностью до замены знаков у X_α и до автоморфизмов алгебры $\mathfrak{g}$.

При описании K-форм полупростой группы G нам понадобится знание структуры группы автоморфизмов $\operatorname{Aut} G$. Оказывается, что $\operatorname{Aut} G$ является полупрямым произведением группы внутренних автоморфизмов $\operatorname{Int} G$, которую можно отождествить с соответствующей присоединенной группой $\bar{G}$, и некоторой конечной группы, которую мы сейчас определим. Предположим вначале, что группа G односвязна. Тогда любая симметрия σ диаграммы Дынкина системы корней $R = R(T, G)$ индуцирует такой автоморфизм $f_\sigma \in \operatorname{Aut} G$, что $f_\sigma(T) = T$, $f_\sigma(B) = B$ и $d_e f_\sigma(X_\alpha) = X_{\sigma\alpha}$, где $\alpha \in \Pi$ и X_α — соответствующий элемент базиса Шевалле алгебры Ли $\mathfrak{g}$. При этом соответствие $\sigma \longmapsto f_\sigma$ задает вложение группы $\operatorname{Sym}(R)$ симметрий диаграммы Дынкина системы корней R в $\operatorname{Aut} G$, образ которого мы будем также обозначать через $\operatorname{Sym}(R)$.

Теорема 8. *Группа автоморфизмов* $\operatorname{Aut} G$ *односвязной полупростой группы* G *является полупрямым произведением* $\operatorname{Int} G \simeq \bar{G}$ *и* $\operatorname{Sym}(R)$. *Для произвольной полупростой группы* G *группа* $\operatorname{Aut} G$ *изоморфна подгруппе группы* $\operatorname{Aut} \tilde{G}$ *соответствующей универсальной накрывающей* $\tilde{G} \xrightarrow{\pi} G$, *оставляющих инвариантной фундаментальную группу* $F = \operatorname{Ker} \pi$.

Мы изложили основные факты теории полупростых алгебраических групп над алгебраически замкнутым полем. Для полупростых групп, определенных над произвольным полем K, теория становится более сложной и не столь законченной (некоторые ее аспекты мы затронем в следующем пункте). Однако для полупростых K-разложимых групп теория развивается практически параллельно случаю алгебраически замкнутого

поля. В частности, для любой системы корней R существует такая односвязная полупростая K-разложимая группа G с максимальным K-разложимым тором $T \subset G$, что система корней $R(T, G)$ совпадает с R. Эту группу нам доставляет конструкция Шевалле (см. Стейнберг [2]). Вообще, теория полупростых K-разложимых групп фактически совпадает с теорией групп Шевалле, изложению которой посвящена цитированная книга Стейнберга. В соответствующей алгебре Ли $\mathfrak{g}$ можно выбрать базис Шевалле, лежащий в $\mathfrak{g}_K$. Группа автоморфизмов $\operatorname{Aut} G$ является определенным над K полупрямым произведением $\operatorname{Sym}(R) \cdot \bar{G}$, причем все автоморфизмы из $\operatorname{Sym}(R)$ определены над K. Любая K-разложимая полупростая группа G обладает определенным над K универсальным накрытием $\pi\colon \bar{G} \to G$.

14. Относительные системы корней. Пусть G — полупростая K-определенная группа, $S \subset G$ — максимальный K-разложимый тор. Размерность $\dim S$ называется *K-рангом* G и обозначается $\operatorname{rang}_K G$. Отметим, что все максимальные K-разложимые торы в G сопряжены с помощью элементов группы G_K, так что, в частности, K-ранг определен корректно. Группы, для которых $\operatorname{rang}_K G > 0$ (соответственно $\operatorname{rang}_K G = 0$), называются *$K$-изотропными* (соответственно *K-анизотропными*). Доказывается, что K-анизотропность G равносильна отсутствию в G_K неединичных унипотентных элементов. Для изотропных групп Борелем, Титсом [1] была построена структурная теория, которая по форме аналогична описанной выше теории для случая алгебраически замкнутого поля, однако приводит к более скромным результатам, а именно, позволяет определить структуру группы по модулю знания структуры так называемого *анизотропного ядра*. В основе теории, как и в абсолютном случае, лежит сопоставление группе некоторой системы корней. Для этого фиксируется максимальный K-разложимый тор S и рассматривается присоединенное действие S на $\mathfrak{g} = L(G)$. Для $\alpha \in \mathbf{X}(S)$ положим $\mathfrak{g}_\alpha = \{X \in \mathfrak{g} \mid \operatorname{Ad}(s)X = \alpha(s)X \ \forall s \in S\}$ и введем множество $R(S, G) = \{\alpha \in \mathbf{X}(S) \mid \alpha \neq 0 \text{ и } \mathfrak{g}_\alpha \neq 0\}$. Тогда имеет место разложение $\mathfrak{g} = L(Z(S)) \oplus \left(\bigoplus_{\alpha \in R(S, G)} \mathfrak{g}_\alpha\right)$, где $L(Z(S))$ — алгебра Ли централизатора $Z(S)$ тора S, совпадающая с весовым пространством веса 0, причем все весовые пространства $\mathfrak{g}_\alpha$ определены над K. Оказывается, что множество $R_K = R(S, G)$ образует систему корней в пространстве $V = X(S) \otimes_{\mathbb{Z}} \mathbb{R}$, которая называется системой относительных корней или системой K-корней. Отличие от абсолютного случая состоит в том, что пространства $\mathfrak{g}_\alpha (\alpha \in R_K)$, вообще говоря, не являются одномерными, а система корней R_K — приведенной. Группа Вейля $W(R_K)$ системы корней R_K может быть отождествлена с группой Вейля $W(S, G)$ группы G относительно тора S, которая определяется как факторгруппа

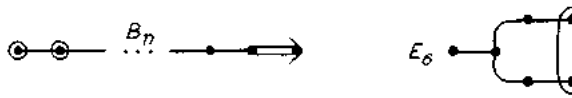
$N(S)/Z(S)$ нормализатора тора S по его централизатору; при этом любой элемент из $W(S, G)$ имеет представителя в $N(S)_K$. Если $\Pi \subset R_K$ — система простых корней, R_{+K}^{Π} — соответствующая система положительных корней, то группа $U(\Pi)$, порожденная U_α для $\alpha \in R_{+K}^{\Pi}$, где U_α — унипотентная подгруппа в G с алгеброй Ли $\mathfrak{g}_\alpha$, унипотентна, нормализуется группой $Z(S)$ и полупрямое произведение $P(\Pi) = Z(S)U(\Pi)$ является минимальной K-определенной параболической подгруппой. При этом соответствие $\Pi \to P(\Pi)$ задает биекцию между системами простых корней в R_K и минимальными K-определенными параболическими подгруппами в G, содержащими S. Полагая для краткости $P = P(\Pi)$ и $U = U(\Pi)$ и выбирая для каждого $w \in W(S, G)$ представителя $n_w \in N(S)_K$, получим разложение Брюа

$$G_K = \bigcup_{w \in W(S,\, G)} P_K n_w P_K,$$

причем $P_K n_w P_K = U_K n_w P_K$. Отметим, что в относительном случае связь между неприводимостью системы R_K и K-простотой группы G, т. е. отсутствием собственных связных K-определенных нормальных делителей, носит односторонний характер: если G K-проста, то система R_K неприводима.

Графически информацию о полупростой K-группе G удобно изображать в виде «оснащенной» диаграммы Дынкина — так называемого *индекса Титса*, метод построения которой мы сейчас опишем (см. Титс [2], Борель—Титс [1]). Рассмотрим максимальный K-разложимый тор $S \subset G$ и содержащий его максимальный K-определенный тор $T \subset G$. Пусть $R = R(T, G)$ — система корней группы G относительно тора T, $\Pi \subset R$ — подсистема простых корней. Поскольку группа G и тор T определены над K, группа Галуа $\mathcal{G} = \mathrm{Gal}(\bar{K}/K)$, действуя на $\mathbf{X}(T)$, индуцирует перестановку множества R. Определим индуцированное действие (так называемое *$*$-действие*) $\mathcal{G}$ на диаграмме Дынкина, вершины которой находятся в биективном соответствии с элементами множества Π. А именно, для $\sigma \in \mathcal{G}$ множество $\sigma(\Pi)$ является системой простых корней в $R = \sigma(R)$, и поэтому существует единственный элемент w из группы Вейля $W(R)$ такой, что $w(\sigma(\Pi)) = \Pi$; положим тогда $\sigma^* = w \circ \sigma\colon \Pi \to \Pi$. Группа G называется *внутренней* (соответственно *внешней*) формой, если $*$-действие тривиально (соответственно нетривиально). Далее, будем называть вершину диаграммы Дынкина *выделенной* (и обводить ее кружком), если ограничение соответствующего простого корня на S нетривиально. Кроме того, вершины диаграммы, принадлежащие одной орбите группы $\mathcal{G}$, располагаются «близко» друг к другу и, будучи выделенными, обводятся общим кружком). Диаграммы Дынкина с указанием

выделенных вершин и $*$-действия и называются *индексом Титса*. Например,



Принято также указывать порядок факторгруппы $\mathscr{G}$, эффективно действующей на П. Так, вторая диаграмма относится к типу ${}^2E_6$, а все внутренние формы — к типу ${}^1X$. Отметим, что если диаграмма не имеет симметрий (как, скажем, B_n), то любая K-группа этого типа автоматически является внутренней формой.

По индексу Титса легко найти диаграммы *анизотропного ядра* группы G (так мы называем коммутант централизатора $Z(S)$ максимального K-разложимого тора, который является полупростой K-анизотропной группой): для этого надо отбросить выделенные вершины с соответствующими связями. При этом, если все вершины выделенные, то группа G является квазиразложимой. Можно также найти максимальный K-разложимый тор S и соответствующую относительную систему корней. А именно, S выделяется в T уравнениями $\alpha(x)=1$, где α — невыделенный корень, и уравнениями $\alpha_1(x)=\ldots=\alpha_l(x)$, если $\alpha_1, \ldots, \alpha_l$ лежат в одной орбите $*$-действия. Отсюда следует, что если квазиразложимая группа является внутренней формой (в частности, если у соответствующей диаграммы нет симметрий), то она разложима. Относительные корни получаются ограничением на S корней из R, для которых это ограничение нетривиально. (Примеры соответствующих вычислений см. в гл. VI.)

§ 2.2. Классификация K-форм при помощи когомологий Галуа

1. L/K-формы. Пусть X — некоторый объект с K-структурой (K-определенное многообразие, K-определенная алгебраическая группа и т. д.), L/K — конечное расширение Галуа. Говорят, что K-объект Y является *L/K-формой* объекта X, если существует L-определенный изоморфизм $f\colon X\to Y$. Группа Галуа $\mathscr{F}=\mathrm{Gal}(L/K)$ естественным образом действует на L-морфизмах K-объектов, и для любого $\sigma\in\mathscr{F}$ морфизм $a_\sigma=f^{-1}\circ f^\sigma$ лежит в группе $\mathrm{Aut}_L(X)$ L-определенных автоморфизмов X, причем соответствие $\sigma\mapsto a_\sigma$ определяет (некоммутативный) 1-коцикл на $\mathscr{F}$ со значениями в группе $\mathrm{Aut}_L(X)$ (см. § 1.3, п. 2). Возникает отображение

$$F(L/K, X)\xrightarrow{\varphi} H^1(\mathscr{F}, \mathrm{Aut}_L(X))$$

множества классов K-изоморфных L/K-форм объекта X в множество одномерных когомологий.

Теорема 9. *Если X является аффинным K-многообразием либо алгебраической K-группой, то отображение φ биективно.*

Укажем на основные моменты доказательства (см. Воскресенский [3], гл. III). Вначале показывается, что φ корректно определено (т. е. не зависит ни от выбора L/K-формы Y в классе K-изоморфных, ни от выбора L-изоморфизма $f\colon X \to Y$) и инъективно. Эта часть рассуждений носит формальный характер и справедлива в гораздо более общей ситуации. Доказательство сюръективности φ требует более тонких соображений и основано на уже знакомой нам конструкции *скручивания*.

В § 1.3, п. 2 мы использовали это понятие для исследования точных последовательностей некоммутативных когомологий, но оказывается, что оно применимо и при доказательстве сюръективности φ. А именно, как и в п. 2 § 1.3, рассмотрим некоторую группу G, некоторую G-группу A и G-множество F, на котором действует A, причем это действие согласовано с действием группы G. Тогда для любого коцикла $a \in Z^1(G, A)$ определено «скрученное» множество ${}_aF$, которое с точностью до G-изоморфизма зависит лишь от класса эквивалентности a в $H^1(G, A)$. Положим $H = {}_aF$ и обозначим через $f\colon F \to H$ отображение, индуцированное тождественным отображением F. Тогда из определения ${}_aF$ вытекает, что коцикл $\{f^{-1} \circ f^s\}_{s \in G} \in Z^1(G, A)$ совпадает с исходным коциклом a. Отметим, однако, что если F обладает некоторой структурой (например алгебраического многообразия), то это абстрактное рассуждение требует дополнительных уточнений, связанных с доказательством того, что скрученный объект ${}_aF$ также обладает этой структурой. В ситуации, описанной в теореме 9, это получается рассмотрением алгебры регулярных функций. Поскольку аффинное алгебраическое многообразие определяется своей алгеброй регулярных функций, а задание структуры алгебраической группы равносильно заданию на алгебре регулярных функций структуры алгебры Хопфа (см. Борель [8]), то для построения L/K-формы X, отвечающей коциклу $a = \{a_\sigma\} \in H^1(\mathcal{F}, \mathrm{Aut}_L(G))$, следует рассмотреть алгебру L-определенных регулярных функций $A = L[X]$ и определить на ней новое действие группы $\mathcal{F}$ по формуле

$$\sigma'(f) = (\sigma \circ a_\sigma)^*(f),$$

где $(\sigma \circ a_\sigma)^*$ обозначает K-автоморфизм L-алгебры A, отвечающий $\sigma \circ a_\sigma$. Полученная таким образом L-алгебра B и будет служить алгеброй L-определенных регулярных функций на искомом многообразии Y. При этом Y будет обладать структурой алгебраической K-группы, если X обладало этой структурой. Допуская некоторую вольность речи, мы будем говорить, что H получено из G скручиванием при помощи коцикла a и писать $Y = {}_aX$.

Замечание. Теорема 9 остается справедливой и для проективных многообразий.

Пример 1. Пусть $X = \boldsymbol{G}_m$ — одномерный K-разложимый тор, $L = K(\sqrt{c})$ — квадратичное расширение K и τ — образующая группы Галуа $\mathscr{F} = \mathrm{Gal}(L/K)$. Рассмотрим коцикл $a = \{a_\sigma\} \in Z^1(\mathscr{F}, \mathrm{Aut}_L X)$ такой, что $a_e = \mathrm{id}_X$, $a_\tau = \theta$, где $\theta(x) = x^{-1}$ для всех $x \in X$. Тогда $A = L[X]$ есть $L[t, t^{-1}]$, $A_K = K[t, t^{-1}]$, причем автоморфизмы θ и σ действуют на A так:

$$\theta^*\colon f(t) + g(t^{-1}) \longmapsto f(t^{-1}) + g(t),$$
$$\sigma\colon f(t) + g(t^{-1}) \longmapsto f^\sigma(t) + g^\sigma(t^{-1}).$$

Отсюда следует, что на «скрученной» алгебре $B = L[t, t^{-1}]$ σ действует по формуле

$$\sigma\colon f(t) + g(t^{-1}) \overset{\sigma}{\longmapsto} f^\sigma(t^{-1}) + g^\sigma(t).$$

Прямое вычисление показывает, что K-алгебра $B_K = B^\sigma$ изоморфна $C = K[u, v]/(u^2 - cv^2 - 1)$ (u, v — независимые переменные), причем изоморфизм $C \to B_K$ осуществляется по формулам

$$u \longmapsto \frac{t + t^{-1}}{2}, \qquad v \longmapsto \frac{t - t^{-1}}{2\sqrt{c}}.$$

Но $C = K[Y]$, где $Y = \mathbf{R}^{(1)}_{L/K}(\boldsymbol{G}_m)$ — соответствующий норменный тор, причем указанный изоморфизм $C \simeq B_K$ согласован со структурами алгебр Хопфа на B_K и C. Таким образом, здесь ${}_aX = Y$.

Во многих случаях задание самого объекта X и K-структуры на нем определяется заданием множества K-точек X_K. (Примерами могут служить векторные пространства, векторные пространства с некоторыми тензорами, скажем, квадратичными формами, алгебры и т. д.) Тогда зачастую, допуская некоторую вольность речи, под «объектом» понимают множества X_K и под скрученным объектом — соответствующее множество Y_K. Такой «жаргон» имеет очевидные границы, в частности, он неприменим к алгебраическим многообразиям, ибо может, например, случиться, что $X_K = Y_K = \varnothing$, но X и Y не являются K-изоморфными, но в ряде случаев он эффективен и мы будем его использовать.

Пример 2. Пусть $V = K^2$ — двумерное векторное пространство над K, снабженное квадратичной формой f, которая в стандартном базисе e_1, e_2 имеет вид $f(x_1, x_2) = x_1x_2$. Снова рассмотрим квадратичное расширение $L = K(\sqrt{c})$, и пусть σ — образующая $\mathscr{F} = \mathrm{Gal}(L/K)$. Обозначим через $b = \{b_\tau\}$ следующий коцикл в $Z^1(\mathscr{F}, \boldsymbol{O}_2(f)_L)$, где $\boldsymbol{O}_2(f)$ — ортогональная группа формы f: $b_e = \mathrm{id}$, $b_\sigma = g$, где $g \in \boldsymbol{O}_2(f)$ переставляет e_1 и e_2. Рассмотрим пространство $V \otimes_K L$ и, скрутив его при помощи a,

положим $W = {}_a(V \otimes L)_K$. Прямое вычисление показывает, что K-базис пространства W образует векторы $u_1 = \frac{1}{2}(e_1 + e_2)$, $u_2 = \frac{1}{2}\sqrt{c}(e_1 - e_2)$, причем в этом базисе форма f (точнее, ее продолжение на $V \otimes_K L$) имеет вид $f(y_1, y_2) = y_1^2 - cy_2^2$. Таким образом, в результате скручивания квадратичного пространства (V, f) получается квадратичное пространство (W, h), где h имеет вид $h(y_1, y_2) = y_1^2 - cy_2^2$. Отметим, что этот пример непосредственно связан с предыдущим, ибо $\boldsymbol{SO}_2(f) = \boldsymbol{G}_m$, $\boldsymbol{SO}_2(h) = \mathbf{R}^{(1)}_{L/K}(\boldsymbol{G}_m)$, и мы рекомендуем читателю самостоятельно проанализировать эту связь.

Пример 2 допускает следующее обобщение.

2. Пространства с тензорами. Рассмотрим пару (V, x), где V — конечномерное векторное пространство над K, а x — некоторый тензор на V типа (p, q), т. е. элемент $T^q_p(V) = T^p(V) \otimes \otimes T^q(V^*)$ (читатель, не знакомый с тензорами, может понимать под x некоторую билинейную форму на V, т. е. тензор типа $(0, 2)$; тензоры других типов нам в этой книге встречаться не будут). Для любого расширения Галуа L/K с группой Галуа $\mathscr{F}$ можно рассмотреть пространство $V_L = V \otimes_K L$ и тензор $x_L = x \otimes 1 \in T^p_q(V_L) = T^p_q(V) \otimes_K L$. Пара (W, y), где W — пространство над K той же размерности, что и V, $y \in T^p_q(W)$, называется L/K-формой (V, x), если существует изоморфизм $(V_L, x_L) \simeq (W_L, y_L)$. Как и в п. 1, возникает отображение

$$F(L/K, (V, x)) \xrightarrow{\varphi} H^1(L/K, \operatorname{Aut}_L(V_L, x_L)).$$

Предложение 5. *Отображение φ является биекцией.*

В доказательстве нуждается лишь сюръективность φ. Для этого используется

Лемма 2. $H^1(\mathscr{F}, GL_n(L)) = 1$ для любого $n \geqslant 1$. *В частности,* $H^1(\mathscr{F}, L^*) = 1$.

(Последнее утверждение известно как «теорема 90» Гильберта. Если L/K — циклическое расширение и σ — образующая его группы Галуа $\mathscr{F}$, то, используя описание $H^1(\mathscr{F}, L^*)$ в этом случае (см. § 1.3, п. 1), можно дать эквивалентную переформулировку, которой мы уже неоднократно пользовались в § 1.3—1.4: любой элемент $a \in L^*$ такой, что $N_{L/K}(a) = 1$, имеет вид $a = \sigma(b)/b$, где $b \in L^*$.)

Доказательство. Рассмотрим пространство $V = K^n$. Тогда $V_L = L^n$ с покоординатным действием группы $\mathscr{F} = \operatorname{Gal}(L/K)$. Пусть теперь $a = \{a_\sigma\}$ — 1-коцикл на $\mathscr{F}$ со значениями в $GL_n(L)$. Определим новое «скрученное» действие $\mathscr{F}$ на V_L, полагая для $\sigma \in \mathscr{F}$, $v \in V_L$

$$\sigma'(v) = a_\sigma \sigma(v),$$

и обозначим через U пространство неподвижных точек. Ясно, что для любого $v \in V_L$ вектор $b(v) = \sum_{\sigma \in \mathcal{F}} a_\sigma \sigma(v)$ лежит в U. Покажем, что векторы $b(v)$ порождают V_L над L, откуда, в частности, будет следовать, что $U \otimes_K L \simeq V_L$. Действительно, пусть u — линейная форма на V_L, аннулирующая все векторы $b(v)$. Тогда для любого $h \in L$ и любого $v \in V_L$ имеем

$$0 = u(b(hv)) = \sum \sigma(h) u(a_\sigma \sigma(v)),$$

так что из теоремы о линейной независимости характеров (см. Ленг [3]) вытекает, что $u(a_\sigma \sigma(v)) = 0$, откуда $u = 0$. Итак, можно выбрать векторы $v_1, \ldots, v_n \in V_L$ таким образом, что векторы $b(v_1), \ldots, b(v_n)$ будут линейно независимыми. Тогда, обозначив через c матрицу, переводящую канонический базис в векторы $v_1, \ldots, v_n$, получим невырожденную матрицу $b = \sum_\sigma a_\sigma \sigma(c)$, и прямой подсчет показывает, что $a_\sigma = b\sigma(b)^{-1}$, что и требовалось.

Пусть теперь $a = \{a_\sigma\}$ — произвольный коцикл на $\mathcal{F}$ со значениями в $\mathrm{Aut}_L(V_L, x_L)$. Поскольку последняя группа является подгруппой в $GL(V_L)$, то из леммы 2 вытекает существование такого $b \in GL(V_L)$, что $a_\sigma = b^{-1}\sigma(b)$. Продолжим b до автоморфизма $T_q^p(V_L)$ и покажем, что тензор $x' = b(x)$ лежит в $T_q^p(V)$. Для этого достаточно показать, что x' инвариантен относительно группы $\mathcal{F}$. Имеем

$$\sigma(x') = \sigma(b)(\sigma(x)) = \sigma(b)(x) = b(b^{-1}\sigma(b))(x) = ba_\sigma(x) = b(x) = x',$$

что и требовалось. Рассмотрим теперь K-пространство $W = b^{-1}(V_K)$ и обозначим через y тензор x', перенесенный на W. Тогда пара (W, y) отвечает коциклу a. Отметим, что в действительности W совпадает с пространством U, введенным при доказательстве леммы, а y — с ограничением x на W. При этом, как мы показали, y определен над K. Предложение доказано.

Рассматривая невырожденные билинейные симметрические (или, эквивалентно, квадратичные) формы на V, из предложения 5 получаем

Предложение 6. *Пусть f — невырожденная квадратичная форма на n-мерном векторном пространстве V над полем K. Тогда для любого расширения Галуа L/K с группой Галуа $\mathcal{F}$ элементы множества $H^1(\mathcal{F}, \boldsymbol{O}_n(f)_L)$, где $\boldsymbol{O}_n(f)$ — ортогональная группа формы f (см. § 2.3), находятся в биективном соответствии с классами эквивалентности над K тех квадратичных форм на V, которые L-эквивалентны f.*

Рассматривая невырожденные билинейные кососимметрические формы на V и учитывая, что все они эквивалентны над K (Бурбаки [1], гл. 9, § 5), получаем

Предложение 7. *Пусть f — невырожденная билинейная кососимметрическая форма на n-мерном векторном пространстве V над полем K. Тогда для любого расширения Галуа L/K имеем $H^1(\mathcal{F}, \mathbf{Sp}_n(f)_L) = 1$, где $\mathbf{Sp}_n(f)$ — симплектическая группа формы f (см. § 2.3).*

Имеются и другие применения предложения 5. В частности, структура алгебры на векторном пространстве задается тензором типа $(1, 2)$, так что L/K-формы алгебры A находятся в биективном соответствии с элементами множества $H^1(\mathcal{F}, \mathrm{Aut}_L(A_L))$, где $\mathrm{Aut}_L(A_L)$ — группа L-автоморфизмов алгебры $A_L = A \otimes_K L$. Полагая $A = M_n(K)$ и учитывая, что любой автоморфизм A_L внутренний, т. е. $\mathrm{Aut}_L(A_L) = PGL_n(L)$, получаем, что элементы множества $H^1(\mathcal{F}, PGL_n(L))$ взаимно однозначно соответствуют L/K-формам алгебры A, т. е. простым центральным алгебрам размерности n^2 над K, которые расщепляются полем L.

В приведенных примерах группы L-автоморфизмов являются группами L-точек алгебраических групп (это всегда так, если мы имеем дело с группами автоморфизмов тензора), поэтому мы специально рассмотрим

3. Когомологии алгебраических групп. Пусть G — алгебраическая группа, L/K — некоторое конечное расширение Галуа с группой Галуа $\mathcal{F}$. Тогда на группе L-точек G_L действует группа $\mathcal{F}$ и можно определить множество $H^1(\mathcal{F}, G_L)$, которое в дальнейшем будет обозначаться через $H^1(L/K, G)$. Если $M \supset L$ — два конечных расширения Галуа поля K, то определено отображение $H^1(M/K, G) \xrightarrow{\rho_L^M} H^1(L/K, G)$. Это позволяет распространить определение $H^1(L/K, G)$ на бесконечные расширения Галуа L/K. А именно, группа Галуа $\mathrm{Gal}(L/K)$ представляется в виде проективного предела $\varprojlim \mathrm{Gal}(L_i/K)$ групп Галуа конечных подрасширений, и тогда полагаем $H^1(L/K, G) = \varinjlim H^1(L_i/K, G)$, где индуктивный предел берется относительно системы отображений $\rho_{L_j}^{L_i}$ для $L_i \supset L_j$. Можно дать эквивалентное определение $H^1(L/K, G)$ в этом случае как множества непрерывных 1-когомологий проконечной группы $\mathrm{Gal}(L/K)$ с коэффициентами в дискретной группе G_L. При этом мы будем писать $H^1(K, G)$ вместо $H^1(\bar{K}/K, G)$.

Переходя к индуктивному пределу в теореме 9, получаем, что множество $H^1(K, G)$ в общем случае параметризует классы K-изоморфных $\bar{K}/K$-форм некоторого K-объекта X с группой автоморфизмов G, т. е. классы K-изоморфных объектов Y, которые становятся изоморфными X над $\bar{K}$. Отметим также, что для любой алгебраической K-группы G

$$H^0(K, G) = G_K.$$

Из точных последовательностей некоммутативных когомологий, описанных в § 1.3, как частный случай получаются аналогичные точные последовательности для когомологий Галуа алгебраических групп. В частности, точной последовательности $1 \to F \to G \to H \to 1$, состоящей из K-групп и K-гомоморфизмов, отвечает точная последовательность множеств с отмеченными элементами

$$1 \to F_K \to G_K \xrightarrow{\varphi} H_K \xrightarrow{\psi_K} H^1(K, F) \to H^1(K, G) \to H^1(K, H), \qquad (1)$$

где ψ_K — так называемое *кограничное отображение*. При этом если F лежит в центре G, то ψ_K является гомоморфизмом групп и определено отображение δ_K: $H^1(K, H) \to H^2(K, F)$, продолжающее точную последовательность (1) еще на один член:

$$\ldots \to H^1(K, H) \xrightarrow{\delta_K} H^2(K, F).$$

Приведем некоторые примеры вычисления когомологий алгебраических групп. Рассмотрим точную последовательность

$$1 \to \boldsymbol{SL}_n \to \boldsymbol{GL}_n \xrightarrow{d} \boldsymbol{G}_m \to 1,$$

где отображение d индуцировано определителем, и запишем для этого случая соответствующую точную когомологическую последовательность (1):

$$GL_n(K) \xrightarrow{d} K^* \to H^1(K, \boldsymbol{SL}_n) \to H^1(K, \boldsymbol{GL}_n). \qquad (2)$$

Из леммы 2 вытекает, что $H^1(K, \boldsymbol{GL}_n) = 1$. С другой стороны, отображение определителя det: $GL_n(K) \to K^*$ сюръективно. Поэтому из точности последовательности (2) вытекает

Лемма 3. $H^1(K, \boldsymbol{SL}_n) = 1$.

Далее, частный случай леммы 2 для $n = 1$ (теорема 90 Гильберта) утверждает, что $H^1(K, \boldsymbol{G}_m) = 1$. Тогда по лемме Шапиро $H^1(K, \mathbf{R}_{L/K}(\boldsymbol{G}_m)) = H^1(L, \boldsymbol{G}_m) = 1$ для любого конечного расширения L/K. Поэтому из определения квазиразложимого K-тора получается

Лемма 4. *Пусть T — квазиразложимый K-тор. Тогда $H^1(K, T) = 1$.*

Рассмотрим теперь точную последовательность

$$1 \to \mathbf{R}^{(1)}_{L/K}(\boldsymbol{G}_m) \to \mathbf{R}_{L/K}(\boldsymbol{G}_m) \xrightarrow{\varphi} \boldsymbol{G}_m \to 1,$$

где φ — норменное отображение. Переходя к когомологиям, будем иметь точную последовательность

$$L^* \xrightarrow{N_{L/K}} K^* \to H^1(K, \mathbf{R}^{(1)}_{L/K}(\boldsymbol{G}_m)) \to H^1(K, \mathbf{R}_{L/K}(\boldsymbol{G}_m)) = 1,$$

откуда следует

Лемма 5. $H^1(K, \mathbf{R}^{(1)}_{L/K}(\boldsymbol{G}_m)) \simeq K^*/N_{L/K}(L^*)$.

Обратимся теперь к точной последовательности

$$1 \to \mu_n \to \boldsymbol{G}_m \xrightarrow{[n]} \boldsymbol{G}_m \to 1, \tag{3}$$

где $[n]$ означает морфизм возведения в n-ю степень, $\mu_n = \operatorname{Ker}[n]$ — группа корней степени n из единицы. Из последовательности (3) получаем точные последовательности

$$K^* \xrightarrow{[n]} K^* \to H^1(K, \mu_n) \to H^1(K, \boldsymbol{G}_m) = 1$$

и

$$1 = H^1(K, \boldsymbol{G}_m) \to H^2(K, \mu_n) \to H^2(K, \boldsymbol{G}_m) \xrightarrow{[n]} H^2(K, \boldsymbol{G}_m). \tag{4}$$

Так как $H^1(K, \boldsymbol{G}_m) = 1$, а $H^2(K, \boldsymbol{G}_m)$ отождествляется с группой Брауэра $\operatorname{Br}(K)$, то из (4) получается

Лемма 6. $H^1(K, \mu_n) \simeq K^*/K^{*n}$, $H^2(K, \mu_n) = \operatorname{Br}(K)_n$ — *группа элементов из* $\operatorname{Br}(K)$ *экспоненты* n.

Наконец, если при доказательстве предложения 6 вместо леммы 2 использовать лемму 3, то получится следующая интерпретация множества 1-когомологий $H^1(K, \boldsymbol{SO}_n(f))$ специальной ортогональной группы $\boldsymbol{SO}_n(f)$ невырожденной квадратичной формы f (см. также § 6.6).

Предложение 8. *Элементы множества* $H^1(K, \boldsymbol{SO}_n(f))$ *находятся в биективном соответствии с классами* K*-эквивалентности тех квадратичных форм степени* n *над* K, *которые имеют тот же дискриминант, что и* f.

С другими примерами когомологических вычислений мы встретимся в гл. VI, специально посвященной когомологиям Галуа алгебраических групп, а сейчас завершим наше краткое знакомство с этой темой редукцией задачи вычисления когомологий связных групп к редуктивным группам.

Лемма 7. *Пусть* K — *поле характеристики нуль. Тогда для любой* K*-определенной унипотентной подгруппы* U *имеем* $H^1(K, U) = 1$.

Доказательство. Вначале установим аддитивную форму теоремы 90 Гильберта, которая утверждает, что $H^1(K, \boldsymbol{G}_a) = 1$, т. е. $H^1(\mathscr{F}, L) = 0$ для любого конечного расширения Галуа L/K с группой Галуа $\mathscr{F}$. Пусть $c \in L$ такой элемент, что след $\operatorname{Tr}_{L/K}(c)$ отличен от нуля. Для заданного 1-коцикла $a = \{a_\sigma\} \in Z^1(\mathscr{F}, L)$ положим

$$b = \frac{1}{\operatorname{Tr}_{L/K}(c)} \sum_{\tau \in \mathscr{F}} a_\tau \tau(c).$$

Тогда прямое вычисление показывает, что $a_\sigma = b - \sigma(b)$ для любого $\sigma \in \mathscr{F}$, т. е. коцикл a тривиален. В действительности, как следует из теоремы о нормальном базисе (см. Ленг [3], с. 260), L является индуцированным $\mathscr{F}$-модулем, и поэтому по лемме Шапиро $H^i(\mathscr{F}, L) = 0$ для всех $i \geqslant 1$. Для произвольной

унипотентной K-группы U доказательство проводится индукцией по $\dim U$. Рассматривая ряд, указанный в п. 8 § 2.1, найдем K-определенный нормальный делитель $W \subset U$, изоморфный $\boldsymbol{G}_a$. Тогда из точной последовательности

$$1 \to W \to U \to U/W \to 1$$

получаем точную когомологическую последовательность

$$H^1(K, W) \to H^1(K, U) \to H^1(K, U/W).$$

Так как тривиальность $H^1(K, W)$ доказана выше, а $H^1(K, U/W) = 1$ по предположению индукции, то $H^1(K, U) = 1$, что и требовалось.

Заметим, что утверждение леммы сохраняется для любого совершенного поля K, если предполагать группу U связной (доказательство при этом не изменяется). В общем случае (т. е. если U несвязна либо поле K не является совершенным), вообще говоря, $H^1(K, U) \neq 1$ (см. Серр [2], гл. III).

Предложение 9. *Пусть G — связная редуктивная группа, определенная над полем K нулевой характеристики, H — ее максимальная редуктивная K-подгруппа (см. теорему 3). Тогда вложение $H \subset G$ индуцирует биекцию $H^1(K, H) \xrightarrow{\sim} H^1(K, G)$.*

Доказательство. Пусть $G = HU$ — соответствующее разложение Леви, где $U = R_u(G)$ — унипотентный радикал G (см. п. 9 в § 2.1), и π: $G \to G/U = H$ — каноническое факторотображение. Тогда композиция $H \xrightarrow{\varphi} G \xrightarrow{\pi} H$, где φ — естественное вложение, является тождественным отображением, так что композиция соответствующих отображений когомологий

$$H^1(K, H) \xrightarrow{\varphi_*} H^1(K, G) \xrightarrow{\pi_*} H^1(K, H)$$

также является тождественным отображением. Поэтому для доказательства предложения достаточно убедиться в инъективности π_*. Отображение π_* входит в точную когомологическую последовательность

$$H^1(K, U) \to H^1(K, G) \xrightarrow{\pi_*} H^1(K, H), \tag{5}$$

которая соответствует точной последовательности $1 \to U \to G \to H \to 1$. Согласно лемме 7 $H^1(K, U) = 1$, поэтому из (5) вытекает, что π_* имеет тривиальное ядро. К сожалению, в некоммутативных когомологиях утверждать, что из тривиальности $\operatorname{Ker} \pi_*$ вытекает инъективность π_*, вообще говоря, нельзя. Здесь применяется стандартный прием, основанный на конструкции скручивания. А именно, пусть для $g, h \in Z^1(K, G)$ имеем $\pi_*(g) = \pi_*(h)$ (мы обозначаем теми же буквами соответствующие классы когомологий). Обозначим через ${}_gG$ (соответственно ${}_gU$) группу, получающуюся из G (соответственно U) скручиванием при помощи g, и пусть τ_g: $H^1(K, {}_gG) \to H^1(K, G)$ — со-

ответствующая биекция (см. лемму 1.5). Положим $F = {}_gG/{}_gU = {}_g(G/U)$ и рассмотрим последовательность, аналогичную (5),

$$H^1(K, {}_gU) \to H^1(K, {}_gG) \xrightarrow{g\pi_*} H^1(K, F). \tag{6}$$

Тогда очевидно, что $f = \tau_g^{-1}(h) \in \operatorname{Ker} {}_g\pi_*$. С другой стороны, группа ${}_gU$ изоморфна U над $\bar{K}$, и поэтому унипотентна, так что $H^1(K, {}_gU) = 1$ в силу леммы 7. Тогда из точности (6) получаем, что $\operatorname{Ker} {}_g\pi_*$ тривиально, и поэтому $f = 1$ и $g = h$. Предложение доказано,

4. Классификация K-форм алгебраических групп. Мы рассмотрим два частных случая: случай алгебраических торов и случай полупростых групп.

Пусть T — алгебраический d-мерный K-тор с полем разложения L, $\mathscr{F} = \operatorname{Gal}(L/K)$. Тогда имеет место L-определенный изоморфизм $T \simeq \boldsymbol{G}_m^d$. Тем самым все такие K-торы являются L/K-формами d-мерного K-разложимого тора $\boldsymbol{G}_m^d$. Поэтому согласно теореме 9 классы K-изоморфных таких торов находятся во взаимно однозначном соответствии с элементами множества $H^1(\mathscr{F}, \operatorname{Aut}_L(\boldsymbol{G}_m^d))$. Но из теоремы 1 вытекает, что $\operatorname{Aut}_L(\boldsymbol{G}_m^d) = \operatorname{Aut}_K(\boldsymbol{G}_m^d) \simeq \mathrm{GL}_d(\mathbb{Z})$, откуда следует, что указанные классы биективно соответствуют классам эквивалентности d-мерных целочисленных представлений $\mathscr{F}$. Например, если L/K — квадратичное расширение, то любой конечнопорожденный $\mathbb{Z}[\mathscr{F}]$-**модуль M без $\mathbb{Z}$-кручения представим в виде** $M = \mathbb{Z}^l \oplus \mathbb{Z}[\mathscr{G}]^m \oplus I^n$, где I — ядро пополняющего гомоморфизма $\mathbb{Z}[\mathscr{G}] \to \mathbb{Z}$, причем числа l, m и n определены однозначно. Поэтому любой K-определенный и L-разложимый тор T представим в виде $\boldsymbol{T} = \boldsymbol{G}_m^l \times \mathbf{R}_{L/K}(\boldsymbol{G}_m)^m \times \mathbf{R}_{L/K}^{(1)}(\boldsymbol{G})^n$ для некоторых однозначно определенных целых неотрицательных l, m, n, причем K-анизотропный тор из этого класса обязательно имеет вид $\boldsymbol{T} = \mathbf{R}_{L/K}^{(1)}(\boldsymbol{G}_m)^n$.

Перейдем теперь к полупростому случаю. Прежде всего показывается, что для любой полупростой K-группы G существует такая K-разложимая группа G_0, что $G \simeq G_0$ над $\bar{K}$. Для этого рассматривается универсальное K-определенное накрытие $\tilde{G} \xrightarrow{\pi} G$ (см. § 2.1, п. 13). Тогда существует $\bar{K}$-изоморфизм $\varphi: \tilde{G} \xrightarrow{\sim} \tilde{G}_0$ с K-разложимой односвязной группой G_0 того же типа, что и G, и для доказательства существования G_0 достаточно показать, что группа $\varphi(\operatorname{Ker}\pi)$ определена над K. Но центр Z группы $\tilde{G}_0$ содержится в максимальном K-разложимом торе, откуда следует, что группа Галуа действует на группе характеров $\boldsymbol{X}(Z)$ тривиально, и любая подгруппа в Z, в частности, $\varphi(\operatorname{Ker}\pi)$ определена над K. Таким образом, любая полупростая K-группа G получается из подходящей K-разложимой группы

G_0 путем скручивания при помощи коцикла из $H^1(K, \mathrm{Aut}_{\overline{K}}(G_0))$. Поскольку группа $\mathrm{Aut}_{\overline{K}}(G_0)$ отождествляется с подгруппой в $\mathrm{Aut}_{\overline{K}}(\tilde{G}_0)$, состоящей из элементов, оставляющих подгруппу $\mathrm{Ker}\,\pi$ инвариантной (теорема 8), то универсальное K-определенное накрытие $\tilde{G}_0 \to G_0$ можно скрутить при помощи любого элемента из $H^1(K, \mathrm{Aut}_{\overline{K}}(G_0))$. Отсюда получается

Предложение 10. *Пусть G — полупростая K-определенная группа. Тогда существует универсальное накрытие π: $\tilde{G} \to G$, определенное над K.*

В арифметической теории алгебраических групп факт существования универсального K-определенного накрытия для произвольной полупростой K-группы играет важную роль, ибо односвязные группы обладают в этой теории рядом замечательных свойств, перенесение которых на произвольные полупростые группы связано с рассмотрением универсальных накрытий и изучением соответствующих фундаментальных групп. К сожалению, для произвольных редуктивных групп «канонического» аналога универсального накрытия не существует, однако в ряде случаев заменой ему служат так называемые *специальные накрытия* (см. Сансюк [1]). Определенная над K изогения f: $H \to G$ редуктивных K-групп называется *специальным накрытием*, если группа H является прямым произведением полупростой односвязной K-группы D и некоторого квазиразложимого над K тора S. Простые примеры показывают, что редуктивная группа, вообще говоря, не обязана обладать специальным накрытием, однако справедливо следующее

Предложение 11. *Для произвольной редуктивной K-группы G найдется такое целое $m > 0$ и такой квазиразложимый над K тор T, что группа $G^m \times T$ обладает специальным накрытием.*

Доказательство. Согласно теореме 4 группа G является почти прямым произведением своей полупростой части D_1 и максимального центрального тора S_1. Используя предложение 3, найдем целое $m > 0$ и такой квазиразложимый над K тор T, что произведение $S_1^m \times T$ накрывается подходящим квазиразложимым тором S, т. е. существует K-определенная изогения $S \xrightarrow{\varphi} S_1^m \times T$. Рассмотрим также универсальное K-определенное накрытие $D \xrightarrow{\pi} D_1$ и положим $H = D^m \times S$. Тогда сквозное отображение

$$H = D^m \times S \xrightarrow{\pi^m \times \varphi} D_1^m \times S_1^m \times T \to (D_1 S_1)^m \times T = G^m \times T$$

и будет искомым накрытием.

В силу предложения 10 классификация полупростых K-групп сводится к односвязным. Из теоремы 6 вытекает, что односвязная K-группа является прямым произведением односвязных

K-простых групп (т. е. групп, не содержащих собственных связных K-определенных нормальных делителей), причем любая односвязная K-простая группа имеет вид $\mathbf{R}_{L/K}(G)$, где G — абсолютно простая L-определенная группа. Поэтому достаточно рассмотреть вопрос о K-формах абсолютно простых односвязных групп.

Пусть G — простая односвязная K-разложимая группа данного типа, $\bar{G} = G/Z(G)$ — соответствующая присоединенная группа. Отождествим $\bar{G}_{\bar{K}}$ группой $\mathrm{Int}_{\bar{K}} G$ внутренних автоморфизмов группы G. Тогда полная группа автоморфизмов $\mathrm{Aut}_{\bar{K}} G$ является определенным над K полупрямым произведением группы $\mathrm{Sym}(R)$ симметрий диаграммы Дынкина системы корней R группы G и группы $\bar{G}_{\bar{K}}$ (см. п. 13 § 2.1), причем группа Галуа $\mathscr{G} = \mathrm{Gal}(\bar{K}/K)$ действует на $\mathrm{Sym}(R)$ тривиально. Таким образом, имеем точную расщепляющуюся последовательность K-групп

$$1 \to \bar{G}_{\bar{K}} \to \mathrm{Aut}_{\bar{K}} G \underset{\psi}{\overset{\varphi}{\rightleftarrows}} \mathrm{Sym}(R) \to 1. \tag{7}$$

Из (7) получаем точную когомологическую последовательность

$$H^1(K, \bar{G}) \to H^1(K, \mathrm{Aut}_{\bar{K}} G) \underset{\beta}{\overset{\alpha}{\rightleftarrows}} H^1(K, \mathrm{Sym}(R)).$$

Поскольку $\mathrm{Sym}(R) = \mathrm{Sym}(R)_K$, то коцикл a на $\mathscr{G}$ со значениями в $\mathrm{Sym}(R)$ — это просто непрерывный гомоморфизм $\mathscr{G} \to \mathrm{Sym}(R)$, и $H^1(K, \mathrm{Sym}(R))$ есть множество классов сопряженности таких гомоморфизмов. Как известно, $\psi(\mathrm{Sym}(R)) \subset \mathrm{Aut}_{\bar{K}} G$ состоит из автоморфизмов, оставляющих инвариантными максимальный K-разложимый тор $T \subset G$ и содержащую его борелевскую K-подгруппу $B \subset G$. Поэтому для любого $a \in H^1(K, \mathrm{Sym}(R))$ K-форма группы, отвечающая коциклу $\beta(a) \in H^1(K, \mathrm{Aut}_{\bar{K}} G)$, обладает K-определенной подгруппой Борля, т. е. является квазиразложимой над K. Таким образом, для любого $a \in H^1(K, \mathrm{Sym}(R))$ слой $\alpha^{-1}(a)$ содержит квазиразложимую над K группу ${}_aG$, которая при этом определена однозначно с точностью до K-изоморфизма. Говорят также, что слой $\alpha^{-1}(a)$ состоит из групп одного и того же внутреннего типа. Это связано с тем обстоятельством, что слой $\alpha^{-1}(a)$ совпадает с образом отображения $H^1(K, {}_a\bar{G}) \to H^1(K, \mathrm{Aut}({}_aG)) \simeq H^1(K, \mathrm{Aut}_{\bar{K}} G)$, где последний изоморфизм есть «сдвиг» на $\beta(a)$ (см. п. 2 § 1.3), так что группы одного и того же внутреннего типа получаются из соответствующей квазиразложимой группы путем скручивания при помощи элемента из $H^1(K, \bar{G}_a)$, т. е. при помощи внутренних автоморфизмов. Слой α над тривиальным коциклом в $H^1(K, \mathrm{Sym}(R))$ состоит из так называемых внутренних форм группы G, причем легко видеть, что определение в точности

совпадает с определением внутренних форм из предыдущего параграфа. Внутренние формы и только они получаются из G путем скручивания при помощи элементов из $H^1(K, \bar{G})$. Используя эти результаты, мы в следующем параграфе получим явную классификацию групп классических типов.

§ 2.3. Классические группы

Цель этого параграфа — ввести алгебраические группы, группы рациональных точек которых совпадают с так называемыми классическими группами над телами, к числу которых относят специальную линейную группу, симплектическую, специальную ортогональную и специальную унитарную группы. Оказывается, что эти группы (за малыми исключениями) являются простыми алгебраическими группами и относятся к классическим типам A_n, B_n, C_n и D_n. Замечательно, что справедлив и обратный результат: практически любая группа классического типа (за исключением лишь групп типов ${}^3D_4$ и ${}^6D_4$ в обозначениях Титса [2]) с точностью до изогении совпадает с одной из упомянутых классических групп. Этот результат, принадлежащий А. Вейлю [3], к сожалению, до сих пор не излагался в монографической литературе (исключение составляют лишь записи лекций М. Кнезера [12]). Поэтому мы даем практически полные доказательства приводимых результатов. Рассуждения базируются на классификации K-форм при помощи когомологий Галуа и понятии скручивания.

1. Специальная линейная группа. Пусть D — некоторое конечномерное центральное тело индекса d над полем K, $n \geqslant 1$. Тогда алгебра $A = M_n(D)$ является простой и определен гомоморфизм приведенной нормы $\mathrm{Nrd}_{A/K}\colon A^* \to K^*$ (см. § 1.4, п. 1). Положим $\mathrm{SL}_n(D) = \{x \in A^* \mid \mathrm{Nrd}_{A/K}(x) = 1\}$ и покажем, что эта группа является группой K-точек алгебраической группы G, которую мы будем обозначать $\boldsymbol{SL}_n(D)$. Пусть $\rho\colon D \to \boldsymbol{M}_{d^2}(K)$ — регулярное представление тела D *). Образ $\rho(D)$, будучи линейным подпространством в $M_{d^2}(K)$, выделяется некоторой системой

$$f_k(x_{ij}) = 0, \quad i, j = 1, \ldots, d^2; \quad k = 1, \ldots, l,$$

линейных уравнений относительно элементов x_{ij} матрицы $x = (x_{ij})$ с коэффициентами из K. Используя стандартное отождествление $M_{nd^2}(K) \simeq M_n(M_{d^2}(K))$, обозначим через $\tilde{A}$ подмножество в $M_{nd^2}(K)$, состоящее из таких $x = (x_{ij}^{\alpha\beta})$ $(i, j = 1, \ldots, d^2;$ $\alpha, \beta = 1, \ldots, n)$, что

$$f_k(x_{ij}^{\alpha\beta}) = 0 \quad \text{для всех} \quad \alpha, \beta = 1, \ldots, n; \quad k = 1, \ldots, l. \qquad (1)$$

*) При котором элементу $x \in D$ отвечает матричная запись K-линейного преобразования $y \longmapsto xy$ тела D, рассматриваемого как d^2-мерное векторное пространство над K в некотором фиксированном K-базисе.

Легко видеть, что ρ задает отождествление A и $\tilde{A}$. Далее, известно (см. § 1.4, п. 1), что приведенная норма элемента $x \in A$ выражается в виде полинома с коэффициентами из K от координат x в некотором (эквивалентно, в произвольном) базисе A/K. Отсюда следует существование такого полинома $g(x_{ij}^{\alpha\beta})$ над K, что

$$\mathrm{Nrd}_{A/K}((x^{\alpha\beta})) = g(\rho(x^{\alpha\beta})) \quad (\alpha, \beta = 1, \ldots, n).$$

Тогда очевидно, что множество матриц $x = (x_{ij}^{\alpha\beta}) \in M_{nd^2}(K)$, удовлетворяющих (1) и уравнению

$$g(x_{ij}^{\alpha\beta}) = 1, \tag{2}$$

естественным образом отождествляется с $SL_n(D)$. Возьмем в качестве группы $G = \boldsymbol{SL}_n(D)$ множество решений уравнений (1), (2) в $M_{nd^2}(\Omega)$. Тогда G будет K-определенной алгебраической группой, множество K-точек которой совпадает с $SL_n(D)$. При этом, используя изоморфизмы $D \otimes_K \Omega \simeq M_d(\Omega)$, $A \otimes_K \Omega \simeq M_{nd}(\Omega)$, легко построить Ω-изоморфизм $G \simeq SL_{nd}(\Omega)$, откуда следует, что G является простой односвязной K-группой типа A_{nd-1}.

Предложение 12. *Для группы $G = \boldsymbol{SL}_n(D)$ имеем $\mathrm{rang}_K G = n - 1$. В частности, группа $H = \boldsymbol{SL}_1(D)$ является K-анизотропной.*

Доказательство. Обозначим через T множество матриц $x = (x_{ij}^{\alpha\beta}) \in G$ таких, что $x_{ij}^{\alpha\beta} = 0$, если $\alpha \neq \beta$, и $x^{\alpha\beta} = (x_{ij}^{\alpha\beta})_{i,j=1,\ldots,d^2}$ — скалярная матрица, если $\alpha = \beta$. Легко видеть, что T является K-разложимым тором в G размерности $n-1$. При этом централизатор $Z_G(T)$ состоит из матриц $x = (x_{ij}^{\alpha\beta}) \in G$ таких, что $x_{ij}^{\alpha\beta} = 0$ для $\alpha \neq \beta$. Отсюда следует, что группа $H^n = H \times \ldots \times H$, где $H = \boldsymbol{SL}_1(D)$, естественным образом вкладывается в $Z_G(T)$ и ограничение на H^n факторморфизма $Z_G(T) \to Z_G(T)/T$ является изогенией. Поэтому достаточно установить K-анизотропность H. Но любой максимальный K-определенный тор в H имеет вид $\mathbf{R}_{L/K}^{(1)}(\boldsymbol{G}_m)$, где $L \subset D$ — некоторое максимальное подполе, и поэтому K-анизотропен (см. § 2.1, п. 7). Предложение доказано.

Вычислим теперь когомологии группы $G = \boldsymbol{SL}_n(D)$. Для этого рассмотрим вначале алгебраическую группу $H = \boldsymbol{GL}_n(D)$, которая определяется как подгруппа группы $GL_{nd^2}(\Omega)$, высекаемая уравнениями (1). Тогда H имеет в качестве группы K-точек группу $GL_n(D)$ обратимых элементов алгебры $A = M_n(D)$ и над Ω изоморфна группе $GL_{nd}(\Omega)$. Аналогично лемме 2 доказывается

Лемма 8. *$H^1(K, \boldsymbol{GL}_n(D)) = 1$ для любого $n \geqslant 1$.*

Теперь когомологии G вычисляются при помощи точной последовательности

$$1 \to G \to H \xrightarrow{\varphi} \boldsymbol{G}_m \to 1, \tag{3}$$

где φ индуцировано приведенной нормой $\mathrm{Nrd}_{A/K}$. Последовательности (3) отвечает точная когомологическая последовательность

$$GL_n(D) \xrightarrow{\mathrm{Nrd}_{A/K}} K^* \to H^1(K, G) \to H^1(K, H) = 1,$$

из которой получается

Лемма 9. $H^1(K, \boldsymbol{SL}_n(D)) \simeq K^*/\mathrm{Nrd}_{A/K}(GL_n(D)) = K^*/\mathrm{Nrd}_{D/K} D^*$.

2. Симплектическая и ортогональная группы. Пусть $f(x, y)$ — невырожденная знакопеременная (соответственно, симметрическая) билинейная форма на n-мерном векторном пространстве $V = K^n$ над полем K, $\mathrm{char} K \neq 2$ (за определениями и основными свойствами билинейных и полуторалинейных форм мы отсылаем читателя к одной из следующих книг: Бурбаки [1], Дьедонне [2], Артин [1]). Отметим, что если f — невырожденная знакопеременная форма, то необходимо $n = 2m$ — четное число. Группа автоморфизмов формы f, т. е. таких линейных преобразований σ: $V \to V$, что

$$f(\sigma(x), \sigma(y)) = f(x, y) \quad \text{для всех} \quad x, y \in V,$$

в случае знакопеременной формы f называется *симплектической группой* и обозначается $Sp_{2m}(f)$, а в случае симметрической формы f — *ортогональной группой* и обозначается $O_n(f)$. (В силу известной биекции между симметрическими билинейными и квадратичными формами обычно ортогональную группу связывают не с симметрической билинейной, а с соответствующей квадратичной формой, и в этом случае пишут $f(x)$ вместо $f(x, x)$). Определитель преобразования из $Sp_{2m}(f)$ всегда равен единице, а преобразования из $O_n(f)$ равен ± 1, так что $SO_n(f) = \{\sigma \in O_n(f) \mid \det \sigma = 1\}$ является подгруппой индекса 2 в $O_n(f)$.

Пусть $e_1, \ldots, e_n$ — некоторый базис пространства V, $F = (f(e_i, e_j))$ — матрица формы f. Тогда, записывая преобразования в базисе $e_1, \ldots, e_n$, будем иметь

$$\begin{aligned} Sp_{2m}(F) &= \{g \in GL_{2m}(K) \mid {}^t g F g = F\}, \quad \text{причем} \quad {}^t F = -F, \\ O_n(F) &= \{g \in GL_n(K) \mid {}^t g F g = F\}, \quad \text{причем} \quad {}^t F = F, \\ SO_n(F) &= \{g \in O_n(f) \mid \det g = 1\}, \end{aligned} \tag{4}$$

где ^{t} обозначает операцию транспонирования матриц. Обозначим теперь через $\boldsymbol{Sp}_{2m}(F)$, $\boldsymbol{O}_n(F)$ и $\boldsymbol{SO}_n(F)$ множество матриц $g \in GL_n(\Omega)$, удовлетворяющих соответствующим условиям в (4). Тогда каждое из этих множеств является K-определенной

алгебраической группой, группа K-точек которой совпадает с соответствующей группой $Sp_n(F)$, $O_n(F)$ или $SO_n(F)$. (Иногда, допуская некоторую вольность в обозначениях, мы будем писать, например, $\boldsymbol{O}_n(F)$ вместо $\boldsymbol{O}_n(F)$.)

При замене базиса $e_1, \ldots, e_n$ на другой базис $e'_1, \ldots, e'_n$ матрица F меняется на эквивалентную матрицу $F' = {}^t xFx$, где x — матрица перехода, а $\boldsymbol{Sp}_{2m}(F') = x\boldsymbol{Sp}_{2m}(F)x^{-1}$ и т. д. С другой стороны, известно (см. Бурбаки [1]), что любая невырожденная кососимметрическая матрица $F \in M_{2m}(K)$ эквивалентна над K стандартной кососимметрической матрице

$$J = \begin{pmatrix} 0 & E_m \\ -E_m & 0 \end{pmatrix}, \tag{5}$$

так что имеет место K-определенный изоморфизм $\boldsymbol{Sp}_{2m}(F) \simeq \simeq \boldsymbol{Sp}_{2m}(J)$. Положим $T = \{t = \operatorname{diag}(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m) \in \in GL_{2m}(\Omega) \mid \alpha_i\beta_i = 1,\ i = 1, \ldots, m\}$. Легко видеть, что T является K-разложимым тором в $G = \boldsymbol{Sp}_{2m}(J)$, причем непосредственное вычисление показывает, что $Z_G(T) = T$. Тем самым группа G является K-разложимой, T — ее максимальным K-разложимым тором. Проводя аналогично рассуждениям в книге Бурбаки [4] анализ системы корней $R = R(T, G)$, получаем, что R является простой системой типа C_m. Кроме того, используя критерий односвязности (см. утверждение 3) теоремы 6), можно показать, что группа G односвязна. Таким образом, получено

Предложение 13. *Пусть $G = \boldsymbol{Sp}_{2m}(F)$ $(m \geqslant 1)$, где F — невырожденная кососимметрическая матрица. Тогда G является K-разложимой группой типа C_m.*

Аналогично, над $\bar{K}$ любая невырожденная симметрическая матрица эквивалентна одной из матриц

$$Q_1 = \begin{pmatrix} 0 & E_m \\ E_m & 0 \end{pmatrix}, \qquad n = 2m, \tag{6}$$

либо

$$Q_2 = \begin{pmatrix} 0 & & E_m & 0 \\ & & & \vdots \\ & & & \vdots \\ E_m & & 0 & 0 \\ 0 & \ldots & 0 & 1 \end{pmatrix}, \quad n = 2m + 1.$$

Тогда $T = \{t = \operatorname{diag}(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m) \mid \alpha_i\beta_i = 1,\ i = 1, \ldots, m\}$ (соответственно, $T = \{t = \operatorname{diag}(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_m, 1) \mid \alpha_i\beta_i = = 1,\ i = 1, \ldots, m\}$), является максимальным тором в $G = = \boldsymbol{SO}_n(Q_1)$ (соответственно, $G = \boldsymbol{SO}_n(Q_2)$) и соответствующая система корней $R = R(T, G)$ имеет тип $D_m (m \geqslant 2)$ в первом случае и тип $B_m (m \geqslant 1)$ во втором (группа $G = \boldsymbol{SO}_2(Q_1)$ является одномерным тором), см. Бурбаки [4]. Таким образом, при $n \geqslant 3$ группа $G = \boldsymbol{SO}_n(F)$ является полупростой (в

действительности простой, за исключением случая $n=4$, когда $D_2=A_1+A_1$) группой типа $B_{\frac{n-1}{2}}$ (n нечетно), либо $D_{\frac{n}{2}}$ (n четно). Группа G неодносвязна; ее универсальной K-определенной накрывающей является так называемая спинорная группа $\tilde{G}=\boldsymbol{Spin}_n(F)$, конструируемая при помощи алгебр Клиффорда (см. Бурбаки [1], Дьедонне [2]). Ядро $\Phi=\operatorname{Ker}\pi$ универсального K-определенного накрытия $\pi\colon \tilde{G}\to G$ имеет порядок 2 и состоит из $\{\pm 1\}$ в смысле соответствующей алгебры Клиффорда. Отсюда следует, что при $l\leqslant n$ имеет место коммутативная диаграмма универсальных накрытий

$$\begin{array}{ccc} \boldsymbol{Spin}_n & \to & \boldsymbol{SO}_n \\ \uparrow & & \uparrow \\ \boldsymbol{Spin}_l & \to & \boldsymbol{SO}_l \end{array}$$

причем вертикальные стрелки являются вложениями.

Предложение 14. *Пусть $G=\boldsymbol{SO}_n(F)$ $(n\geqslant 3)$, где F — невырожденная симметрическая матрица. Тогда G является неодносвязной полупростой K-группой типа $B_{\frac{n-1}{2}}$, если n нечетно, и типа $D_{\frac{n}{2}}$, если n четно. При этом* $\operatorname{rang}_K G$ *совпадает с индексом Витта соответствующей квадратичной формы f. В частности, группа G является K-анизотропной в том и только том случае, если анизотропна форма f.*

Нам осталось доказать лишь утверждение о K-ранге группы G. Для этого напомним, что *индексом Витта* формы f называется размерность максимального вполне изотропного подпространства $W\subset V=K^n$ (т. е. такого подпространства, что $f(x)=0$ для всех $x\in W$). Положим $l=\dim W$. Тогда форма f эквивалентна над K форме вида $x_1x_{l+1}+\ldots+x_lx_{2l}+f_0(x_{2l+1},\ldots,x_n)$, где f_0 — некоторая K-анизотропная форма, поэтому можно без ограничения общности считать, что сама форма f имеет такой вид. Пусть $T=\{t=\operatorname{diag}(\alpha_1,\ldots,\alpha_l,\beta_1,\ldots,\beta_l)\in GL_n(\bar{K})\mid \alpha_i\beta_i=1$ для $i=1,\ldots,l\}$ — l-мерный разложимый тор. Легко видеть, что $T\subset \boldsymbol{SO}_n(f)$, и прямое вычисление показывает, что $Z_G(T)\simeq \simeq T\times \boldsymbol{SO}_{n-2l}(f_0)$. Поэтому достаточно установить K-анизотропность группы $H=\boldsymbol{SO}_{n-2l}(f_0)$. Но если $S\subset H$ — нетривиальный K-разложимый тор, то существует ненулевой вектор $v\in K^{n-2l}$, являющийся собственным для S с ненулевым характером χ. Тогда для любого $s\in S$ имеем $f_0(v)=f_0(sv)=f_0(\chi(s)v)=\chi(s)^2f_0(v)$, откуда $f_0(v)=0$, что противоречит K-анизотропности f_0. Предложение 14 полностью доказано.

3. Унитарные группы. Вначале несколько слов об алгебрах с инволюциями. Пусть A — конечномерная (ассоциативная) алгебра над полем K, $L=Z(A)$ — центр A. *Инволюцией* τ алгебры A называется произвольный K-антиавтоморфизм $\tau\colon A\to A$

порядка 2. Говорят, что τ является *инволюцией первого рода*, если ее ограничение на центр тривиально, и *инволюцией второго рода* в противном случае. Алгебра A с инволюцией τ будет обозначаться (A, τ).

Приведем некоторые примеры инволюций:

1) $A = M_n(K)$, $\tau(x) = {}^t x$ — операция транспонирования матриц.

2) $A = M_n(K)$, $\tau(x) = J^t x J^{-1}$, где J задается соотношением (5).

3) $A = A_1 \oplus A_2$, $A_i = M_n(K)$, $\tau(x, y) = ({}^t y, {}^t x)$.

Наша цель — показать, что любая инволюция на простой алгебре при расширении поля до алгебраически замкнутого переходит в одну из указанных инволюций 1)—3). Итак, пусть (A, τ) — произвольная простая K-алгебра с инволюцией. Тогда ее центр L является полем. Всюду в дальнейшем мы будем считать, что K совпадает с подполем L^τ τ-инвариантных элементов центра.

Пусть σ — другая инволюция алгебры A, такая, что $\tau|_L = \sigma|_L$. Тогда $\varphi = \sigma\tau^{-1}$ является автоморфизмом алгебры A, тривиально действующим на центре, так что по теореме Сколема — Нётер $\varphi = \operatorname{Int} g$ для подходящего $g \in A^*$. В этом случае $\sigma(x) = g\tau(x)g^{-1}$, $x \in A$, и из условия $\sigma^2 = \mathrm{id}$ получаем, что $g\tau(g)^{-1} \in L$. Если теперь предположить, что τ — инволюция первого рода, т. е. $L = K$, то отсюда моментально получаем, что $\tau(g) = \pm g$. Если же τ — инволюция второго рода, то поскольку $N_{L/K}(g\tau(g)^{-1}) = g\tau(g)^{-1}\tau(g\tau(g)^{-1}) = 1$, в силу теоремы 90 Гильберта найдется $a \in L$ со свойством $g\tau(g)^{-1} = a\tau(a)^{-1}$. Тогда, заменяя g на ga^{-1}, можно считать, что $\tau(g) = g$. Таким образом, получена

Лемма 10. *Пусть τ и σ — две инволюции простой алгебры A, ограничения которых на центр A совпадают (так называемые центроинвариантные инволюции). Тогда для подходящего $g \in A^*$*

$$\sigma(x) = g\tau(x)g^{-1}, \quad x \in A, \tag{6}$$

причем $\tau(g) = \pm g$ в случае инволюций первого рода и $\tau(g) = g$ в случае инволюций второго рода. Обратно, для любой инволюции τ и любого $g \in A^*$ с описанными свойствами отображение σ, задаваемое (6), *будет инволюцией A.*

Пусть теперь (A, τ) — некоторая простая K-алгебра с инволюцией. Если τ — инволюция первого рода, то K совпадает с центром A, и поэтому $A \otimes_K \bar{K} \overset{\varphi}{\simeq} M_n(\bar{K})$. Покажем, что изоморфизм φ здесь можно выбрать таким образом, что $\bar{K}$-линейное продолжение τ (которое мы будем обозначать той же буквой) перейдет в одну из инволюций пунктов 1), 2).

Пусть σ — инволюция транспонирования матриц, $\nu = \varphi\tau\varphi^{-1}$. Применяя к инволюциям σ и ν лемму, получим существование

такого элемента $F \in GL_n(K)$, что ${}^tF = \pm F$ и $\nu(x) = F^t x F^{-1}$. Далее, существует такая матрица $B \in GL_n(\bar{K})$, что $F = B^t B$, если F — симметрическая, и $F = {}^tBJB$, если F — кососимметрическая. Тогда прямое вычисление показывает, что изоморфизм ψ: $A \otimes_K \bar{K} \simeq M_n(\bar{K})$, $\psi = \operatorname{Int} B^{-1} \circ \varphi$ обладает требуемым свойством.

Если τ — инволюция второго рода, то $[L:K] = 2$, так что $A \otimes_K \bar{K} = (A \otimes_K L) \otimes_L \bar{K} \overset{\varphi}{\simeq} M_n(\bar{K}) \oplus M_n(\bar{K})$. Здесь алгебра $A \otimes_K \bar{K}$ является не простой, а полупростой, однако доказательство леммы 10 проходит без каких-либо изменений. Рассуждая как и выше, мы построим такой изоморфизм ψ: $A \otimes_K \bar{K} \xrightarrow{\sim} M_n(\bar{K}) \oplus \oplus M_n(\bar{K})$, при котором инволюция τ переходит в инволюцию, описанную в пункте 3).

Пусть теперь $f(x, y)$ — невырожденная эрмитова или косоэрмитова полуторалинейная форма на m-мерном векторном пространстве $V = D^m$ над телом D, снабженным инволюцией τ, L — центр D, и $K = L^\tau$ — поле τ-инвариантных элементов. Группа автоморфизмов формы f называется *унитарной группой* и обозначается через $U_m(D, f)$, а ее подгруппа, состоящая из автоморфизмов с приведенной нормой 1, — *специальной унитарной группой* $SU_m(D, f)$. Пусть $e_1, \ldots, e_m$ — некоторый базис пространства V, $F = (f(e_i, e_j))$ — матрица формы f. Тогда в базисе $e_1, \ldots, e_m$

$$U_m(D, f) = \{g \in GL_m(D) \mid {}^*gFg = F\}, \quad \text{причем} \quad {}^*F = \pm F,$$
$$SU_m(D, f) = \{g \in U_m(D, f) \mid \operatorname{Nrd}_{M_m(D)/L}(g) = 1\},$$

где ${}^*g = (\tau(g^{\beta\alpha}))$, если $g = (g^{\alpha\beta})$ (отметим, что $*$ является инволюцией алгебры $A = M_n(D)$ того же рода, что и τ). Чтобы реализовать группы $U_m(D, f)$ и $SU_m(D, f)$ как группы K-рациональных точек некоторых алгебраических групп, следует, как и в п. 1, рассмотреть регулярное представление ρ: $D \to \to M_{ln^2}(K)$ тела D над K (n — индекс D, $l = [L:K]$) и соответствующие уравнения вида (1), определяющие D как подпространство в $M_{ln^2}(K)$. Пусть, далее, $\tilde{\tau}$: $M_{ln^2}(K) \to M_{ln^2}(K)$ — линейный автоморфизм, продолжающий инволюцию $\rho\tau\rho^{-1}$ на $\rho(D)$, и $\Phi = (\rho(f^{\alpha\beta}))$ — отвечающая $F = (f^{\alpha\beta})$ матрица из $M_{lmn^2}(K)$. Тогда образ $U_m(D, f)$ в $M_{lmn^2}(K)$ при гомоморфизме, индуцируемом ρ, состоит из матриц

$$g = (g_{ij}^{\alpha\beta}) \quad (\alpha, \beta = 1, \ldots, m;\ i, j = 1, \ldots, ln^2),$$

удовлетворяющих (1) и уравнению

$$(\tilde{\tau}(g_{ij}^{\beta\alpha}))\, \Phi\, (g_{ij}^{\alpha\beta}) = \Phi. \tag{7}$$

Соответственно образ $SU_m(D, f)$ задается уравнениями (1), (7) и уравнением вида (2). Рассмотрев решения этих уравнений

в $\bar{K}$, мы получим соответствующие K-определенные алгебраические группы $\boldsymbol{U}_m(D, f)$ и $\boldsymbol{SU}_m(D, f)$.

Чтобы исследовать структуру этих групп, положим $\sigma(x) = F^{-1} \cdot xF$. Тогда, в силу леммы 10, σ является инволюцией на матричной алгебре $\Lambda = M_m(D)$, причем $U_m(D, f) = \{g \in GL_m(D) \mid \sigma(g) g = E_m\}$, $SU_m(D, f) = \{g \in U_m(D, f) \mid \mathrm{Nrd}_{A/L}(g) = 1\}$. Выше мы показали, что в случае, когда τ — инволюция первого рода, можно выбрать изоморфизм $A \otimes_K \bar{K} \simeq M_{mn}(\bar{K})$ таким образом, что σ перейдет в одну из инволюций ν, указанных в 1) или 2). Тогда соответственно группы $\boldsymbol{U}_m(D, f) = \{g \in (A \otimes_K \bar{K})^* \mid \sigma(g) g = E_m\}$ и $\boldsymbol{SU}_m(D, f) = \{g \in \boldsymbol{U}_m(D, f) \mid \mathrm{Nrd}_{A \otimes_K \bar{K}/\bar{K}}(g) = 1\}$ перейдут в группы $G = \{g \in GL_{mn}(\bar{K}) \mid \nu(g) g = E_{mn}\}$ и $H = \{g \in SL_{mn}(\bar{K}) \mid \nu(g) g = E_{mn}\}$, которые есть не что иное, как ортогональная и специальная ортогональная группы, если ν описывается как в п. 1 (так называемая *инволюция первого типа*), и которые совпадают с симплектической группой, если ν описывается как в п. 2 (*инволюция второго типа*). Отметим, что существует инвариантное описание инволюций первого и второго типа: τ относится к первому (соответственно второму) типу, если $\dim_K D^\tau = \frac{n(n+1)}{2}$ $\left(\text{соответственно } \dim_K D^\tau = \frac{n(n-1)}{2}\right)$. При этом ν относится к тому же типу, что и τ, если матрица F эрмитова, и к противоположному типу, если она косоэрмитова.

Пусть теперь τ — инволюция второго рода. Тогда можно выбрать изоморфизм $A \otimes_K \bar{K} \simeq M_{mn}(\bar{K}) \oplus M_{mn}(\bar{K})$ таким образом, что τ перейдет в инволюцию ν, указанную в п. 3. При этом группы $\boldsymbol{U}_m(D, f)$ и $\boldsymbol{SU}_m(D, f)$ перейдут соответственно в группы

$$G = \{(X, Y) \in GL_{mn}(\bar{K}) \times GL_{mn}(\bar{K}) \mid (X, Y)({}^tY, {}^tX) = (E_{mn}, E_{mn})\},$$

$$H = \{(X, Y) \in SL_{mn}(\bar{K}) \times SL_{mn}(\bar{K}) \mid (X, Y)({}^tY, {}^tX) = (E_{mn}, E_{mn})\}.$$

Отсюда видно, что $G = \{(X, {}^tX^{-1}) \mid X \in GL_{mn}(\bar{K})\}$, $H = \{(X, {}^tX^{-1}) \mid X \in SL_{mn}(\bar{K})\}$, так что группы $\boldsymbol{U}_m(D, f)$, $\boldsymbol{SU}_m(D, f)$ изоморфны над $\bar{K}$ группам $GL_{mn}(\bar{K})$ и $SL_{mn}(\bar{K})$ соответственно.

Предложение 15. *Пусть $G = \boldsymbol{SU}_m(D, f)$, где D — тело индекса n с инволюцией τ, f — невырожденная эрмитова либо косоэрмитова форма. Тогда над полем $\bar{K}$*

1) *$G \simeq \boldsymbol{Sp}_{mn}$, т. е. является простой односвязной группой типа $C_{\frac{mn}{2}}$, если τ — инволюция первого рода первого типа, а форма f косоэрмитова, либо τ — инволюция первого рода второго типа, а форма f эрмитова;*

2) $G \simeq \boldsymbol{SO}_{mn}$, *т. е. является полупростой неодносвязной группой типа* $B_{\frac{mn-1}{2}}$ *или* $D_{\frac{mn}{2}}$ *(отметим, что тип B реализуется лишь в случае* $n=1$, *т. е.* $D=K$), *если* τ — *инволюция первого рода первого типа, а форма* f *эрмитова, либо* τ — *инволюция первого рода второго типа, а форма* f *косоэрмитова;*

3) $G \simeq \boldsymbol{SL}_{mn}$, *т. е. является простой односвязной группой типа* A_{mn-1}, *если* τ — *инволюция второго рода.*

При этом $\operatorname{rang}_K G$ *совпадает с индексом Витта формы* f, *т. е. размерностью максимального вполне изотропного подпространства в* D^m.

Отметим, что рассмотренные в п. 2 группы $\boldsymbol{SO}_n(F)$ и $\boldsymbol{Sp}_{2m}(F)$ можно трактовать как унитарные группы относительно тождественной инволюции тела $D=K$. Кроме того, когомологии унитарных групп вычисляются точно так же, как в предложении 6 вычислялись когомологии ортогональной группы. А именно, используя вместо леммы 2 лемму 8, мы приходим к следующему результату:

Предложение 16. *Элементы множества* $H^1(K, \boldsymbol{U}_m(D, f))$ *биективно соответствуют классам эквивалентности m-мерных невырожденных форм над D того же типа, что и f. При этом классы собственной эквивалентности (т. е. эквивалентности относительно группы* $SL_m(D)$) *таких форм, имеющих тот же дискриминант, что и f, биективно соответствуют элементам из*

$$\operatorname{Ker}(H^1(K, \boldsymbol{SU}_m(D, f))) \to H^1(K, \boldsymbol{SL}_m(D)).$$

Вместо того чтобы давать доказательство предложения 16 в духе предложений 6—8, укажем на то обстоятельство, что все эти утверждения вытекают из следующего общего принципа, обоснование которого получается из точной последовательности (6) в п. 2 § 1.3: если X — однородное K-определенное пространство алгебраической K-группы G (т. е. задано транзитивное K-определенное действие $G \times X \to X$), $x \in X_K$ — некоторая точка и $H = G(x)$ — ее стабилизатор (так что X можно отождествить с G/H), то орбиты группы G_K на X_K взаимно однозначно соответствуют элементам из $\operatorname{Ker}(H^1(K, H) \to H^1(K, G))$.

4. Группы классических типов. Наша цель — установить обращение предложения 15, а именно, показать, что любая простая K-группа классического типа, кроме ${}^3D_4$ и ${}^6D_4$, с точностью до изогении есть либо группа $\boldsymbol{SL}_m(D)$, либо одна из унитарных (в частности, симплектических или ортогональных) групп.

Разберем вначале внутренние формы типа A_{n-1}. Мы знаем, что односвязные группы этого типа получаются из $G = \boldsymbol{SL}_n$ путем скручивания при помощи коциклов из $H^1(K, \bar{G})$, где $\bar{G} = \boldsymbol{PSL}_n$. Но группа $\bar{G}$ является в то же время группой автоморфизмов полной матричной алгебры M_n и для любого коцикла $a = \{a_\sigma\} \in H^1(K, \bar{G})$ можно рассмотреть скрученную ал-

гебру $A = {}_aM_n$. Пусть $B = A^{\mathrm{Gal}(\bar{K}/K)}$ — множество неподвижных точек. Тогда $B \otimes_K \bar{K} \simeq M_n(\bar{K})$, откуда следует, что алгебра B является простой и поэтому имеет вид $B = M_m(D)$ для некоторого центрального тела над K индекса d, причем $md = n$. Как и при определении специальной линейной группы, рассмотрим регулярное представление $\rho\colon D \to M_{d^2}(K)$ и соответствующее представление $\psi\colon B \to M_{md^2}(K)$. Имеем цепочку изоморфизмов

$$M_n(\bar{K}) \overset{\varphi}{\simeq} B \otimes_K \bar{K} \overset{\psi}{\simeq} \psi(B) \otimes_K \bar{K}.$$

Тогда, поскольку изоморфизм ψ определен над K, имеем $(\psi\varphi)^{-1}(\psi\varphi)^\sigma = \varphi^{-1}\varphi^\sigma = a_\sigma$. С другой стороны, поскольку, по определению, $\mathrm{Nrd}_{B/K}(b) = \det(\varphi^{-1}(b))$ для $b \in B$, то ограничение $\psi\varphi$ на $SL_n(\bar{K})$ индуцирует изоморфизм $SL_n(\bar{K})$ и группы $\boldsymbol{SL}_m(D)$, построенной в п. 1. Таким образом, получено

Предложение 17. *Односвязными группами, относящимися к внутренним формам типа A_{n-1}, являются группы $\boldsymbol{SL}_m(D)$, где D — центральное тело индекса d над K и $n = md$.*

Займемся теперь внешними формами типа A_{n-1}. Эти формы получаются из $G = \boldsymbol{SL}_n$ скручиванием при помощи коцикла $a = \{a_\sigma\}$ из $H^1(K, \mathrm{Aut}\,G)$, не лежащего в $H^1(K, \bar{G})$ и, следовательно, имеющего нетривиальную проекцию в $H^1(K, \mathrm{Sym}\,R)$. Для системы корней R типа A_{n-1} $(n > 1)$ группа $\mathrm{Sym}\,R$ имеет порядок 2, причем соответствие $\alpha \mapsto -\alpha$, $\alpha \in R$, доставляет автоморфизм R, не лежащий в группе Вейля $W(R)$. Отсюда следует, что группа $\mathrm{Aut}\,G$ порождается $\bar{G}$ и автоморфизмом второго порядка $x \mapsto {}^tx^{-1}$. Как и выше, реализуем элементы $\mathrm{Aut}\,G$ в качестве автоморфизмов некоторой алгебры. Рассмотрим алгебру $A = M_n(K) \oplus M_n(K)$ с инволюцией τ: $\tau(X, Y) = ({}^tY, {}^tX)$ и вложение $GL_n \to A$, задаваемое формулой $X \to (X, {}^tX^{-1})$. Мы видели, что таким образом $\boldsymbol{GL}_n$ отождествляется с группой $\boldsymbol{U} = \{Z \in A \mid Z\tau(Z) = E\}$; обозначим также через $\boldsymbol{SU}$ образ $\boldsymbol{SL}_n$ при этом вложении. Покажем, что группа $\mathrm{Aut}\,G$ естественным образом отождествляется с группой тех автоморфизмов алгебры A, которые коммутируют с инволюцией τ. Из теоремы Сколема — Нётер вытекает, что группа автоморфизмов A порождается внутренними автоморфизмами и автоморфизмом $(X, Y) \to (Y, X)$, который, очевидно, перестановочен с τ. С другой стороны, если внутренний автоморфизм перестановочен с τ, то легко показать, что он индуцируется элементом из $\boldsymbol{SU}$. Отсюда следует, что ограничение этих автоморфизмов на $\boldsymbol{SU}$ индуцирует все автоморфизмы группы $\boldsymbol{SU}$, которую мы отождествляем с G, причем автоморфизм A определяется своим ограничением на $\boldsymbol{SU}$ однозначно.

Пусть теперь $a = \{a_\sigma\} \in H^1(K, \mathrm{Aut}_{\bar{K}}G)$ — произвольный коцикл, не лежащий в $H^1(K, \bar{G})$. Рассмотрим a как коцикл

в $H^1(K, \mathrm{Aut}_{\bar{K}} A)$ и построим скрученную алгебру $B = {}_a A$. Поскольку элементы a_σ перестановочны с инволюцией τ, алгебра B обладает инволюцией ν, перестановочной с действием $\mathrm{Gal}(\bar{K}/K)$. Положим $C = B^{\mathrm{Gal}(\bar{K}/K)}$, тогда ограничение ν на C индуцирует инволюцию θ алгебры C и существует изоморфизм алгебр с инволюциями

$$(A, \tau) \overset{\varphi}{\rightarrow} (C \otimes \bar{K}, \theta).$$

Выясним структуру алгебры C. Поскольку $C \otimes \bar{K} \simeq M_n(\bar{K}) \oplus \oplus M_n(\bar{K})$, алгебра C может быть либо прямой суммой двух простых центральных алгебр над K, либо простой центральной алгеброй над некоторым квадратичным расширением L поля K. Покажем, что в нашей ситуации реализуется вторая возможность. Действительно, $Z(C) = {}_a(\bar{K} \oplus \bar{K})^{\mathrm{Gal}(\bar{K}/K)}$. По условию коцикл в $H^1(K, \mathrm{Sym}\, R)$, являющийся образом a, нетривиален, т. е. является нетривиальным гомоморфизмом $\mathrm{Gal}(L/K) = \mathrm{Gal}(\bar{K}/K)/\mathrm{Gal}(\bar{K}/L)$ в $\mathrm{Sym}\, R$ для некоторого квадратичного расширения L/K. Тогда легко видеть, что действие $\mathrm{Gal}(\bar{K}/K)$ на ${}_a(\bar{K} \oplus \bar{K})$ совпадает с действием $\mathrm{Gal}(\bar{K}/K)$ на $L \otimes \bar{K}$ через второй сомножитель, откуда $Z(C) = L$. При этом, поскольку τ действует на $\bar{K} \oplus \bar{K}$ перестановкой слагаемых, ограничение θ на L нетривиально. Таким образом, C является простой алгеброй над L с инволюцией θ второго рода.

Далее, известно (см. Алберт [1]), что $C = M_m(D)$ для некоторой алгебры с делением D над L индекса d ($md = n$), наделенной такой инволюцией второго рода δ, что ограничения θ и δ на L совпадают. Тогда, в силу леммы 10, $\theta(x) = F^* x F^{-1}$, $x \in M_n(D)$, где ${}^*(x_{ij}) = (\delta(x_{ji}))$ и ${}^*F = F$. Рассмотрим эрмитову форму f на пространстве $V = D^m$, имеющую в каноническом базисе $e_1, \ldots, e_n$ матрицу F. Утверждается, что ${}_a G = \boldsymbol{SU}_m(D, f)$. Для этого рассмотрим регулярное представление ρ: $D \to M_{2d^2}(K)$ над K и соответствующее представление ψ: $C \to M_{2md^2}(K)$. Имеем цепочку изоморфизмов

$$(A, \tau) \overset{\varphi}{\rightarrow} (C \otimes_K \bar{K}, \theta) \overset{\psi}{\rightarrow} (\psi(C) \otimes \bar{K}, \psi \circ \theta \circ \psi^{-1}).$$

Тогда $(\psi\varphi)^{-1}(\psi\varphi)^\sigma = a_\sigma$, ибо φ определен над K. При этом композиция $\psi\varphi$ и указанное выше вложение $G \to A$ задают K-определенный изоморфизм $G \simeq \boldsymbol{SU}_m(D, f)$. Мы получили

Предложение 18. *Односвязными K-группами, относящимися к внешним формам типа ${}^2A_{n-1}$, являются группы $\boldsymbol{SU}_m(D, f)$, где D — тело индекса d, наделенное инволюцией второго рода τ, причем K совпадает с полем τ-инвариантных элементов центра D, f — невырожденная m-мерная эрмитова форма и $n = md$.*

Перейдем теперь к описанию K-форм типа C_n. Разложимой односвязной группой этого типа является группа $G = \boldsymbol{Sp}_{2n}(\bar{K}) = \{X \in GL_{2n}(\bar{K}) \mid {}^tXJX = J\}$, где J определяется соотношением (5). Рассмотрим инволюцию τ алгебры $A = M_{2n}(\bar{K})$, определенную формулой $\tau(X) = J^{-1}{}^tXJ$. (Эта инволюция является инволюцией первого рода второго типа.) Любой автоморфизм группы G является внутренним (см. теорему 8), так что любая форма группы G получается из G скручиванием при помощи коцикла $a = \{a_\sigma\} \in H^1(K, \bar{G})$. Ясно, что a_σ можно рассматривать как автоморфизм алгебры A, перестановочный с действием инволюции τ. Тогда, как и выше, заключаем, что скрученная алгебра $B = {}_aA$ обладает инволюцией ν, перестановочной с действием группы Галуа $\mathrm{Gal}(\bar{K}/K)$ и поэтому ограничение ν на алгебру неподвижных точек $C = B^{\mathrm{Gal}(\bar{K}/K)}$ индуцирует инволюцию θ последней. Имеем изоморфизм алгебр с инволюциями

$$(A, \tau) \simeq (C \otimes_K \bar{K}, \theta).$$

Алгебра C проста над K, так что $C = M_m(D)$ для некоторого центрального тела индекса d над K, $md = 2n$, обладающего инволюцией первого рода (см. Алберт [1]). Отметим, что последний факт легко следует из следующего критерия: алгебра E над K обладает инволюцией первого рода в том и только том случае, если она изоморфна противоположной алгебре E^0, в частности, простая алгебра обладает инволюцией первого рода тогда и только тогда, когда она представляет элемент порядка 2 в группе Брауэра. В нашей ситуации C обладает инволюцией первого рода, следовательно C, а вместе с ней и D, представляют элемент порядка 2 в группе Брауэра; но тогда D обладает инволюцией δ первого рода. По желанию, мы можем считать инволюцию δ инволюцией первого или второго типа (в самом деле, если δ имеет, скажем, первый тип, то инволюция δ', определяемая формулой $\delta'(x) = c\delta(x)c^{-1}$, где c — произвольный кососимметрический относительно δ обратимый элемент, относится ко второму типу; при этом соответствие $x \mapsto cx$ определяет биекцию между δ-симметрическими и δ'-кососимметрическими элементами в D). Из леммы 10 тогда получаем, что $\theta(x) = F^*xF^{-1}$, где $^*(x_{ij}) = (\delta(x_{ji}))$, $^*F = -F$, если инволюция δ — первого типа, и $^*F = F$, если инволюция δ — второго типа. Вводя теперь соответственно косоэрмитову, либо эрмитову форму f на пространстве $V = D^m$ с матрицей F и рассуждая, как и выше, мы получим, что ${}_aG = \boldsymbol{SU}_m(D, f)$. Таким образом, справедливо

Предложение 19. *Односвязными K-формами типа C_n являются группы $\boldsymbol{SU}_m(D, f)$, где D — центральное тело индекса d над K, наделенное инволюцией первого рода τ, а невырожденная*

форма f эрмитова, если τ имеет второй тип, и косоэрмитова, если τ имеет первый тип, $2n = md$.

Наконец, рассмотрим K-формы типов B_n и D_n, отличные от ${}^3D_4$ и ${}^6D_4$. Односвязной K-разложимой группой здесь является спинорная группа $\tilde{G} = \boldsymbol{Spin}_m(f)$, где f — квадратичная форма максимального индекса Витта над K (ее матрица F совпадает с одной из матриц Q_1, Q_2 в (6), в зависимости от того, является число m четным или нечетным). Нам, однако, будет удобнее работать с соответствующей ортогональной группой $G = \boldsymbol{SO}_m(f)$. Обозначим через π: $\tilde{G} \to G$ соответствующее универсальное накрытие. Выясним взаимоотношения между группами $\operatorname{Aut} G$ и $\operatorname{Aut} \tilde{G}$. Известно (см. § 2.1, теорема 8), что $\operatorname{Aut} G$ отождествляется с подгруппой в $\operatorname{Aut} \tilde{G}$, состоящей из элементов, оставляющих группу $\operatorname{Ker} \pi$ инвариантной. Если G относится к типу B_n, то $\operatorname{Ker} \pi = Z(G)$, откуда следует, что группы $\operatorname{Aut} G$ и $\operatorname{Aut} \tilde{G}$ совпадают. (Это вытекает также из того факта, что диаграмма Дынкина системы корней типа B_n не имеет нетривиальных симметрий, и поэтому все автоморфизмы здесь внутренние.) Пусть теперь G относится к типу D_n, т. е. m четно. В этом случае автоморфизм G, индуцируемый сопряжением при помощи матрицы из $\boldsymbol{O}_m(f) \setminus \boldsymbol{SO}_m(f)$, является внешним, так что $[\operatorname{Aut} G: \operatorname{Int} G] \geqslant 2$. С другой стороны, если $n \neq 4$, то соответствующая диаграмма Дынкина имеет в точности две симметрии, так что $[\operatorname{Aut} \tilde{G}: \operatorname{Int} \tilde{G}] = 2$. Таким образом, и в этом случае $\operatorname{Aut} G = \operatorname{Aut} \tilde{G}$, причем все автоморфизмы G индуцируются сопряжением при помощи элементов группы $\boldsymbol{O}_m(f)$. В оставшемся случае $n = 4$ группа симметрий диаграммы Дынкина системы типа D_4 изоморфна симметрической группе S_3. Тогда, исследуя действие S_3 на центре группы $\tilde{G}$, легко показать, что $\operatorname{Aut} G$ изоморфна подгруппе индекса 3 в $\operatorname{Aut} \tilde{G}$ и все такие подгруппы сопряжены в $\operatorname{Aut} \tilde{G}$. При этом опять все автоморфизмы G индуцируются сопряжениями из $\boldsymbol{O}_m(f)$.

Из этого обсуждения групп $\operatorname{Aut} G$ и $\operatorname{Aut} \tilde{G}$ вытекает, что если тип K-формы H группы $\tilde{G}$ отличен от ${}^3D_4$ и ${}^6D_4$, то она получается из $\tilde{G}$ скручиванием при помощи коцикла $a = (a_\sigma) \in H^1(K, \operatorname{Aut} G)$. В этом случае $H = {}_a\tilde{G}$ является универсальной накрывающей группы ${}_aG$. Таким образом, достаточно описать K-формы группы G. Дословно повторяя рассуждения, которые применялись нами для описания K-форм типа C_n, получим, что группа ${}_aG$ является специальной унитарной группой $\boldsymbol{SU}_l(D, f)$, где D — конечномерное центральное тело индекса d над K с инволюцией первого рода τ, а f — невырожденная эрмитова либо косоэрмитова форма на пространстве $V = D^l$ в зависимости от того, имеет τ соответственно первый тип или второй, $m = ld$. При этом, если мы имеем дело с группами типа B_n, то, с одной стороны, m должно быть нечетным, с другой — число d должно быть степенью двойки, ибо D имеет экс-

поненту 2 в $\mathrm{Br}(K)$. Поэтому $d=1$, т. е. $D=K$, $\tau=\mathrm{id}$ и f является обычной квадратичной формой.

Предложение 20. 1) *Односвязными K-формами типа B_n являются спинорные группы невырожденных квадратичных форм над K степени $m=2n+1$.*

2) *Односвязными K-формами типа D_n, отличными от ${}^3D_4$ и ${}^6D_4$, являются универсальные накрывающие специальных унитарных групп $\boldsymbol{SU}_l(D,f)$, где D — конечномерное центральное тело индекса d над K с инволюцией первого рода τ, а невырожденная форма f эрмитова, если τ имеет первый тип, и косоэрмитова, если τ имеет второй тип, $2n=ld$. (При $d=1$, $\tau=\mathrm{id}$ мы получаем спинорные группы $\boldsymbol{Spin}_{2n}(f)$ невырожденных квадратичных форм.)*

В случае, когда K является локальным полем либо полем алгебраических чисел, предыдущие результаты допускают существенное уточнение. Известно (см. Алберт [1]), что над локальным полем тела с инволюцией второго рода индекса $d>1$ отсутствуют. Поэтому здесь односвязные K-группы типа ${}^2A_{n-1}$ исчерпываются специальными унитарными группами $\boldsymbol{SU}_n(L,f)$, где L — квадратичное расширение K, f — невырожденная форма на $V=L^n$, эрмитова относительно нетривиального автоморфизма $\sigma\in\mathrm{Gal}(L/K)$. В ортогональном базисе $e_1,\ldots,e_n$ пространства V форма f запишется в виде

$$f(x_1,\ldots,x_n;\ y_1,\ldots,y_n)=a_1\sigma(x_1)y_1+\ldots+a_n\sigma(x_n)y_n,$$

где коэффициенты a_i удовлетворяют условию $\sigma(a_i)=a_i$, т. е. $a_i\in K$. В частности, полагая для краткости $f(x)=f(x,x)$, будем иметь

$$f(x_1,\ldots,x_n)=a_1N_{L/K}(x_1)+\ldots+a_nN_{L/K}(x_n).$$

Далее, известно (см. § 1.4—1.5), что над локальными полями и полями алгебраических чисел экспонента простой алгебры в группе Брауэра совпадает с ее индексом, поэтому тела с инволюцией первого рода являются телами кватернионов. Любое тело кватернионов D над K обладает канонической инволюцией τ, задаваемой в стандартном базисе $1,\ i,\ j,\ k$ тела D формулой $\tau(a_0+a_1i+a_2j+a_3k)=a_0-a_1i-a_2j-a_3k$ (см. Пирс [1]). В нашей классификации эта инволюция относится ко второму типу, причем множество D^τ симметрических элементов совпадает с центром K тела D. Отсюда следует, что любая эрмитова относительно τ форма f на пространстве $V=D^m$ в ортогональном базисе пространства V имеет вид

$$f(x_1,\ldots,x_n;\ y_1,\ldots,y_n)=\tau(x_1)a_1y_1+\ldots+\tau(x_n)a_ny_n. \quad (8)$$

Коэффициенты a_i здесь удовлетворяют соотношению $\tau(a_i)=a_i$, откуда $a_i\in K$. Поэтому

$$f(x_1,\ldots,x_n)=a_1\mathrm{Nrd}_{D/K}(x_1)+\ldots+a_n\mathrm{Nrd}_{D/K}(x_n).$$

Таким образом, любая односвязная K-группа типа C_n (где K — либо локально, либо есть поле алгебраических чисел) является специальной унитарной группой $\boldsymbol{SU}_n(D, f)$, отвечающей форме f вида (8).

Наконец, односвязные K-группы типа D_n, не изоморфные спинорным группам квадратичных форм, являются универсальными накрывающими специальных унитарных групп $\boldsymbol{SU}_n(D, f)$, где D — тело кватернионов над K с канонической инволюцией τ, f — невырожденная косоэрмитова форма на D^n.

Подводя итоги, мы для удобства ссылок выпишем список простых односвязных алгебраических K-групп классических типов для случая, когда K есть либо локальное поле, либо поле алгебраических чисел. Прежде всего это группы $G = \boldsymbol{SL}_m(D)$, где D — центральное тело над K индекса d, относящиеся к внутренним формам типа A_n, $n = md - 1$. Все остальные группы, за исключением ${}^3D_4$ и ${}^6D_4$, получаются из специальных унитарных групп $\boldsymbol{SU}_m(D, f)$. Точнее, любая односвязная K-группа G такого типа является универсальной накрывающей некоторой специальной унитарной группы $H = \boldsymbol{SU}_m(D, f)$, где D — тело индекса d с центром L, снабженное такой инволюцией τ, что поле L^τ неподвижных относительно τ элементов совпадает с K, f — невырожденная эрмитова либо косоэрмитова относительно τ форма на m-мерном пространстве W над телом D. В зависимости от D, τ и f имеются следующие возможности, при перечислении которых мы указываем также некоторое число m_0, которое будет возникать при работе с группами классических типов:

1) $[L:K] = 2$, т. е. τ — инволюция второго рода, и форма f — эрмитова. В этом случае $G = H$ является группой типа ${}^2A_n$, где $n = md - 1$ ($m_0 = 2$).

В остальных случаях $L = K$, т. е. τ — инволюция первого рода. Тогда тело D либо совпадает с K, либо является телом кватернионов над K, и тем самым продолжение списка классических групп имеет следующий вид:

2) $D = K$ и форма f — симметрическая. Тогда H является специальной ортогональной группой $\boldsymbol{SO}_m(f)$, а G — спинорной группой $G = \boldsymbol{Spin}_m(f)$, причем эти группы относятся к типу $B_{\frac{m-1}{2}}$ при нечетном m и к типу $D_{\frac{m}{2}}$ при четном m ($m_0 = 4$).

3) $D = K$ и форма f кососимметрическая. Тогда m четно и $G = H$ совпадает с симплектической группой $\boldsymbol{Sp}_m(f)$, которая относится к типу $C_{\frac{m}{2}}$ ($m_0 = 2$).

4) D — тело кватернионов над K, τ — его каноническая инволюция и форма f — эрмитова. Тогда $G = H$ — группа типа C_m ($m_0 = 1$).

5) при тех же D, τ, что и в п. 4), форма f — косоэрмитова. Тогда H является неодносвязной группой типа D_m, и $H \simeq \simeq SO_{2m}(\bar{f})$ над $\bar{K}$ $(m_0 = 3)$.

5. Теорема Витта. Сохраним обозначения G, H, f, W, ..., введенные в конце предыдущего пункта. Группа H действует на пространстве $\bar{W} = W \otimes_K \bar{K}$, сохраняя естественное продолжение формы f. Эта реализация группы H индуцирует реализацию группы G, которой мы будем свободно пользоваться без дополнительных пояснений, называя при этом m степенью группы G. В дальнейшем нам понадобится так называемая теорема Витта, которая описывает орбиты действия $U_m(D, f)$ на W (относительный вариант) и орбиты G на $\bar{W}$ (абсолютный вариант).

Теорема 10 (теорема Витта; относительный вариант). *Пусть $a, b \in W$ — два ненулевые вектора, такие, что $f(a) = f(b)$. Тогда существует такой элемент $g \in U_m(D, f)$, что $b = ga$.*

Доказательство — см. Бурбаки [1], гл. 9, с. 396—398. Отметим, что в действительности под теоремой Витта понимают обычно более общее утверждение о том, что любой метрический изоморфизм σ: $U_1 \to U_2$ между двумя подпространствами U_1, $U_2 \subset W$ продолжается до изометрии всего пространства W, т. е. индуцируется элементом из $U_m(D, f)$.

Если исключить пункт 3) в приведенном выше списке из рассмотрения, то в пространстве W всегда существует ортогональный относительно формы f базис. В частности, всегда существует такой вектор $a \in W$, что $f(a) \neq 0$ (анизотропный вектор).

Теорема 11 (теорема Витта; абсолютный вариант). *Пусть $m \geqslant 2$ и $a \in W$ — анизотропный вектор. Тогда для любого $b \in \bar{W}$, такого, что $f(b) = f(a)$, найдется $g \in G$ со свойством $b = ga$.*

Доказательство. Достаточно найти $h \in H$ со свойством $b = ha$. В ситуации п. 2 существование h непосредственно вытекает из теоремы 10, примененной к пространству $\bar{W}$ над полем $\bar{K}$, и предположения о том, что $m \geqslant 2$. Разберем теперь случаи, описанные в пунктах 4)—5). Для этого включим a в ортогональный базис $e_1 = a$, e_2, ..., e_m пространства W и будем в дальнейшем рассматривать координаты относительно этого базиса. Если $f(e_i) = d_i$, то форма f имеет в этом базисе вид

$$f(x_1, \ldots, x_m) = \tau(x_1) d_1 x_1 + \ldots + \tau(x_m) d_m x_m.$$

Выберем далее кососимметрический элемент $c \in D^*$ и перейдем от инволюции τ к инволюции σ, задаваемой формулой $\sigma(d) = c\tau(d)c^{-1}$. Тогда σ имеет первый тип, и поэтому можно выбрать изоморфизм $\bar{D} = D \otimes_K \bar{K} \xrightarrow{\sim} M_2(\bar{K})$ таким образом, что инволюция σ перейдет в операцию транспонирования матриц. Легко видеть, что для $d \in D$ равенства $\tau(d) = \pm d$ и $\sigma(cd) =$

$= \mp cd$ равносильны, поэтому элементам cd_i отвечают симметрические в случае 5) и кососимметрические в случае 4) матрицы $D_i \in \mathrm{GL}_2(\bar{K})$. Если $b = (b_1, \ldots, b_m)$, причем элементам $b_i \in \bar{D}$ отвечают матрицы $B_i \in M_2(\bar{K})$, то

$$ {}^tB_1D_1B_1 + \ldots + {}^tB_mD_mB_m = D_1. \tag{9} $$

Мы знаем, что при изоморфизме $\bar{D} \simeq M_2(\bar{K})$ группа H перейдет соответственно в $\tilde{H} = \boldsymbol{SO}_{2m}(\tilde{f})$ или $\tilde{H} = \boldsymbol{Sp}_{2m}(\tilde{f})$, где матрица формы $\tilde{f}$ имеет вид $\mathrm{diag}(D_1, \ldots, D_m)$. Пусть $B_i = \begin{pmatrix} b_{11}^{(i)} & b_{12}^{(i)} \\ b_{21}^{(i)} & b_{22}^{(i)} \end{pmatrix}$. Тогда из (9) вытекает изометричность относительно формы $\tilde{f}$ подпространства, порожденного первыми двумя координатными векторами $u_1, u_2 \in \bar{K}^{2m}$, и подпространства, порожденного векторами $w_1 = (b_{11}^{(1)}, b_{21}^{(1)}, \ldots, b_{11}^{(m)}, b_{21}^{(m)})$ и $w_2 = (b_{12}^{(1)}, b_{22}^{(1)}, \ldots, b_{12}^{(m)}, b_{22}^{(m)})$. Поэтому из теоремы Витта для подпространств вытекает существование такого $\tilde{h} \in \tilde{H}$, что $\tilde{h}(u_i) = w_i$ $(i = 1, 2)$, или, в матричной записи, $\tilde{h}(E_2, 0, \ldots, 0) = (B_1, \ldots, B_m)$. Последнее означает, что отвечающий $\tilde{h}$ элемент $h \in H$ обладает свойством $ha = b$, что и требовалось.

В случае 1) рассуждения аналогичны, но имеют несколько другой характер. Опять, пусть $e_1 = a, e_2, \ldots, e_m$ — ортогональный базис пространства W, причем $f(e_i) = d_i$ так, что $f(x_1, \ldots, x_m) = \tau(x_1)d_1x_1 + \ldots + \tau(x_m)d_mx_m$. Выберем изоморфизм $D \otimes_K \bar{K} \simeq M_d(\bar{K}) \oplus M_d(\bar{K})$ таким образом, чтобы инволюции τ отвечала инволюция $(X, Y) \to ({}^tY, {}^tX)$ (см. п. 3), которую мы также будем обозначать через τ. Пусть $d_i = (C_i, {}^tC_i)$, $b = (b_1, \ldots, b_m)$ и $b_i = (B_i^{(1)}, B_i^{(2)})$. Тогда соотношение $f(b) = f(a)$ может быть записано в виде двух эквивалентных матричных равенств

$$ \begin{aligned} {}^tB_1^{(1)}C_1B_1^{(2)} + \ldots + {}^tB_m^{(1)}C_mB_m^{(2)} &= C_1, \\ {}^tB_1^{(2)}{}^tC_1B_1^{(1)} + \ldots + {}^tB_m^{(2)}{}^tC_mB_m^{(1)} &= {}^tC_1. \end{aligned} \tag{10} $$

Группе H при этом отвечает группа $\tilde{H} = \{(X, {}^tC^{-1}\,{}^tX^{-1}\,{}^tC) \mid X \in SL_n(\bar{K})\}$, где $n = md$, $C = \mathrm{diag}(C_1, \ldots, C_m)$ и $M_n(\bar{K})$ отождествляется с $M_m(M_d(\bar{K}))$. Поэтому нам нужно показать, что если $B_i^{(1)}, B_i^{(2)}$ удовлетворяют (10), то найдется $X \in SL_n(\bar{K})$ со свойствами

$$ X\begin{pmatrix} E_d \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} B_1^{(1)} \\ \vdots \\ B_m^{(1)} \end{pmatrix}, \quad ({}^tC^{-1}\,{}^tX^{-1}\,{}^tC)\begin{pmatrix} E_d \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} B_1^{(2)} \\ \vdots \\ B_m^{(2)} \end{pmatrix}. \tag{11} $$

Второе уравнение в (11) можно переписать в виде

$$ {}^tX \begin{pmatrix} {}^tC_1B_1^{(2)} \\ \vdots \\ {}^tC_mB_m^{(2)} \end{pmatrix} = \begin{pmatrix} {}^tC_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{12} $$

Первому уравнению в (11) удовлетворяют в точности матрицы

$$ X = \begin{pmatrix} B_1^{(1)} & X_{12} & \dots & X_{1m} \\ \dots & \dots & \dots & \dots \\ B_m^{(1)} & X_{m2} & \dots & X_{mm} \end{pmatrix} $$

с произвольными X_{ij}, $1 \leqslant i \leqslant m$, $2 \leqslant j \leqslant m$. Учитывая (10), получаем, что такая матрица удовлетворяет (12) в том и только том случае, если

$$ X_{1i}{}^tC_1B_1^{(2)} + \dots + X_{mi}{}^tC_mB_m^{(2)} = 0, \quad i = 2, \dots, m. \tag{13} $$

Учитывая, что (13) сводится к m линейным уравнениям на каждый столбец матрицы X, начиная с $(m+1)$-го, легко видеть, что существует решение (13), удовлетворяющее условию

$$ \operatorname{rang} \begin{pmatrix} X_{12} & \dots & X_{1m} \\ \dots & \dots & \dots \\ X_{m2} & \dots & X_{mm} \end{pmatrix} = n - m. $$

Тогда в силу невырожденности C_1 матрица X также будет невырожденной. Более того, используя однородность (13) и условие $m \geqslant 2$, можно добиться, чтобы в действительности $X \in SL_n(K)$. Теорема 11 доказана.

Замечание. Поскольку в ситуации п. 4 списка классических групп $\boldsymbol{U}_m(D, f) = \boldsymbol{SU}_m(D, f)$ для всех $m \geqslant 1$, утверждение теоремы 11 в этом случае сохраняет силу и при $m = 1$.

Таким образом, во всех рассматриваемых случаях «сфера» $X_{(f,a)} = \{x \in \overline{W} \mid f(x) = f(a)\}$ является однородным пространством группы G, и поэтому может быть отождествлена с $G/G(a)$, где $G(a)$ — стабилизатор a. В дальнейшем нам понадобится информация о стабилизаторах $G(a)$ векторов $a \in W$ и стабилизаторах $G(a, b)$ пар векторов $a, b \in W$.

Предложение 21. *Если $m \geqslant m_0$, то для любого анизотропного вектора $a \in W$ стабилизатор $G(a)$ относится к тому же типу, что и исходная группа G, и является полупростой односвязной группой (мы не исключаем случай $G(a) = (e)$). Следовательно, если $m \geqslant m_0 + 1$, то аналогичными свойствами обладает стабилизатор произвольной пары векторов $G(a, b)$, порождающих невырожденное двумерное подпространство.*

Доказательство. Легко видеть, что для анизотропного $a \in W$ стабилизатор $H(a)$ совпадает с группой $\boldsymbol{SU}_{m-1}(D, g)$, где g — ограничение f на ортогональное дополнение к x. С другой стороны, группа $G(a)$ совпадает с прообразом $H(a)$ при универ-

сальном накрытии π: $G \to H$. Из проведенного выше исследования групп классических типов вытекает, что при наших ограничениях на m группа $H(a)$ полупроста, поэтому остается проверить, что $\pi|_{G(a)}$: $G(a) \to H(a)$ является универсальным накрытием. Это очевидно для групп, указанных в пп. 1), 4) приведенного в п. 4 списка классических групп, ибо здесь группы H и $H(a)$ односвязны (напомним, что п. 3) мы исключаем из рассмотрения). Для оставшихся пп. 2), 4) это следует из согласованности универсальных накрытий специальных ортогональных групп для пространства и подпространства, доставляемых соответствующими спинорными группами (см. п. 2). Второе утверждение предложения, касающееся стабилизаторов пар векторов, непосредственно вытекает из первого.

§ 2.4. Некоторые результаты из алгебраической геометрии

Большинство многообразий, с которыми мы будем работать, являются аффинными либо проективными, т. е. бирегулярно изоморфны замкнутым подмножествам соответственно в n-мерном аффинном пространстве $\mathbb{A}^n$ либо n-мерном проективном пространстве $\mathbb{P}^n$. Мы предполагаем известными стандартные понятия алгебраической геометрии вплоть до понятия размерности (см. Шафаревич [1], Хартсхорн [1], а также гл. АГ в книге Борель [8]). Некоторые более специальные факты будут перечислены ниже.

1. Поле определения алгебраического многообразия (Борель [8], гл. АГ, § 12—14). Пусть K — подполе универсальной области Ω. Говорят, что замкнутое подмногообразие $X \subset \mathbb{A}^n$ определено над K, если идеал $\mathfrak{a} \subset \Omega[x_1, \ldots, x_n]$, состоящий из многочленов, обращающихся в нуль на X, порождается пересечением $\mathfrak{a} \cap K[x_1, \ldots, x_n]$ (здесь x_i — стандартная координатная функция на $\mathbb{A}^n$). Регулярное (рациональное) отображение f: $X \to Y$ двух K-определенных подмногообразий $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ определено над K, если существуют такие полиномы $f_i \in K[x_1, \ldots, x_n]$ (соответственно, рациональные функции $f_i \in K(x_1, \ldots, x_n)$), $i = 1, \ldots, m$, что $f(x) = (f_1(x), \ldots, f_m(x))$ для всех $x \in X$. В случае совершенного поля K известен следующий критерий Галуа для K-определенности: замкнутое подмногообразие $X \subset \mathbb{A}^n$ определено над K в том и только том случае, если X определено над $\bar{K}$ и $X = X^\sigma$ для всех $\sigma \in \mathrm{Gal}(\bar{K}/K)$, где X^σ определяется идеалом $(\mathfrak{a} \cap K[x_1, \ldots, x_n])^\sigma \subset \bar{K}[x_1, \ldots, x_n]$. Аналогичное утверждение может быть сформулировано и доказано для произвольных многообразий и регулярных (рациональных) отображений.

2. Доминантные морфизмы. Морфизм φ: $X \to Y$ называется *доминантным*, если $\varphi(X)$ плотно в Y в топологии Зарисского. Для таких морфизмов имеет место

Теорема 12 (о размерности слоев морфизма). *Пусть* $\varphi: X \to Y$ *доминантный морфизм неприводимых алгебраических многообразий,* $r = \dim X - \dim Y$. *Тогда*

1) *для любой точки* $y \in \varphi(X)$ *имеем* $\dim \varphi^{-1}(y) \geqslant r$,

2) *множество* $\{y \in Y \mid \dim \varphi^{-1}(y) = r\}$ *является непустым и открытым.*

Доказательство — см. Шафаревич [1], гл. I, § 6.

3. Касательные пространства. Простые и особые точки (Шафаревич [1], гл. II). Данные понятия носят локальный характер, т. е. не зависят от того, рассматривать ли их относительно некоторого многообразия X или какой-либо окрестности данной точки в X. Поэтому можно вместо X рассмотреть аффинную окрестность фиксированной точки $x \in X$ и тем самым считать многообразие X аффинным. Пусть $X \subset \mathbb{A}^n$ и $\mathfrak{a} \subset \Omega[x_1, \ldots, x_n]$ — идеал многочленов, обращающихся в нуль на X. Для произвольного многочлена $f(x_1, \ldots, x_n) \in \Omega[x_1, \ldots, x_n]$ и точки $x \in \mathbb{A}^n$ обозначим через $d_x f(X_1, \ldots, X_n)$ линейную форму $\sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(x) X_i$, где $X_i (i = 1, \ldots, n)$ — координаты в n-мерном векторном пространстве, полученном, если точку x принять за начало координат в $\mathbb{A}^n$. *Касательным пространством* к многообразию X в точке $x \in X$ называется подпространство $T_x(X)$ в этом n-мерном векторном пространстве, определяемое уравнениями

$$d_x f(X_1, \ldots, X_n) = 0, \quad f \in \mathfrak{a}. \tag{1}$$

По теореме Гильберта о базисе идеал $\mathfrak{a}$ порождается конечным числом многочленов $f_1, \ldots, f_r$, и тогда вместо (1) можно рассматривать эквивалентную систему

$$d_x f_i(X_1, \ldots, X_n) = 0, \quad i = 1, \ldots, r. \tag{2}$$

Если теперь многообразие X определено над K и $x \in X_K$, то, выбирая в качестве f_i образующие $\mathfrak{a}$ с коэффициентами из K, мы видим, что касательное пространство $T_x(X)$ также определено над K. Регулярное отображение $\varphi: X \to Y$ алгебраических многообразий для любой точки $x \in X$ индуцирует линейное отображение $d_x\varphi: T_x(X) \to T_{\varphi(x)}(Y)$ соответствующих касательных пространств, называемое *дифференциалом* φ в точке x, причем $d_x\varphi$ определено над K, если таковым является φ и $x \in X_K$.

В уравнениях (1), (2) точка x предполагается фиксированной. Если же заставить x пробегать все X, т. е. рассмотреть совокупность точек $(x, t) \in \mathbb{A}^n \times \mathbb{A}^n$ таких, что $x \in X$, $t \in T_x(X)$, то мы получим так называемое *касательное расслоение* $T(X)$ многообразия X. Система (2) показывает, что $T(X)$ является многообразием. Считая X неприводимым и применяя к канонической проекции $T(X) \to X$ теорему 12, получаем, что для всех точек x из некоторого открытого по Зарисскому подмножества

$U \subset X$ размерность $\dim T_x(X)$ соответствующего касательного пространства принимает одно и то же значение d, причем $\dim T_x(X) \geqslant d$ для любой точки $x \in X$. Далее, оказывается, что число d совпадает с размерностью многообразия $\dim X$. Таким образом, $\dim T_x(X) \geqslant \dim X$ для всех $x \in X$, причем точки, для которых достигается равенство (они называются *простыми*, остальные точки — *особыми*), образуют непустое открытое по Зарисскому множество. В случае приводимого X точка $x \in X$ называется простой, если она принадлежит единственной неприводимой компоненте $Y \subset X$ и является простой на Y.

Предложение 22. *Точка x многообразия $X \subset \mathbb{A}^n$ является простой в том и только том случае, если найдутся такие многочлены $f_1, \ldots, f_r \in \Omega[x_1, \ldots, x_n]$, где $r = n - \dim_x X$ *), и такое открытое по Зарисскому подмножество $U \subset \mathbb{A}^n$, что $x \in Y = \{y \in U \mid f_i(y) = 0,\ i = 1, \ldots, r\}$, $Y \subset X$ и ранг матрицы Якоби*

$$\left(\frac{\partial f_i}{\partial x_j}(x)\right)_{\substack{i=1,\ldots,r\\ j=1,\ldots,n}}$$

равен r. Если многообразие X определено над K и $x \in X_K$ — простая точка, то многочлены $f_1, \ldots, f_r$ можно выбрать с коэффициентами из K.

Многообразие, все точки которого простые, называется *гладким*. Так как простые точки всегда существуют, то любое однородное многообразие является гладким. В частности, гладким будет многообразие произвольной алгебраической группы.

4. Бирациональные изоморфизмы. Рациональное отображение $\varphi\colon X \to Y$ неприводимых многообразий называется *бирациональным изоморфизмом*, если существует обратное рациональное отображение $\varphi^{-1}\colon Y \to X$. В этом случае φ индуцирует бирегулярный изоморфизм открытых по Зарисскому множеств $U \subset X$, $V \subset Y$. Многообразия, бирационально изоморфные аффинным пространствам, называются *рациональными*. Доминантный морфизм $\varphi\colon X \to Y$ является бирациональным изоморфизмом, если соответствующий коморфизм φ^* индуцирует изоморфизм полей рациональных функций $\Omega(X)$ и $\Omega(Y)$. В частности, многообразие X рационально в том и только том случае, если поле рациональных функций $\Omega(X)$ является чисто трансцендентным расширением Ω. Отметим, что все указанные определения и свойства имеют очевидные аналоги для K-определенных многообразий.

Имеется одно полезное достаточное условие для того, чтобы доминантный морфизм $\varphi\colon X \to Y$ являлся бирациональным изоморфизмом, для формулировки которого напомним, что φ называется сепарабельным, если коморфизм φ^* определяет сепа-

*) $\dim_x X$ означает размерность X в точке x, т. е. максимум размерностей неприводимых компонент X, проходящих через x.

рабельное расширение полей $\Omega(X)/\varphi^*\Omega(Y)$ (естественно, что условие сепарабельности автоматически выполняется в характеристике нуль).

Теорема 13. *Пусть* $\varphi\colon X \to Y$ — *инъективный доминантный сепарабельный морфизм неприводимых многообразий. Тогда* φ *является бирациональным изоморфизмом. Если при этом* φ *является* K-*определенным морфизмом* K-*многообразий, то он является* K-*бирациональным изоморфизмом.*

Доказательство — см. Хамфри [1], гл. I, п. 4.6.

Из теоремы вытекает, что для доказательства K-рациональности некоторого многообразия X достаточно построить инъективный доминантный сепарабельный K-морфизм $\varphi\colon U \to X$ некоторого открытого подмножества $U \subset \mathbb{A}^n$. Отметим также, что K-многообразие X, для которого существует доминантный K-определенный морфизм $\varphi\colon U \to X$ открытого по Зарисскому подмножества $U \subset \mathbb{A}^n$, называется *унирациональным*. Вопрос о том, всякое ли унирациональное многообразие является рациональным, известен под названием проблемы Люрота. К настоящему времени показано, что проблема Люрота как в относительном варианте (т. е. над незамкнутым основным полем), так и в абсолютном (т. е. над замкнутым основным полем), решается, вообще говоря, отрицательно. Многообразие связной (линейной) алгебраической K-группы G всегда унирационально над K, если либо поле K совершенно, либо группа G редуктивна (см. Борель [8], § 18), откуда, в частности, вытекает доказательство теоремы 2. Тем самым вопрос о K-рациональности многообразий K-определенных алгебраических групп имеет характер относительного варианта проблемы Люрота (его обсуждение — см. в § 7.3).

Следующая теорема позволяет проследить, насколько бирациональные морфизмы отличаются от бирегулярных.

Теорема 14. *Пусть* $\varphi\colon X \to Y$ — *регулярное отображение и бирациональный изоморфизм неприводимых многообразий,* $x \in X$. *Предположим, что точка* $y = \varphi(x)$ *является простой на многообразии* Y. *Тогда если обратное рациональное отображение* $\psi = \varphi^{-1}$ *нерегулярно в точке* y, *то* $\dim \varphi^{-1}(y) \geqslant 1$.

Доказательство — см. Шафаревич [1], гл. II, § 4.

Из теорем 13, 14 вытекает, что если $\varphi\colon X \to Y$ — биективный регулярный морфизм неприводимых многообразий в характеристике нуль, причем многообразие Y гладко, то φ является бирегулярным изоморфизмом.

5. Действия алгебраических групп на многообразиях. Говорят, что алгебраическая группа G *действует* на алгебраическом многообразии X, если задан морфизм $\mu\colon G \times X \to X$ такой, что

1) $$\mu(e, x) = x,$$

2) $$\mu(gh, x) = \mu(g, \mu(h, x)).$$

(Мы дали определение так называемого «левого» действия. Иногда, однако, удобно рассматривать «правое» действие μ: $X \times G \to X$, подчиняющееся законам $\mu(x, e) = x$ и $\mu(x, gh) = \mu(\mu(x, g), h)$). В целях сокращения записи обычно пишут gx вместо $\mu(g, x)$. *Действие определено над K*, если группа G, многообразие X и морфизм μ определены над K.

Из общих результатов о действиях алгебраических групп нам понадобится лишь так называемая лемма о замкнутых орбитах (см. Борель [8], п. 1.8).

Предложение 23. *Пусть G — алгебраическая группа, действующая на многообразии X. Тогда каждая орбита является гладким многообразием, открытым в своем замыкании. Ее граница есть объединение орбит строго меньшей размерности. В частности, орбиты минимальной размерности замкнуты.*

Многообразие X называется однородным пространством группы G, если существует транзитивное действие $G \times X \to X$. Если зафиксировать точку $x \in X$, то в этом случае имеем биекцию $G/G(x) \leftrightarrow X$ между левыми смежными классами по стабилизатору $G(x)$ точки x и точками многообразия X, которую можно использовать для наделения множества $G/G(x)$ структурой алгебраического многообразия. (Отметим, что из гладкости однородного пространства и результатов п. 3 вытекает, что, по крайней мере в характеристике нуль, эта структура определена однозначно.) Возникает вопрос, для любой ли (замкнутой) подгруппы $H \subset G$ существуют такое действие G на некотором алгебраическом многообразии X и такая точка $x \in X$, что $G(x) = H$. Утвердительный ответ здесь вытекает из следующей теоремы Шевалле (см. Борель [8], п. 5.1; Хамфри [1]): *пусть G — произвольная K-группа, H — замкнутая подгруппа, определенная над K; существуют точное K-определенное представление ρ: $G \to GL(V)$ и K-определенное одномерное подпространство $D \subset V$, такие, что $H = \{g \in G \mid gD = D\}$.* Рассматривая тогда индуцированное действие G на проективном пространстве $\mathbb{P}(V)$ и точку $x \in \mathbb{P}(V)$, отвечающую D, мы получаем геометрическую реализацию G/H как орбиты Gx, которая оказывается квазипроективным многообразием, т. е. открытым подмножеством некоторого проективного многообразия. При построении теории приведения в гл. IV, V нам понадобится следующий результат, детализирующий теорему Шевалле (см. Борель [6], § 7).

Теорема 15 (усиленная теорема Шевалле). *Пусть G — связная алгебраическая группа, H — ее редуктивная подгруппа, определенные над полем K характеристики нуль. Тогда существуют K-определенное представление ρ: $G \to GL(V)$ и вектор $x \in V_K$ такие, что $G(x) = H$ и орбита Gx замкнута в V.*

Поскольку этот результат не столь популярен, как теорема Шевалле, мы дадим набросок доказательства. Рассматривается

действие H на G левыми сдвигами и соответствующее представление H в алгебре регулярных функций $\bar{K}[G]$. Хорошо известно, что это представление локально конечномерно, а классические рассуждения Нагаты [1] из теории инвариантов редуктивных групп показывают, что алгебра инвариантов $A = \bar{K}[G]^H$ конечно порождена и инвариантные функции разделяют непересекающиеся замкнутые H-инвариантные подмножества в G (в частности, различные левые смежные классы). Исходя из этих результатов, выберем в A_K конечную систему образующих $x_1, \ldots, x_r$ и обозначим через V_i конечномерное G-инвариантное K-определенное подпространство в A, содержащее x_i. Покажем, что естественное представление в пространстве $V = \bigoplus_{i=1}^{r} V_i$ и точка $x = (x_1, \ldots, x_r) \in V_K$ являются искомыми. Действительно, по построению $x_i \in A = \bar{K}[G]^H$, откуда $G(x) \supset H$. С другой стороны, если $gx = g$, то, в частности, $x_i(g) = x_i(e)$. Но поскольку функции x_i порождают A, они должны разделять различные смежные классы, откуда $gH = H$ и $g \in H$. Остается показать, что орбита Gx замкнута. Положим $X = \overline{Gx}$ и рассмотрим коморфизм η: $\bar{K}[X] \to \bar{K}[G]$, отвечающий морфизму $G \to X, g \mapsto gx$. Из наших построений вытекает, что η осуществляет изоморфизм $\bar{K}[X]$ и A. При этом, используя биекцию между точками аффинного многообразия и максимальными идеалами кольца регулярных функций, легко показать, что утверждение о том, что $X = Gx$, равносильно следующему факту: для любого собственного максимального идеала $\mathfrak{m} \subset A$ идеал $\mathfrak{m}\bar{K}[G]$ нетривиален. Но в силу редуктивности H существует A-линейная проекция $\bar{K}[G] \to A$, так что из равенства $\mathfrak{m}\bar{K}[G] = \bar{K}[G]$ получаем, что $\mathfrak{m}A = A$, — противоречие.

Отметим, что, применяя теорему 15, в гл. IV, V мы будем использовать вместо ρ соответствующее правое представление ρ^*, определяемое формулой $\rho^*(g) = \rho(g^{-1})$, и записывать действие так: $x\rho^*(g)$; тогда $x\rho^*(gh) = (x\rho^*(g))\rho^*(h)$.

При доказательстве некоторых результатов арифметической теории алгебраических групп мы будем использовать ряд конкретных многообразий, к конструкции и описанию свойств которых мы сейчас переходим.

6. Многомерные классы сопряженности. Орбитами присоединенного действия $G \times G \to G$, $(g, h) \mapsto ghg^{-1}$, являются классы сопряженности в G. Известно (см. Семинар по алгебраическим группам, с. 191), что класс сопряженности элемента $h \in G$ замкнут в том и только том случае, если этот элемент полупрост. Аналогично, можно рассмотреть присоединенное действие G на декартовой степени G^d: $(g, (h_1, \ldots, h_d)) \mapsto (gh_1g^{-1}, \ldots, gh_dg^{-1})$. Тогда возникающие здесь орбиты естественно называть *многомерными классами сопряженности*. Нам понадо-

бится одно достаточное условие замкнутости многомерных классов сопряженности. Будем называть подгруппу $H \subset G$ (не обязательно замкнутую) *редуцированной*, если при некотором точном представлении ρ: $G \to GL_n(\Omega)$ она переходит во вполне приводимую линейную группу.

Теорема 16. *Пусть группа G редуктивна, а элементы $h_1, \ldots, h_d \in G$ порождают редуцированную подгруппу. Тогда многомерный класс сопряженности в G элемента $(h_1, \ldots, h_d)$ замкнут в G^d.*

Доказательство. Рассмотрим вначале случай, когда $G = GL_n(\Omega)$, а подгруппа $H \subset G$, порожденная $h_1, \ldots, h_d$, является вполне приводимой. Тогда Ω-оболочка H, т. е. подалгебра в $M_n(\Omega)$, порожденная H, которую мы обозначим через A, является полупростой алгеброй. Пусть $u_1, \ldots, u_m$ — некоторый базис алгебры A, содержащийся в H, и $w_i (i = 1, \ldots, m)$ — такие слова от d переменных, что $u_i = w_i(h_1, \ldots, h_d)$. Имеем

$$u_i u_j = \sum_{k=1}^{m} c_{ij}^k u_k$$

для некоторых $c_{ij}^k \in \Omega$, называемых структурными константами алгебры A. Кроме того, найдутся такие $d_{ij} \in \Omega (i = 1, \ldots, d;$ $j = 1, \ldots, m)$, что

$$h_i = \sum_{j=1}^{m} d_{ij} u_j.$$

Обозначим через F подмногообразие в G^d, определяемое уравнением

$$w_i(x_1, \ldots, x_d)\, w_j(x_1, \ldots, x_d) = \sum_{k=1}^{m} c_{ij}^k w_k(x_1, \ldots, x_d) \qquad (3)$$

$$(i, j = 1, \ldots, m),$$

$$x_i = \sum_{j=1}^{m} d_{ij} w_j(x_1, \ldots, x_d) \qquad (i = 1, \ldots, d), \qquad (4)$$

и покажем, что F совпадает с многомерным классом сопряженности C элемента $h = (h_1, \ldots, h_d)$. Включение $C \subset F$ очевидно. Пусть теперь $f = (f_1, \ldots, f_d) \in F$. Обозначим через B подпространство, натянутое на элементы $v_i = w_i(f_1, \ldots, f_d)$ $(i = 1, \ldots, m)$. Из уравнений (3) вытекает, что B является подалгеброй в $M_n(D)$ и соответствие $u_i \to v_i$ $(i = 1, \ldots, m)$ продолжается до сюръективного гомоморфизма алгебр φ: $A \to B$, а из (4) — что при этом $\varphi(h_i) = f_i (j = 1, \ldots, d)$. Пусть $A = \bigoplus_{i=1}^{t} A_i$ — разложение A в прямую сумму простых подалгебр. Тогда для каждого $i = 1, \ldots, t$ либо $\varphi(A_i) = 0$, либо ограничение $\varphi|_{A_i}$ —

изоморфизм на образ. Используя теорему Сколема — Нётер (см. п. 1 § 1.4), получаем, что существует такой $g \in \mathrm{GL}_n(\Omega)$, что для гомоморфизма $\psi\varphi$, где $\psi = \operatorname{Int} g$, выполняется следующее условие: для любого $i = 1, \ldots, t$ ограничение $\psi\varphi|_{A_i}$ является либо нулевым гомоморфизмом, либо тождественным. С другой стороны, если предположить, что $\psi\varphi|_{A_i} = 0$ для некоторого i, то алгебра $B = \varphi(A)$ состоит целиком из вырожденных матриц. Это противоречит тому, что $f_i \in B$. Итак, $\psi\varphi|_A = \mathrm{id}_A$, откуда $f_i = \varphi(h_i) = \psi^{-1}(h_i) = g^{-1}h_i g$ для всех $i = 1, \ldots, d$, т. е. $f \in C$, что и требовалось.

Общий случай в теореме 16 сводится к только что рассмотренному. Выберем точное представление $\rho\colon G \to \mathrm{GL}_n(\Omega)$, при котором группа H переходит во вполне приводимую линейную группу, и будем считать G подгруппой группы $G_0 = \mathrm{GL}_n(\Omega)$. Обозначим через C_0 (соответственно C) многомерный класс сопряженности элемента $h = (h_1, \ldots, h_d)$ в G_0 (соответственно в G). Ясно, что $C \subset C_0 \cap G^d$.

Лемма 11. *C совпадает с неприводимой компонентой пересечения $C_0 \cap G^d$.*

Доказательство получается при помощи обобщения рассуждений Ричардсона [1]. Обозначим через Z неприводимую компоненту пересечения $C_0 \cap G^d$, содержащую C, и покажем, что $Z = C$. Для этого, используя редуктивность G, а значит, полную приводимость всех представлений в случае $\operatorname{char} K = 0$ (см. теорему 4), в алгебре Ли $\mathfrak{g}_0 = L(G_0)$ выберем G-инвариантное подпространство $\mathfrak{m}$, дополнительное к $\mathfrak{g} = L(G)$. Рассмотрим отображение $\pi\colon G_0 \to D_0$, где $D_0 = C_0 h^{-1}$, определяемое формулой $\pi(g) = (gh_1g^{-1}h_1^{-1}, \ldots, gh_dg^{-1}h_d^{-1})$. Легко видеть, что $\pi(G_0) = D_0$, $d_e\pi(X) = (X - \operatorname{Ad}(h_1)(X), \ldots, X - \operatorname{Ad}(h_d)(X))$, $X \in \mathfrak{g}_0$, причем $d_e\pi(\mathfrak{g})$ совпадает с касательным пространством $T_e(D_0)$ к многообразию D_0 в единице. Покажем, что

$$\mathfrak{g}^d \cap d_e\pi(\mathfrak{g}_0) = d_e\pi(\mathfrak{g}). \tag{5}$$

Действительно, пусть $d_e\pi(X) \in \mathfrak{g}^d$ для $X \in \mathfrak{g}_0$. Представим X в виде $X = Y + Z$, где $Y \in \mathfrak{g}$, $Z \in \mathfrak{m}$. Тогда для любого $i = 1, \ldots, d$

$$X - \operatorname{Ad}(h_i)(X) = (Y - \operatorname{Ad}(h_i)(Y)) + (Z - \operatorname{Ad}(h_i)(Z)),$$

откуда $Z - \operatorname{Ad}(h_i)(Z) \in \mathfrak{m} \cap \mathfrak{g} = (0)$ в силу G-инвариантности $\mathfrak{m}$ и $d_e\pi(X) = d_e\pi(Y)$, т. е. (5) доказано. В силу предложения 13 C является гладким многообразием, открытым в своем замыкании. Рассмотрим касательное пространство $T_e(D)$ к многообразию $D = Ch^{-1}$. Тогда из включений

$$d_e\pi(\mathfrak{g}) \subset T_e(D) \subset T_e(Zh^{-1}) \subset \mathfrak{g}^d \cap d_e\pi(\mathfrak{g}_0)$$

и (5) вытекает, что $T(Ch^{-1})_e = T(Zh^{-1})_e$, т. е. C открыто в Z. Это рассуждение применимо к любому многомерному классу сопряженных элементов G, содержащемуся в Z. Поскольку Z — неприводимое многообразие, существует только один такой класс, таким образом, $C = Z$, и лемма доказана.

Так как неприводимые компоненты замкнутого подмножества $C_0 \cap G^d$, совпадающие по лемме с многомерными классами сопряженности, замкнуты, то доказательство теоремы 16 завершено.

Мы будем применять теорему для групп над полями характеристики нуль в двух случаях, когда H есть либо связная редуктивная, либо конечная подгруппа.

Отметим, что при $d = 1$ условие редуцированности подгруппы, порожденной элементом $h \in G$, равносильно полупростоте h, и мы получаем одну из импликаций в упоминавшемся критерии замкнутости обычного класса сопряженности. В связи с этим было бы интересно выяснить, допускает ли теорема 16 обращение.

7. Многообразия представлений. Пусть Γ — произвольная конечнопорожденная группа, G — некоторая алгебраическая K-группа. Покажем, что множество всех гомоморфизмов (т. е. представлений) группы Γ в G находится в биективном соответствии с точками некоторого K-многообразия $R(\Gamma, G)$, называемого *многообразием представлений*. Для этого рассмотрим произвольную систему образующих $\gamma_1, \ldots, \gamma_d$ группы Γ и ассоциированный с ней сюръективный гомоморфизм π: $F_d \to \Gamma$ свободной группы ранга d с образующими $x_1, \ldots, x_d$, переводящий x_i в $\gamma_i (i = 1, \ldots, d)$. Пусть $N = \operatorname{Ker} \pi$ — множество всех соотношений между $\gamma_1, \ldots, \gamma_d$ в Γ. Положим тогда

$$R(\Gamma, G) = \{(g_1, \ldots, g_d) \in \\ \in G^d \mid w(g_1, \ldots, g_d) = e \ \forall w = w(x_1, \ldots, x_d) \in N\}.$$

Из того факта, что алгебраические операции в G являются регулярными K-определенными отображениями, вытекает, что для каждого слова $w = w(x_1, \ldots, x_d)$ от переменных $x_1, \ldots, x_d$ соотношение $w = e$ задает в G^d K-замкнутое подмножество, поэтому $R(\Gamma, G)$ является K-замкнутым подмножеством (подмногообразием) в G^d. С другой стороны, для точки $(g_1, \ldots, g_d) \in G^d$ гомоморфизм $\Gamma \to G$ такой, что $\gamma_i \mapsto g_i$, существует в том и только в том случае, если $(g_1, \ldots, g_d) \in R(\Gamma, G)$. Так как любой гомоморфизм Γ однозначно определяется заданием образов образующих, то многообразие $R(\Gamma, G)$ действительно решает задачу параметризации всех представлений группы Γ в G. Отметим, что многообразие $R(\Gamma, G)$ с точностью до изоморфизма не зависит от выбора исходной системы образующих $\gamma_1, \ldots, \gamma_d$. Действительно, если $\delta_1, \ldots, \delta_l$ — другая система

образующих, причем

$$\delta_i = w_i(\gamma_1, \ldots, \gamma_d), \quad i = 1, \ldots, l,$$
$$\gamma_j = \theta_j(\delta_1, \ldots, \delta_l), \quad j = 1, \ldots, d,$$

то отображения

$$(g_1, \ldots, g_d) \longmapsto (w_1(g_1, \ldots, g_d), \ldots, w_l(g_1, \ldots, g_d)),$$
$$(\delta_1, \ldots, \delta_l) \longmapsto (\theta_1(\delta_1, \ldots, \delta_l), \ldots, \theta_d(\delta_1, \ldots, \delta_l))$$

являются взаимно обратными K-определенными морфизмами между многообразиями представлений $R_\gamma(\Gamma, G)$ и $R_\delta(\Gamma, G)$, построенными по системам образующих $\gamma_1, \ldots, \gamma_d$ и $\delta_1, \ldots, \delta_l$ соответственно. На многообразии $R(\Gamma, G)$ естественным образом действует группа G:

$$g(g_1, \ldots, g_d) = (gg_1g^{-1}, \ldots, gg_dg^{-1}).$$

При этом орбиты G отвечают классам эквивалентных относительно G представлений.

В последнее время появился ряд интересных результатов о многообразиях представлений $R(\Gamma, G)$ и связанных с ними многообразиях характеров (см. Платонов [22, 23], Платонов, Беняш-Кривец [1]). Мы, однако, ограничимся здесь доказательством лишь следующего утверждения.

Теорема 17. *Пусть Γ — конечная группа, а G — редуктивная группа. Тогда имеется лишь конечное число орбит естественного действия G на $R(\Gamma, G)$, причем эти орбиты замкнуты.* (*Напоминаем*, $\operatorname{char} K = 0$.)

Доказательство. Утверждение о замкнутости орбит вытекает из теоремы о замкнутости многомерных классов сопряженных элементов, ибо в силу условия $\operatorname{char} K = 0$ образ любого гомоморфизма $\Gamma \to GL_n(\Omega)$ является вполне приводимой группой. Доказательство конечности числа орбит для случая $G = GL_n(\Omega)$ вытекает из классической теории представлений конечных групп, согласно которой имеется лишь конечное число неэквивалентных неприводимых представлений Γ. Общий случай сводится к рассмотренному при помощи леммы 11. Действительно, если C_0 — класс эквивалентности некоторого представления $\rho \in R(\Gamma, G)$ относительно группы $GL_n(\Omega)$, то неприводимые компоненты пересечения $R(\Gamma, G) \cap C_0$ являются классами эквивалентности относительно группы G. С другой стороны, неприводимых компонент имеется лишь конечное число. Теорема 17 доказана.

8. **Многообразия торов.** Пусть G — редуктивная K-группа, $T \subset G$ — максимальный K-определенный тор и $N = N_G(T)$ — его нормализатор. Из теоремы о сопряженности максимальных торов вытекает, что соответствие $gN \longmapsto T_g = gTg^{-1}$ задает биекцию между максимальными торами группы G и точками многообразия $\mathcal{T} = G/N$, называемого *многообразием* (*максимальных*)

торов группы G. При этом K-определенным максимальным торам в G отмечают точки из $\mathcal{T}_K$. (Отметим, что многообразие $\mathcal{T}$ с точностью до K-изоморфизма не зависит от выбора исходного тора T.)

Теорема 18 (Шевалле [3], Борель — Спрингер [1]). *Если* $\operatorname{char} K = 0$, *то многообразие* $\mathcal{T}$ *является рациональным над* K.

Доказательство. Пусть $\mathfrak{g} = L(G)$, $\mathfrak{h} = L(T)$ — алгебры Ли G и T соответственно. Обозначим через $\mathfrak{m}$ такое K-определенное T-инвариантное подпространство в $\mathfrak{g}$, что $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{m}$, и пусть $X \in \mathfrak{h}_K$ — регулярный элемент. Обозначим через $\mathfrak{m}_0$ подмножество в $\mathfrak{m}$, состоящее из таких Z, что элемент $X + Z$ полупрост и регулярен, и его централизатор $\mathfrak{z}_{\mathfrak{g}}(X + Z)$ не пересекается с $\mathfrak{m}$. Утверждается, что $\mathfrak{m}_0$ является открытым подмножеством в $\mathfrak{m}$. Так как открытость множества регулярных полупростых элементов хорошо известна (см. п. 11 в § 2.1), то достаточно показать, что множество $\mathfrak{m}_1 = \{Z \in \mathfrak{m} \mid \mathfrak{z}_{\mathfrak{g}}(X + Z) \cap \mathfrak{m} = (0)\}$ также открыто. Для этого введем многообразие $P = \{(Y, Z) \in \mathfrak{m} \times \mathfrak{m} \mid [X + Z, Y] = 0\}$ и рассмотрим проекцию $P \xrightarrow{\pi} \mathfrak{m}$, $(Y, Z) \mapsto Z$. Ясно, что для любого $Z \in \mathfrak{m}$ имеем $(Z, 0) \in P$, в частности, π сюръективно, причем $\pi^{-1}(0) = (0, 0)$, ибо по построению $\mathfrak{z}(X) = \mathfrak{h}$ и $\mathfrak{h} \cap \mathfrak{m} = (0)$. По теореме о размерности слоев морфизма отсюда вытекает, что $\dim P = \dim \mathfrak{m}$ и множество $\{Z \in \mathfrak{m} \mid \dim \pi^{-1}(Z) = 0\}$ открыто в $\mathfrak{m}$. Однако легко видеть, что последнее множество совпадает с $\mathfrak{m}_1$.

Положим $W = \{(Z, g) \in \mathfrak{m} \times G \mid g^{-1}(X + Z)g \in \mathfrak{h}\}$, $U = (\mathfrak{m}_0 \times G) \cap W$. Так как W является прообразом $\mathfrak{h}$ при K-морфизме $\varphi\colon \mathfrak{m} \times G \to \mathfrak{g}$, $\varphi(z, g) = g^{-1}(X + Z)g$, то W — замкнутое K-определенное подмножество в $\mathfrak{m} \times G$. С другой стороны, $(0, 1) \in U$, так что U — непустое открытое подмножество в W. Рассмотрим проекции $\theta\colon W \to \mathfrak{m}$ и $\delta\colon W \to G$. Поскольку для $Z \in \mathfrak{m}_0$ централизатор $\mathfrak{z}_{\mathfrak{g}}(X + Z)$ является алгеброй Ли некоторого максимального тора, то из теоремы сопряженности вытекает существование такого $g \in G$, что $g^{-1}(X + Z)g \in \mathfrak{h}$, откуда $\theta(U) = \mathfrak{m}_0$. При этом по построению

$$g\mathfrak{h}g^{-1} \cap \mathfrak{m} = (0), \tag{6}$$

$$\theta^{-1}(Z) = (Z, gN). \tag{7}$$

Далее, если $x = (Z, g) \in U$ и $x' = (Z', g') \in \delta^{-1}(\delta(x))$, то $g' \in gN$ и $X + Z$, $X + Z' \in g\mathfrak{h}g^{-1} = g'\mathfrak{h}(g')^{-1}$, откуда $Z - Z' \in \mathfrak{m} \cap (g\mathfrak{h}g^{-1})$ и в силу (6) $Z = Z'$. Таким образом, если рассмотреть отображение $\psi\colon \mathfrak{m} \times G \to \mathfrak{m} \times \mathcal{T}$, индуцируемое факторморфизмом $G \to \mathcal{T} = G/N$, и соответствующие проекции $\theta'\colon \overline{\psi(W)} \to \mathfrak{m}$ и $\delta'\colon \overline{\psi(W)} \to G$, то ограничение $\theta'|_{\psi(U)}$ осуществляет биекцию между $\psi(U)$ и $\mathfrak{m}_0$, а ограничение $\delta'|_{\psi(U)}$ инъективно. Тогда согласно теореме 13 существует K-определенное

рациональное отображение χ: $\mathfrak{m}_0 \to \overline{\varphi(W)}$, обратное к θ' (напоминаем, что у нас $\operatorname{char} K = 0$), причем композиция $\xi = \delta' \circ \chi$ инъективна на области определения. Поскольку $\dim \mathfrak{m} = \dim \mathscr{T}$, то опять, применяя теорему 13, получаем, что ξ осуществляет бирациональный изоморфизм между $\mathfrak{m}$ и $\mathscr{T}$, и теорема доказана.

Предложение 24. *Пусть G — связная алгебраическая группа над полем K характеристики нуль, $W \subset G$ — множество регулярных полупростых элементов. Тогда существует такое регулярное K-определенное отображение φ: $W \to \mathscr{T}$, что $x \in T_{\varphi(x)}$ для всех $x \in W$, т. е. каждый элемент отображается в содержащий его тор.*

Доказательство. Зафиксируем максимальный K-определенный тор $T \subset G$, при помощи которого определяется многообразие торов $\mathscr{T} = G/N$, $N = N_G(T)$, и положим $Z = \{(x, g) \in W \times \times G \mid g^{-1}xg \in T\}$. Очевидно, Z — замкнутое подмножество в $W \times G$. Обозначим через θ: $W \times G \to W \times \mathscr{T}$ регулярное отображение, индуцированное факторизоморфизмом ψ: $G \to \mathscr{T}$. Легко видеть, что $Z = \theta^{-1}(\theta(Z))$, так что из открытости ψ (см. Борель [8], § 6) вытекает замкнутость $Y = \theta(Z)$. Пусть π_1: $W \times \times \mathscr{T} \to W$, π_2: $W \times \mathscr{T} \to \mathscr{T}$ — естественные проекции. Утверждается, что ограничение $\pi_1|_Y$: $Y \to W$ биективно. Действительно, для любого $x \in W$ из теоремы о сопряженности максимальных торов вытекает существование, а из регулярности x — единственность с точностью до элемента из N, такого $g \in G$, что $g^{-1}xg \in T$. Поскольку множество W открыто в G и, следовательно, является гладким многообразием, в силу результатов п. 3 существует обратное к $\pi_1|_Y$ регулярное отображение δ: $W \to Y$. Тогда отображение $\varphi = \pi_2 \circ \delta$ и будет искомым. Предложение доказано.

Отметим, что если рассмотреть действие G на W посредством сопряжения, а на $\mathscr{T}$ — посредством сдвигов, то построенное отображение φ будет G-эквивариантным.

9. Многообразие борелевских подгрупп. В § 2.1 мы видели, что подгруппы Бореля связной алгебраической группы G находятся во взаимно однозначном соответствии с точками фактормногообразия $\mathscr{B} = G/B$, где $B \subset G$ — некоторая фиксированная подгруппа Бореля, поэтому многообразие $\mathscr{B}$ естественно называют *многообразием борелевских подгрупп*. Если K-группа G обладает борелевской подгруппой, определенной над K, то $\mathscr{B}$, очевидно, является K-многообразием, причем действие G на B левыми сдвигами K-определено. Однако, как мы знаем, наличие K-определенной борелевской подгруппы является сравнительно редким явлением, и поэтому естественно спросить, обладает ли $\mathscr{B}$ K-структурой в общем случае.

Теорема 19. *Пусть G — связная алгебраическая K-группа. Тогда многообразие $\mathscr{B}$ борелевских подгрупп обладает такой*

K-структурой, что точки из $\mathscr{B}_K$ отвечают K-определенным борелевским подгруппам и действие G на $\mathscr{B}$ K-определено.

Доказательство. Положим $H = G/R(G)$, $\bar{H} = H/Z(H)$. Тогда $\bar{H}$ является полупростой присоединенной группой. Обозначим через φ: $G \to \bar{H}$ — соответствующий факторморфизм. Если B — борелевская подгруппа в G, то $\varphi(B)$ — борелевская подгруппа в $\bar{H}$ и $G/B \simeq \bar{H}/\varphi(B)$. Тем самым мы получаем редукцию к случаю полупростых присоединенных групп. Любая такая группа G получается из некоторой квазиразложимой группы G_0 путем скручивания при помощи подходящего коцикла $a = \{a_\sigma = \operatorname{Int} g_\sigma\}$, лежащего в группе $\operatorname{Int} G_0$. Пусть $B \subset G_0$ — K-определенная борелевская подгруппа и $\mathscr{B}_0 = G_0/B_0$ — соответствующее K-многообразие борелевских подгрупп. Тогда левые сдвиги r_σ на элементы g_σ образуют коцикл r в группе K-автоморфизмов многообразия $\mathscr{B}_0$. Так как многообразие $\mathscr{B}_0$ проективно, то существует «скрученное» многообразие $\mathscr{B}_0$ (см. замечание после теоремы 9), которое и будет искомым многообразием $\mathscr{B}$.

ГЛАВА III

АЛГЕБРАИЧЕСКИЕ ГРУППЫ НАД ЛОКАЛЬНО КОМПАКТНЫМИ ПОЛЯМИ

Если в гл. II мы рассматривали те свойства алгебраических групп, которые определяются, в первую очередь, самой группой и не зависят от основного поля, то в настоящей главе и ряде последующих мы будем исследовать влияние на их структуру свойств поля определения. Мы начинаем с рассмотрения групп над локально компактными полями по нескольким причинам. Во-первых, группа рациональных точек над таким полем наделяется естественной дополнительной структурой аналитической группы (группы Ли), что открывает возможность применения весьма развитой структурной теории групп Ли. Во-вторых, арифметические подгруппы и их обобщения, а также группы рациональных точек над числовыми полями, составляющие основной объект изучения арифметической теории алгебраических групп, вкладываются в качестве дискретных подгрупп в подходящие прямые произведения групп рациональных точек над соответствующими пополнениями, так что свойства последних существенным образом влияют на свойства исходных групп.

В § 3.1 излагаются простейшие результаты топологического и аналитического характера, бо́льшая часть которых остается справедливой над любым полем, полным (или гензелевым) относительно некоторого дискретного нормирования. В § 3.2 изучается классическая ситуация, когда основное поле совпадает либо с полем вещественных чисел $\mathbb{R}$, либо с полем комплексных чисел $\mathbb{C}$. Центральный результат здесь — получение разложения Ивасавы, которое будет играть фундаментальную роль в гл. IV. В § 3.3—3.4 мы исследуем группы над неархимедовыми локально компактными полями. При этом в § 3.3 мы излагаем результаты, связанные с использованием методов теории проконечных групп и теории редукции алгебраических многообразий, а в § 3.4 даем обзор необходимых для дальнейшего результатов теории Брюа — Титса. Наконец, в § 3.5 излагаются используемые в книге сведения из теории меры.

§ 3.1. Топология и аналитическая структура

Всюду в этой главе через K обозначается недискретное локально компактное поле характеристики нуль. Хорошо известно (см., например, Бурбаки [5]), что K может быть либо связным

(и тогда оно совпадает или с полем вещественных чисел $\mathbb{R}$, или с полем комплексных чисел $\mathbb{C}$), либо вполне несвязным (и тогда оно является конечным расширением поля p-адических чисел $\mathbb{Q}_p$). В частности, K является полным относительно некоторого нетривиального нормирования $|\ |_v$, которое либо совпадает с обычной абсолютной величиной вещественного или модулем комплексного числа, либо дискретно, т. е. имеет циклическую группу значений. При этом базис топологии K составляют открытые шары $B(a, \varepsilon) = \{x \in K \mid |a - x|_v < \varepsilon\}$, где $a \in K$, $\varepsilon > 0$. Используя топологию на K, можно естественным образом определить топологию на множестве K-точек V_K произвольного K-определенного алгебраического многообразия V. Для этого рассмотрим K-открытое по Зарисскому подмножество $U \subset V$, конечный набор $f_1, \ldots, f_r$ регулярных на U и определенных над K функций и положим

$$V(f_1, \ldots, f_r; \varepsilon) = \{x \in U_K \mid |f_i(x)|_v < \varepsilon,\ i = 1, \ldots, r\},$$

где $\varepsilon > 0$. Легко видеть, что множества $V(f_1, \ldots, f_r; \varepsilon)$ образуют базис некоторой топологии на V_K, которую мы будем называть топологией, определяемой нормированием v, или, более кратко, v-адической топологией. Отметим, что эта топология сильнее топологии Зарисского. В отличие от топологии Зарисского она обладает следующим естественным свойством: если $V = V_1 \times V_2$ — определенное над K произведение двух K-многообразий, то топологическое пространство V_K канонически гомеоморфно $V_{1K} \times V_{2K}$ с топологией прямого произведения. Если W — открытое или замкнутое подмногообразие в V, то W_K является соответственно открытым или замкнутым подпространством в V_K. Отсюда следует, что для произвольного многообразия V пространство V_K является отделимым. В самом деле, диагональ $\Delta \subset V \times V$ является замкнутой в топологии Зарисского, поэтому Δ_K замкнуто в $(V \times V)_K$; так как $(V \times V)_K \simeq V_K \times V_K$ с топологией прямого произведения, то из замкнутости Δ_K вытекает отделимость V_K. Любой регулярный K-определенный морфизм $f\colon V \to W$ индуцирует непрерывное отображение $f_K\colon V_K \to W_K$. Отсюда следует, что если G — алгебраическая K-группа, то G_K является топологической группой.

В случае аффинных или проективных многообразий введенная нами топология допускает более простое и естественное описание. А именно, если $V \subset \mathbb{A}^n$, то она является индуцированной с K^n при вложении $V_K \subset K^n$ (при этом на K^n рассматривается топология прямого произведения $K \times \ldots \times K$; ее стандартный базис состоит из n-мерных шаров $B(a, \varepsilon) = \{x \in K^n \mid \|a - x\|_v < \varepsilon\}$, где $a \in K^n$, $\varepsilon > 0$ и $\|z\|_v = \max_i |z_i|_v$, если $z = (z_1, \ldots, z_n)$). Из этого простого замечания можно извлечь ряд следствий. Во-первых, для аффинного многообразия V про-

странство V_K является локально компактным. Учитывая, что любая точка произвольного многообразия имеет открытую аффинную окрестность, легко показать, что последнее утверждение справедливо для любого многообразия. Во-вторых, если $G \subset GL_n(\Omega)$ — алгебраическая K-подгруппа, то топология на G_K индуцируется естественной топологией группы $GL_n(K)$. В частности, если K неархимедово, то топология на G_K может быть описана следующим образом: пусть $\mathcal{O} \subset K$ — кольцо целых; тогда группа целых точек $G_{\mathcal{O}} = G \cap GL_n(\mathcal{O})$ является «основной» открытой компактной подгруппой, а ее конгруэнц-подгруппы $G_{\mathcal{O}}(\mathfrak{p}^\alpha) = G_{\mathcal{O}} \cap (E_n + \mathfrak{p}^\alpha M_n(\mathcal{O}))$, где $\mathfrak{p} \subset \mathcal{O}$ — максимальный идеал, образуют базис окрестностей единицы группы G_K.

Пусть теперь $V \subset \mathbb{P}^n$ — проективное многообразие. Тогда топология на V_K является индуцированной с $\mathbb{P}^n_K$, а топология на $\mathbb{P}^n_K$ совпадает с фактортопологией относительно канонического отображения $K^{n+1} \setminus (0) \to \mathbb{P}^n_K$. Хорошо известно (см., например, Бурбаки [2]), что относительно этой топологии пространство $\mathbb{P}^n_K$ является компактным, поэтому V_K, будучи замкнутым в $\mathbb{P}^n_K$, также компактно.

Мы не будем здесь рассматривать вопрос о компактности V_K в полной общности, однако дадим критерий компактности в случае, когда V является однородным пространством.

Теорема 1. *Пусть G — K-определенная алгебраическая группа. Тогда для K-определенной подгруппы $H \subset G$ факторпространство G_K/H_K компактно в том и только том случае, когда H содержит максимальную связную K-разложимую подгруппу G^0. В частности, группа G_K компактна в том и только том случае, если связная компонента G^0 редуктивна и анизотропна над K.*

Доказательство легко редуцируется к случаю связной группы G. Предположим, что H содержит максимальную связную K-разложимую разрешимую подгруппу G, которую мы обозначим через B, и покажем, что факторпространство G_K/B_K компактно; тогда факторпространство G_K/H_K также компактно. Согласно теореме Шевалле (см. § 2.4 п. 4) можно выбрать K-определенное представление $G \to GL(V)$ и одномерное подпространство $V_1 \subset V$ такое, что стабилизатор V_1 в G совпадает с B. Так как B разложима над K, то ее образ в $GL(V/V_1)$ триангулируем над K. Отсюда следует, что в пространстве V существует K-определенный флаг $\mathcal{F} = \{V_1 \subset \ldots \subset V_i \subset \ldots \subset V_n = V \mid \dim V_i = i\}$, «начинающийся» с пространства V_1 и инвариантный относительно B. Обозначим через X замыкание орбиты $G\mathcal{F}$ в многообразии флагов $\mathcal{F}(V)$ (см. Борель [8]). В силу проективности $\mathcal{F}(V)$ многообразие X также проективно, и поэтому сделанные выше замечания позволяют утверждать, что пространство X_K компактно. Далее, как мы вскоре увидим (см. следствие 2 из предложения 3), из теоремы об обратной

функции вытекает открытость всех орбит действия G_K на $(G\mathscr{F})_K$. Поэтому если мы покажем, что $X_K=(G\mathscr{F})_K$, то открытыми будут все орбиты группы G_K на X_K, следовательно, орбита $G_K\mathscr{F}$, будучи дополнением к объединению остальных орбит, также и замкнута, т. е. компактна. Так как по построению стабилизатор $\mathscr{F}$ в G совпадает с B, то естественное отображение $\varphi\colon G\to X$, $g\mapsto g\mathscr{F}$ определяет непрерывную биекцию $\psi\colon G_K/B_K\to G_K\mathscr{F}$. Но отображение $\varphi_K\colon G_K\to X_K$ открыто (следствие 1 из предложения 3), поэтому в действительности мы имеем гомеоморфизм $G_K/B_K\xrightarrow{\sim} G_K\mathscr{F}$, который и дает требуемое. Итак, осталось показать, что $X_K\subset G\mathscr{F}$. Пусть $\mathscr{L}\in X_K\setminus G\mathscr{F}$. Тогда размерность орбиты $G\mathscr{L}$ должна быть строго меньше $\dim G\mathscr{F}$ (см. предложение 2.23), т. е. стабилизатор $G(\mathscr{L})$ флага $\mathscr{L}$ в G должен иметь размерность, строго бо́льшую $\dim B$. С другой стороны, группа $G(\mathscr{L})$, очевидно, триангулируема над K, так что связная компонента $G(\mathscr{L})^0$ разложима над K. Но это противоречит тому факту, что B является максимальной связной K-разложимой разрешимой подгруппой в G и, следовательно, имеет максимальную размерность, ибо все максимальные связные K-разложимые разрешимые подгруппы в G сопряжены (см. Борель, Титс [1]).

Перейдем к доказательству обратного утверждения. Пусть пространство G_K/H_K компактно. Выберем максимальную связную разрешимую K-разложимую подгруппу $B\subset G$, содержащую максимальную связную разрешимую K-разложимую подгруппу группы H. Тогда в силу первой части рассуждений пространство $H_K/(H\cap B)_K$ компактно. Отсюда легко следует замкнутость $H_KB_K\subset G_K$. Поэтому пространство $B_K/(B\cap H)_K\simeq B_KH_K/H_K$ компактно. Выведем отсюда, что $B=B\cap H$, т. е. $B\subset H$. Известно (см. § 2.1, п. 8), что в группе B существует определенный над K нормальный ряд $B=B_0\supset B_1\supset\ldots\supset B_r=(e)$, последовательные факторы B_i/B_{i+1} которого K-изоморфны $\boldsymbol{G}_a$ либо $\boldsymbol{G}_m$. Если предположить, что $B\cap H\neq B$, то найдется такой индекс i, что $B_i(B\cap H)=B$, но $F=B_{i+1}(B\cap H)\neq B$. Тогда из компактности $B_K/(B\cap H)_K$ вытекает компактность B_K/F_K. Рассмотрим действие группы $T=B_i/B_{i+1}$, которая изоморфна $\boldsymbol{G}_a$ либо $\boldsymbol{G}_m$, на пространстве B/F. Из следствия 2 предложения 3 вытекает открытость всех орбит T_K на $(B/F)_K$, откуда следует замкнутость T_Ke, где e — класс F в B/F, и, значит, компактность $T_K/\bar{F}_K$, где $\bar{F}$ — образ $F\cap B_i$ в T. Но поскольку $\dim T=1$, то $T\cap\bar{F}$ — конечная группа, и, следовательно, T_K также компактно, — противоречие. Теорема 1 полностью доказана.

Замечание. Используя теоремы конечности для когомологий Галуа над локальными полями (см. § 6.4), легко показать, что G_K имеет конечное число орбит на $(G/H)_K$, откуда следует, что

пространства G_K/H_K и $(G/H)_K$ компактны или некомпактны одновременно.

Из других топологических характеристик пространства V_K отметим следующее: если поле K вполне несвязно, то V_K также вполне несвязно. Вопрос о связности V_K над полями $K = \mathbb{R}, \mathbb{C}$ мы изучим в следующем параграфе.

Большинство из сделанных выше замечаний о топологии пространства V_K в равной степени относятся и к тому случаю, когда K является локально компактным полем характеристики $p > 0$, т. е. изоморфно полю $F((t))$ формальных степенных рядов над конечным полем констант F. Однако переходя к рассмотрению аналитической структуры на V_K, следует сделать оговорку, что здесь наше предположение о том, что $\operatorname{char} K = 0$, существенно и не может быть опущено.

Итак, наша ближайшая цель — ввести на множестве V_K (точнее, на его открытом по Зарисскому подмножестве) структуру аналитического многообразия. Здесь с самого начала удобно считать, что V_K плотно по Зарисскому в V, ибо тогда размерность V_K как аналитического многообразия совпадает с $\dim V$ как многообразия алгебраического. Отметим, что этому условию можно всегда удовлетворить, перейдя от V_K к замыканию W множества V_K в V; так как $\operatorname{char} K = 0$, то W является K-определенным, причем, очевидно, $W_K = V_K$.

Наша цель — показать, что каждая простая точка $x \in V_K$ обладает окрестностью, которая гомеоморфна открытому шару в пространстве K^m, где $m = \dim_x V$. Заменяя V на подходящую аффинную окрестность точки x, можно считать многообразие V аффинным, т. е. $V \subset \mathbb{A}^n$. Затем применяется предложение 2.22 и следующий вариант теоремы об обратной функции:

Теорема 2 (об обратной функции). *Пусть $U \subset K^n$ — открытое подмножество, $x \in U$ и $f = (f_1, \ldots, f_n)$: $U \to K^n$ — полиномиальное (или, более общо, аналитическое) отображение. Положим $y = f(x)$ и предположим, что матрица Якоби $\left(\frac{\partial f_i}{\partial x_j}(x)\right)_{i,j=1,\ldots,n}$ невырожденна. Тогда f является локальным аналитическим изоморфизмом в точке x, т. е. существует такая окрестность $W \subset U$ точки x, что $f(W)$ — окрестность точки y и f осуществляет аналитический изоморфизм W и $f(W)$.*

Доказательство — см. Серр [4], с. 126—129. Там же можно найти обсуждение определений и свойств, относящихся к аналитическим функциям. Отметим, что нам эти свойства фактически не понадобятся, ибо в большинстве приложений достаточно знать, что f при выполнении условий теоремы 2 является локальным гомеоморфизмом в точке x.

Пусть теперь $x = (x_1^0, \ldots, x_n^0)$ — простая точка. (Отметим, что из нашего предположения о плотности V_K в V в топологии

Зарисского и открытости множества простых точек вытекает существование таких точек x.) Тогда, согласно предложению 2.22, V определяется в окрестности точки x r уравнениями, где $r = n - m$, $m = \dim_x V$. Более точно, существует такое открытое по Зарисскому подмножество $U \subset \mathbb{A}^n$ и такие полиномы $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$, что множество $Y = \{y \in U | f_i(y) = 0, i = 1, \ldots, r\}$ содержится в V и ранг матрицы Якоби $\left(\frac{\partial f_i}{\partial x_j}(x)\right)_{\substack{i=1,\ldots,r\\ j=1,\ldots,n}}$ равен r. Без ограничения общности можно считать, что $\det\left(\frac{\partial f_i}{\partial x_j}(x)\right)_{i,j=1,\ldots,r} \neq 0$. Рассмотрим отображение $g = (g_1, \ldots, g_n)$: $K^n \to K^n$, где $g_i = f_i$ для $i \leqslant r$ и $g_i = x_i$ для $i > r$. Ясно, что

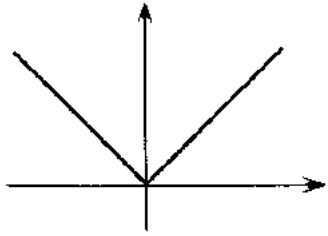
$$\det\left(\frac{\partial g_i}{\partial x_j}(x)\right)_{i,j=1,\ldots,n} = \det\left(\frac{\partial f_i}{\partial x_j}(x)\right)_{i,j=1,\ldots,r} \neq 0.$$

Согласно теореме 2 существует такая окрестность $U \subset K^n$ точки x, что $W = g(U)$ — окрестность точки $g(x)$ и g осуществляет аналитический изоморфизм U и W. Пусть $h = (h_1, \ldots, h_n) = g^{-1}$: $W \to U$. Тогда отображение $\varphi = (\varphi_1(t_1, \ldots, t_{n-r}), \ldots, \varphi_r(t_1, \ldots, t_{n-r}), t_1, \ldots, t_{n-r})$, где $\varphi_i(t_1, \ldots, t_{n-r}) = h_i(x_1^0, \ldots, x_r^0, t_1, \ldots, t_{n-r})$, $i = 1, \ldots, r$, осуществляет параметризацию окрестности точки x в V_K точками некоторого открытого в K^{n-r} множества. При этом параметризующее отображение на самом деле является обращением проекции на (последние) $n - r$ координат. Отсюда легко следует, что две параметризации окрестности фиксированной точки отличаются на аналитический изоморфизм. Таким образом, в случае аффинного многообразия V на множестве простых точек из V_K вводится естественная структура аналитического многообразия (см. Серр [4]). Данная структура согласована с регулярными отображениями аффинных многообразий, а именно, любое K-определенное регулярное отображение f: $V \to W$ аффинных K-определенных многообразий V и W индуцирует аналитическое отображение $\tilde{f}$: $\tilde{V}_K \cap f^{-1}(\tilde{W}_K) \to \tilde{W}_K$, где $\tilde{V}_K$ (соответственно $\tilde{W}_K$) — множество простых точек из V_K (соответственно W_K) с введенной выше структурой аналитического многообразия. Используя аффинные окрестности точек произвольного многообразия, легко показать, что и в общем случае $\tilde{V}_K$ является аналитическим многообразием, причем любое регулярное K-определенное отображение f алгебраических K-многообразий индуцирует аналитическое отображение $\tilde{f}$, как указано выше. В самом деле, координаты в двух аффинных окрестностях одной и той же точки связаны между собой бирациональным преобра-

зованием, определенным в этой точке. Поэтому две параметризации окрестности данной точки, построенные при помощи этих аффинных окрестностей, отличаются на аналитические изоморфизмы. Далее, любое K-определенное регулярное отображение $f\colon V \to W$ индуцирует регулярное отображение аффинных окрестностей, и тем самым — аналитическое отображение $\tilde{f}$. Нами доказано

Предложение 1. *Пусть V — определенное над K алгебраическое многообразие. Тогда множество $\tilde{V}_K$ простых точек из V_K обладает естественной структурой аналитического многообразия над K. Любое регулярное K-определенное отображение $f\colon V \to W$ алгебраических K-многообразий индуцирует аналитическое отображение $\tilde{f}\colon \tilde{V}_K \cap f^{-1}(\tilde{W}_K) \to \tilde{W}_K$.*

Таким образом, мы получаем возможность применять к исследованию V_K аппарат теории аналитических многообразий (см. Серр [3]). Обратим внимание читателя на ряд необходимых нам для дальнейшего понятий. С каждой точкой x аналитического многообразия X связывается касательное пространство $T_x^*(X)$*), которое является векторным пространством над K размерности, равной размерности X, т. е. размерности того аффинного пространства, при помощи областей которого происходит параметризация окрестностей точек X. Морфизмом $f\colon X \to Y$ аналитических многообразий называется непрерывное локально аналитическое отображение, в том смысле, что f индуцирует обычное аналитическое отображение областей параметризации соответствующих точек. Любой морфизм $f\colon X \to Y$ индуцирует линейное отображение $d_x^* f\colon T_x^*(X) \to T_{f(x)}^*(Y)$, называемое *дифференциалом* f в точке. Морфизм f называется *иммерсией в точке* $x \in X$, если $d_x^* f$ инъективно, и просто *иммерсией*, если это выполняется для всех точек. Если топологическое подпространство X многообразия Y также наделено структурой аналитического многообразия и отображение включения $X \hookrightarrow Y$ является иммерсией, то X называется подмногообразием в Y. Поясняющий это понятие пример «не подмногообразия» в $\mathbb{R}^2$ доставляет множество $y = |x|$, см. рис.



*) Мы используем звездочку для того, чтобы в дальнейшем различать касательные пространства к алгебраическому многообразию и к соответствующему аналитическому многообразию.

(Данное множество «негладко» вложено в $\mathbb{R}^2$. Подмногообразие же при подходящей аналитической замене координат можно задать линейными уравнениями в окрестности любой точки.) Нам понадобится также следующий критерий открытости отображения.

Предложение 2. *Пусть $f\colon X \to Y$ — морфизм аналитических многообразий, $x \in X$. Если дифференциал $d_x^* f\colon T_x^*(X) \to T_{f(x)}^*(Y)$ сюръективен, то f является открытым отображением в точке x.*

Доказательство легко получается из теоремы 2 об обратной функции, см. Серр [4], ч. II, гл. III, § 10.

Лемма 1. *Пусть V — определенное над K алгебраическое многообразие, $x \in V_K$. Тогда $T_x^*(\tilde{V}_K) = T_x(V)_K$, т. е. «аналитическое» касательное пространство совпадает с множеством K-элементов «алгебраического» касательного пространства. Если $f\colon V \to W$ — определенное над K регулярное отображение алгебраических K-многообразий, $x \in \tilde{V}_K$, $f(x) \in \tilde{W}_K$, то $d_x^* f = (d_x f) \mid T_x^*(\tilde{V}_K)$.*

Доказательство без труда вытекает из сравнения соответствующих определений.

Предложение 2 и лемма 1 применяются к алгебраическим многообразиям в следующей форме:

Предложение 3. *Пусть $f\colon V \to W$ — доминантный K-определенный морфизм неприводимых алгебраических K-многообразий. Тогда, если $x \in V_K$ — такая простая точка, что точка $f(x)$ является простой на многообразии W и дифференциал $d_x f\colon T_x(V) \to T_{f(x)}(W)$ сюръективен, то отображение $f_K\colon V_K \to W_K$ является открытым в точке x. Следовательно, существует такое открытое по Зарисскому подмножество $U \subset V$, что f_K является открытым в любой точке $x \in U_K$.*

Доказательство. Рассмотрим отвечающее f аналитическое отображение $\tilde{f}\colon \tilde{V}_K \cap f^{-1}(\tilde{W}_K) \to \tilde{W}_K$. Из наших условий на точку x и леммы 1 вытекает, что $x \in \tilde{V}_K \cap f^{-1}(\tilde{W}_K)$, $f(x) \in \tilde{W}_K$, и дифференциал $d_x^* \tilde{f}$ является сюръективным отображением. Поэтому открытость f_K в точке x непосредственно следует из предложения 2. Далее, так как по предположению $\operatorname{char} K = 0$, то морфизм f автоматически является сепарабельным, т. е. сепарабельно соответствующее расширение $K(V)/K(W)$ полей рациональных функций. Отсюда следует (см. Борель [8] и АГ, § 17) существование такого открытого по Зарисскому подмножества $U \subset V$, что для любой точки $x \in U$ выполняются условия, указанные в формулировке предложения, и все доказано.

Следует заметить, что если не предполагать множество V_K плотным в V, то U_K может оказаться пустым, и предложение 4 становится бессодержательным. Поэтому сейчас мы опишем две ситуации, в которых такого вырождения не происходит (именно с ними мы в дальнейшем и будем иметь дело).

Следствие 1. *Пусть в условиях предложения 4 многообразие V является гладким и $V_K \neq \varnothing$. Тогда образ $f_K(F)$ любого открытого множества $F \subset V_K$ содержит непустое открытое в W_K множество. В частности, если f: $G \to H$ — сюръективный K-гомоморфизм алгебраических K-групп, то $f_K(G_K)$ — открытая подгруппа в H_K.*

Доказательство использует следующее утверждение.

Лемма 2. *Пусть V — неприводимое гладкое K-многообразие. Предположим, что $V_K \neq \varnothing$. Тогда для любого непустого K-открытого по Зарисскому множества $U \subset V$ множество U_K плотно в V_K в v-адической топологии. С другой стороны, любое непустое открытое в v-адической топологии подмножество $F \subset V_K$ плотно в V в топологии Зарисского, в частности, V_K плотно в V.*

Доказательство. Нетрудно видеть, что оба утверждения леммы сводятся к доказательству непустоты пересечения $U \cap F$, где $U \subset V$ — открыто по Зарисскому, а $F \subset V_K$ — в топологии, определяемой нормированием. Положим $X = V \setminus U$. Тогда, если мы зафиксируем некоторую точку $x \in F$, то найдется ненулевая регулярная в K-определенной окрестности $W \subset V$ функция $f \in K[W]$, тождественно равная нулю на $X \cap W$. Поскольку по условию многообразие V является гладким, то точка x проста, и, следовательно, согласно предыдущему, существует аналитическая параметризация некоторой окрестности x. Если теперь предположить, что $U \cap F = \varnothing$, т. е. $F \subset X$, то аналитический ряд Тейлора функции f обязан быть нулевым. Так как ряды Тейлора в алгебраическом и аналитическом смыслах совпадают, то последнее противоречит инъективности отображения, сопоставляющего функции, регулярной в простой точке, ее алгебраический ряд Тейлора (см. Шафаревич [1], гл. II). Лемма 2 доказана.

Пусть теперь $U \subset V$ — открытое по Зарисскому подмножество, построенное в предложении 3. Тогда согласно лемме 2 $U \cap F \neq \varnothing$. Так как f_K: $V_K \to W_K$ является открытым в любой точке $x \in U \cap F$, то отсюда вытекает наше первое утверждение. Второе утверждение следствия 1 непосредственно следует из первого.

Следствие 2. *Пусть $G \times X \to X$ — определенное над K действие связной алгебраической K-группы G на многообразии X. Если $x \in X_K$ и Y — замыкание орбиты Gx, то для любого открытого $F \subset G_K$ множество Fx открыто в Y_K.*

Доказательство. Рассмотрим морфизм φ: $G \to Y$, $\varphi(g) = gx$. По построению φ является доминантным, и поэтому, применяя предложение 3, можно найти открытое по Зарисскому множество $U \subset G$ с описанными там свойствами. Тогда φ_K является открытым в любой точке $g \in U_K$. Так как $\varphi(hg) = h\varphi(g)$ для любого $h \in G$, то φ_K в действительности является открытым

в любой точке $h \in G_K$. Отсюда автоматически вытекает открытость $\varphi(F) = Fx$ для любого открытого $F \subset G_K$.

Приведем пример использования полученных результатов применительно к изучению структуры групп рациональных точек над локально компактными полями.

Теорема 3 (Рим [1, 2]). *Пусть G — K-простая алгебраическая группа. Тогда любой нецентральный нормальный делитель группы G_K является открытым.*

Доказательство. Для $g \in G$ положим $W_g = \{[g, h] = g^{-1}h^{-1}gh \mid h \in G\}$. Все множества $W_g (g \in G)$ являются неприводимыми многообразиями, содержат единицу и в совокупности порождают коммутант $[G, G]$ группы G. В нашей ситуации $[G, G] = G$, так что, применяя несложное рассуждение, использующее понятие размерности (см. Борель [8], предложение 2.2), и учитывая равенство $(W_g)^{-1} = W_{g^{-1}}$, получаем существование такого конечного набора элементов $g_1, \ldots, g_n \in G$, что $G = W_{g_1} \ldots W_{g_n}$. Рассмотрим морфизм

$$\psi\colon X = \underbrace{G \times \ldots \times G}_{2n} \to \underbrace{G \times \ldots \times G}_{n+1} = Y,$$

$$\psi(x_1, \ldots, x_n, y_1, \ldots, y_n) = (x_1, \ldots, x_n, [x_1, y_1] \ldots [x_n, y_n]).$$

Согласно теореме о размерности слоев морфизма (см. § 2.4, п. 2) для любой точки $y \in \psi(X)$ имеем $\dim \psi^{-1}(y) \geqslant (n-1)\dim G$; установим существование таких точек, для которых имеет место равенство. По построению морфизм $\varphi_{g_1, \ldots, g_n}$:

$$\underbrace{G \times \ldots \times G}_{n} \to G, \quad \varphi_{g_1, \ldots, g_n}(x_1, \ldots, x_n) = [g_1, x_1] \ldots [g_n, x_n]$$

сюръективен, поэтому существуют такие точки $g \in G$, что

$$\dim \varphi^{-1}_{g_1, \ldots, g_n}(g) = (n-1)\dim G.$$

Тогда в качестве y можно взять точку вида $(g_1, \ldots, g_n, g)$. Опять применяя теорему о размерности слоев морфизма, получаем существование такого открытого по Зарисскому множества $U \subset Y$, что $\dim \varphi^{-1}(x) = (n-1)\dim G$ для любого $x \in U$. Обозначим через V проекцию U на первые n компонент. Тогда V открыто в $\underbrace{G \times \ldots \times G}_{n}$ и для любого $(x_1, \ldots, x_n) \in V$ найдется $g \in G$ со свойством $\dim \varphi^{-1}_{x_1, \ldots, x_n}(g) = n-1$. Отсюда следует, что для $(x_1, \ldots, x_n) \in V$ морфизм $\varphi_{x_1, \ldots, x_n}$ является доминантным. Пусть теперь $N \subset G_K$ — нецентральный нормальный делитель. Так как G_K плотно в G в топологии Зарисского (теорема 2.2; для локального поля это вытекает также из леммы 2),

то замыкание $\bar{N}$ в этой топологии является нецентральным K-определенным нормальным делителем в G, и, следовательно, $\bar{N}=G$, ибо G по условию K-проста. Поэтому из приведенных выше рассуждений следует, что найдутся такие элементы $x_1, \ldots, x_n \in N$, что морфизм $\varphi_{x_1, \ldots, x_n}$ является доминантным. Применяя следствие 1 из предложения 3, получаем, что $\varphi_{x_1, \ldots, x_n}(G_K \times \ldots \times G_K)$ содержит открытое в G_K подмножество. Но $\varphi_{x_1, \ldots, x_n}(G_K \times \ldots \times G_K) = \{[x_1, h_1] \ldots [x_n, h_n] \mid h_i \in G_K\} \subset N$, поэтому N открыт в G_K. Теорема 3 доказана.

Замечание. В доказательстве мы пользовались только предложением 3, которое является формальным следствием теоремы об обратной функции, и нигде не использовали локальную компактность поля K. Поэтому утверждение теоремы имеет место всякий раз, когда над полем K справедлива теорема об обратной функции, скажем, K является полным относительно нетривиального дискретного нормирования. Именно в такой общности данный факт применяется при исследовании отклонения от свойства слабой аппроксимации для односвязных групп над произвольным полем (см. § 7.3). Отметим также, что для локально компактных полей из теоремы 3 можно получить (и мы это проделаем в § 3.2—3.3) более сильный результат: в условиях теоремы 3 любой нецентральный нормальный делитель группы G_K имеет в ней конечный индекс.

В изложенных выше результатах теории аналитических многообразий мы фактически игнорировали тот факт, что на большинстве изучаемых нами многообразий имеется структура группы. Сейчас мы представим ряд результатов, которые получаются благодаря использованию групповой структуры. В целом изучение групповых аналитических многообразий составляет предмет классической теории групп Ли, изложению которой посвящены, например, книги Серра [3], Бурбаки [4], Хелгасона [1]. Мы же ограничимся указанием на ряд фактов, относящихся, главным образом, к группам Ли, возникающим из алгебраических групп. Итак, пусть G — определенная над K алгебраическая группа. Как мы знаем, многообразие G является гладким, поэтому на множестве G_K имеется естественная структура аналитического многообразия над K. При этом групповые операции оказываются аналитическими отображениями, так что в действительности G_K оказывается наделенной структурой аналитической группы или группы Ли (см. Серр [3]). *Алгеброй Ли* $\mathfrak{g}^*$ аналитической группы G_K называется касательное пространство в единице $T_e^*(G_K)$. Согласно лемме 1 $\mathfrak{g}^*$ совпадает с подпространством K-элементов алгебраического касательного пространства $T_e(G)$, т. е. алгебры Ли $\mathfrak{g}=L(G)$ как алгебраической группы; при этом скобка Ли на $\mathfrak{g}^*$ индуцируется с $\mathfrak{g}$.

Можно определить экспоненциальное и логарифмическое отображения exp и log (см. Бурбаки [4]), которые осуществляют взаимно обратные локальные аналитические изоморфизмы $\mathfrak{g}^*$ и G_K. Если $G \subset GL_n(\Omega)$ — матричная реализация G, то exp и log задаются обычными формулами:

$$\begin{gathered}\exp(X) = E_n + \frac{X}{1!} + \frac{X^2}{2!} + \ldots + \frac{X^m}{m!} + \ldots, \quad X \in \mathfrak{g}^*, \\ \log(x) = (x - E_n) - \frac{(x-E_n)^2}{2} + \ldots + (-1)^{m-1}\frac{(x-E_n)^m}{m} + \ldots, \\ x \in G_K.\end{gathered} \tag{1}$$

В частности, экспоненциальное отображение группы индуцирует экспоненциальное отображение подгруппы. Если $X, Y \in \mathfrak{g}$ (соответственно, $x, y \in G$) перестановочны, то

$$\exp(X+Y) = \exp(X)\exp(Y),$$
$$\log(xy) = \log(x) + \log(y)$$

(при этом предполагается, что все участвующие здесь выражения определены, т. е. соответствующие ряды сходятся). Отсюда, в частности, следует, что в группе G_K всегда существует окрестность единицы, не содержащая нетривиальных элементов конечного порядка (см. Серр [4]). Отметим также следующие формулы:

$$\begin{gathered}\exp(x^{-1}Xx) = x^{-1}\exp(X)x, \\ \log(x^{-1}yx) = x^{-1}\log(y)x,\end{gathered} \tag{2}$$

т. е. экспоненциальное и логарифмическое отображения коммутируют с присоединенным действием группы G_K.

Если подгруппа $H \subset G_K$ является также подмногообразием в G_K, то H называется подгруппой Ли в G_K. Из определений вытекает, что если $H \subset G_K$ — подгруппа Ли, то имеет место аналогичное включение для соответствующих алгебр Ли: $\mathfrak{h}^* \subset \mathfrak{g}^*$. Подгруппа Ли $H \subset G_K$ не обязана быть замкнутой ни в топологии группы G_K, ни тем более в топологии Зарисского. Рассмотрим замыкание B группы H в топологии Зарисского. Тогда B_K является подгруппой Ли в G_K, содержащей H. Насколько B_K может отличаться от H? Мы дадим ответ в терминах соответствующих алгебр Ли $\mathfrak{b}^*$ и $\mathfrak{h}^*$.

Предложение 4. *В описанной ситуации $\mathfrak{h}^*$ является идеалом $\mathfrak{b}^*$.*

Доказательство. Рассмотрим присоединенное представление $\mathrm{Ad}\colon G \to GL(\mathfrak{g})$, где $\mathfrak{g} = L(G)$ — алгебра Ли G как алгебраической группы; $\mathfrak{g} = \mathfrak{g}^* \otimes_K \Omega$, где $\mathfrak{g}^*$ — алгебра Ли G_K как аналитической группы. Пространство $\mathfrak{h}^*$, а следовательно, и пространство $\mathfrak{h} = \mathfrak{h}^* \otimes_K \Omega$ являются, очевидно, H-инвариантными. С другой стороны, подгруппа $S \subset G$, состоящая из таких $g \in G$, что $\mathrm{Ad}(g)(\mathfrak{h}) = \mathfrak{h}$, замкнута в топологии Зарисского. Поэтому из

включения $H \subset S$ вытекает, что и $B \subset S$. Учитывая, что дифференциал присоединенного представления алгебраической группы совпадает с присоединенным представлением соответствующей алгебры Ли (см. Борель [8], § 3), для алгебры Ли $\mathfrak{b} = L(B)$ получаем включение $[\mathfrak{b}, \mathfrak{b}] \subset \mathfrak{b}$. Так как $\mathfrak{b}^* \subset \mathfrak{b}_K$, $\mathfrak{b}^* = \mathfrak{b}_K$, то отсюда следует, что $[\mathfrak{b}^*, \mathfrak{b}^*] \subset \mathfrak{b}^*$. Предложение 4 доказано.

Краткий обзор необходимых для дальнейшего фактов теории групп Ли мы завершим формулировкой теоремы Картана.

Теорема 4 (Э. Картан). *Предположим, что поле K совпадает либо с полем вещественных чисел $\mathbb{R}$, либо с полем p-адических чисел $\mathbb{Q}_p$. Тогда замкнутая подгруппа группы Ли над K является группой Ли. Всякий непрерывный гомоморфизм групп Ли над K является аналитическим.*

Доказательство — см. Серр [3], с. 260—263.

В заключение этого параграфа приведем один красивый пример применения техники групп Ли и аналитических многообразий к теории групп.

Предложение 5. *Пусть $G \subset GL_n$ — редуктивная алгебраическая группа, определенная над неархимедовым локальным полем K. Тогда в группе целых точек $G_{\mathcal{O}} = G \cap GL_n(\mathcal{O})$ имеется лишь конечное число попарно не сопряженных конечных подгрупп. В частности, число несопряженных конечных подгрупп группы $SL_n(\mathbb{Z}_p)$ конечно.*

Доказательство. Из сделанных выше замечаний о группах Ли вытекает существование окрестности единицы группы $G_{\mathcal{O}}$, не содержащей нетривиальных элементов конечного порядка. Так как конгруэнц-подгруппы $G_{\mathcal{O}}(\mathfrak{p}^\alpha) = \{x \in G_{\mathcal{O}} \mid x \equiv E_n (\mathrm{mod}\, \mathfrak{p}^\alpha)\}$ *), где $\mathfrak{p} \subset \mathcal{O}$ — идеал нормирования, $\alpha \geqslant 1$, образуют базис окрестностей единицы, то найдется конгруэнц-подгруппа (скажем, $G_{\mathcal{O}}(\mathfrak{p}^\alpha)$), обладающая тем же свойством. Отсюда следует, что любая конечная подгруппа в $G_{\mathcal{O}}$ изоморфна подгруппе группы $G_{\mathcal{O}}/G_{\mathcal{O}}(\mathfrak{p}^\alpha)$, которая конечна в силу компактности $G_{\mathcal{O}}$ и открытости $G_{\mathcal{O}}(\mathfrak{p}^\alpha)$. Поэтому в $G_{\mathcal{O}}$ существует лишь конечное число неизоморфных конечных подгрупп, и достаточно показать, что конечные подгруппы в $G_{\mathcal{O}}$, изоморфные фиксированной группе Γ, разбиваются в конечное число классов сопряженности. Для этого рассмотрим многообразие представлений $R = R(\Gamma, G)$ (см. § 2.4, п. 4) и установим более сильное утверждение о том, что множество $R_{\mathcal{O}} = \mathrm{Hom}(\Gamma, G_{\mathcal{O}})$ состоит из конечного числа орбит относительно естественного действия группы $G_{\mathcal{O}}$. Из теоремы 2.17 вытекает, что имеется лишь конечное число орбит естественного действия G на $R(\Gamma, G)$, причем эти орбиты

---

*) Сравнимость двух матриц над некоторым кольцом по модулю идеала этого кольца означает сравнимость всех соответствующих элементов.

замкнуты в топологии Зарисского. Пусть X — одна из таких орбит. Нам достаточно показать, что $X_{\mathcal{O}}$ состоит из конечного числа орбит группы $G_{\mathcal{O}}$. Это очевидно, если $X_{\mathcal{O}} = \varnothing$. В противном случае орбита X, очевидно, определена над K, и для любой точки $x \in X_{\mathcal{O}}$ орбита $G_{\mathcal{O}}x$ открыта в $X_{\mathcal{O}}$ согласно следствию 2 из предложения 3. С другой стороны, из замкнутости X в R и компактности $\mathcal{O}$ вытекает компактность $X_{\mathcal{O}}$, поэтому из открытого покрытия $X_{\mathcal{O}} = \bigcup_x G_{\mathcal{O}}x$ можно выбрать конечное подпокрытие, что и даст требуемую конечность числа орбит $G_{\mathcal{O}}$ на $X_{\mathcal{O}}$. Предложение 5 доказано.

§ 3.2. Архимедов случай

В предыдущем параграфе был получен ряд утверждений об элементарных топологических и аналитических свойствах пространства X_K, где X — алгебраическое многообразие, определенное над локально компактным полем K. Соответствующие доказательства опирались лишь на теорему об обратной функции, которая одинаково хорошо работает как в «классическом» случае $K = \mathbb{R}$ или $\mathbb{C}$, так и в неархимедовом, когда K — конечное расширение поля $\mathbb{Q}_p$. В настоящем параграфе мы приведем ряд утверждений, которые присущи исключительно архимедову случаю. К их числу прежде всего относятся результаты о связности.

Теорема 5. *Пусть X — неприводимое алгебраическое многообразие, определенное над полем комплексных чисел $\mathbb{C}$. Тогда пространство $X_{\mathbb{C}}$ связно.*

Доказательство — см. Шафаревич [1], гл. VII, § 2. Отметим, что этот результат в данной книге использоваться не будет.

Теорема 6 (Уитни [1]). *Пусть X — алгебраическое многообразие, определенное над полем вещественных чисел $\mathbb{R}$. Тогда пространство $X_{\mathbb{R}}$ имеет конечное число связных компонент.*

Доказательство. Заменяя X на замыкание $X_{\mathbb{R}}$ в топологии Зарисского (что не влияет на $\mathbb{R}$-точки), можно считать, что $X_{\mathbb{R}}$ плотно в X. Тогда вещественные точки плотны в каждой неприводимой компоненте X, и поэтому последние определены над $\mathbb{R}$. Тем самым можно считать X неприводимым. Предположим, что утверждение теоремы для таких многообразий не выполняется, и пусть X — контрпример минимальной размерности (ясно, что $\dim X > 0$). Выберем открытое $\mathbb{R}$-определенное аффинное подмножество $Y \subset X$. Тогда $T = X \setminus Y$ является алгебраическим $\mathbb{R}$-многообразием, размерность которого строго меньше $\dim X$. По предположению $T_{\mathbb{R}}$ имеет конечное число связных компонент, так что число связных компонент пространства $Y_{\mathbb{R}}$ обязано быть бесконечным. По этой причине многообразие X можно считать аффинным. Пусть S — множество особых точек X (см.

§ 2.4, п. 3). Как мы знаем, S — собственное замкнутое подмножество в X. Поэтому рассуждая как и выше, получим, что пространство $V = X_{\mathbb{R}} \setminus S_{\mathbb{R}}$ имеет бесконечное число связных компонент $\{V_j\}_{j=1}^{\infty}$, причем почти все из них, скажем, V_j для $j \geqslant l$ являются связными компонентами пространства $X_{\mathbb{R}}$. В § 3.1 мы показали, что V является аналитическим многообразием, и, в частности, локально связным пространством. Поэтому все V_j являются непересекающимися открыто-замкнутыми подмножествами в V, а V_j для $j \geqslant l$ — открыто-замкнутыми подмножествами в $X_{\mathbb{R}}$. Предположим, что нам удалось найти собственное замкнутое $\mathbb{R}$-определенное подмножество $Z \subset X$, пересекающее почти все V_j. Тогда число связных компонент пространства $Z_{\mathbb{R}}$ не может быть конечным, ибо $Z_{\mathbb{R}} = \bigcup_{j=1}^{\infty} (Z_{\mathbb{R}} \cap V_j)$ и для почти всех j пересечение $Z_{\mathbb{R}} \cap V_j$ является непустым открыто-замкнутым подмножеством в $Z_{\mathbb{R}}$. Но это противоречит нашим построениям, ибо $\dim Z < \dim X$.

Для построения Z предположим, что X реализовано как замкнутое по Зарисскому подмножество аффинного пространства $\mathbb{A}^n$, множество вещественных точек $\mathbb{R}^n$ которого наделим обычной метрикой. Зафиксируем произвольную точку $a = (a_1, \ldots, a_n) \in V_1$. Для каждого $j \geqslant l$ множество V_j замкнуто в $\mathbb{R}^n$, и поэтому можно найти точку $b_j \in V_j$, ближайшую к a. Мы построим собственное замкнутое алгебраическое подмножество $Z \subset X$, содержащее все b_j. Его уравнения легко получить, исходя из того, что b_j являются точками условного экстремума функции $g(X_1, \ldots, X_n) = (X_1 - a_1)^2 + \ldots + (X_n - a_n)^2$. А именно, если $r = n - \dim X$, а — идеал полиномов, обращающихся в нуль на X, то для любых $f_1, \ldots, f_r \in \mathfrak{a}_{\mathbb{R}}$ и любого j линейные формы

$$d_{b_j} f_1, \ldots, d_{b_j} f_r, d_{b_j} g$$

(см. § 2.4, п. 3) *являются линейно зависимыми*, что равносильно выполнению равенств

$$\Delta_i (f_1, \ldots, f_r, g)(b_j) = 0, \quad i = 1, \ldots, C_n^{r+1},$$

где $\Delta_i(f_1, \ldots, f_r, g)(x)$ — все миноры порядка $(r+1) \times (r+1)$ матрицы

$$\begin{pmatrix} \frac{\partial f_1}{\partial X_1}(x) & \ldots & \frac{\partial f_1}{\partial X_n}(x) \\ \cdots & \cdots & \cdots \\ \frac{\partial f_r}{\partial X_1}(x) & \ldots & \frac{\partial f_r}{\partial X_n}(x) \\ \frac{\partial g}{\partial X_1}(x) & \ldots & \frac{\partial g}{\partial X_n}(x) \end{pmatrix}.$$

Пусть Z — подмножество в X, определяемое системой

$$\Delta_i(f_1, \ldots, f_r, g)(x) = 0, \quad i = 1, \ldots, C_n^{r+1}, \quad f_1, \ldots, f_r \in \mathfrak{a}.$$

По построению Z содержит все точки b_i, поэтому надо только убедиться, что $Z \neq X$. Покажем, что $V_1 \not\subset Z$. Так как точка a является простой на X, то существуют такие полиномы $f_1, \ldots, f_r \in \mathfrak{a}_{\mathbf{R}}$, что формы $d_x f_1, \ldots, d_x f_r$ линейно независимы для $x = a$ (предложение 2.1), а значит, и для всех x, достаточно близких к a. Далее, пусть аналитические функции $u_1(t_1, \ldots, t_d), \ldots, u_n(t_1, \ldots, t_d)$ $(d = \dim X > 0)$ осуществляют параметризацию окрестности точки a (см. § 3.1). Так как g представляет собой квадрат расстояния от точки a, то аналитическая функция $\varphi(t_1, \ldots, t_d) = g(u_1(t_1, \ldots, t_d), \ldots, u_n(t_1, \ldots, t_d))$ не сводится к константе. Поэтому

$$\left(\frac{\partial\varphi}{\partial t_1}, \ldots, \frac{\partial\varphi}{\partial t_d}\right) \not\equiv (0, \ldots, 0) \tag{1}$$

на любом открытом множестве изменения параметров. Из равенств

$$f_i(u_1(t_1, \ldots, t_d), \ldots, u_n(t_1, \ldots, t_d)) = 0, \quad i = 1, \ldots, r,$$

вытекают соотношения

$$(d_x f_i)\left(\frac{\partial u_1}{\partial t_j}; \ldots; \frac{\partial u_n}{\partial t_j}\right) = \sum_{k=1}^{n} \frac{\partial f_i}{\partial X_k} \cdot \frac{\partial u_k}{\partial t_j} = 0,$$

$$i = 1, \ldots, r, \quad j = 1, \ldots, d.$$

Тогда если формы $d_x f_1, \ldots, d_x f_r, d_x g$ линейно зависимы, то для всех x, достаточно близких к a, $d_x g$ линейно выражается через $d_x f_1, \ldots, d_x f_r$, ибо последние по построению линейно независимы. Следовательно,

$$(d_x g)\left(\frac{\partial u_1}{\partial t_j}; \ldots; \frac{\partial u_n}{\partial t_j}\right) = \sum_{k=1}^{n} \frac{\partial g}{\partial X_k} \cdot \frac{\partial u_k}{\partial t_j} = 0, \quad j = 1, \ldots, d. \tag{2}$$

Но левая часть (2) совпадает с $\partial\varphi/\partial t_j$, так что (2) противоречит (1). Таким образом, формы $d_x f_1, \ldots, d_x f_r, d_x g$ не могут быть линейно зависимыми во всех точках $x \in V_1$. Поэтому не все определители $\Delta_i(f_1, \ldots, f_r, g)(x)$ тождественно равны нулю на V_1, т. е. $V_1 \not\subset Z$. Теорема 6 доказана.

Следствие 1. *Пусть G — алгебраическая $\mathbf{R}$-определенная группа. Тогда группа $G_{\mathbf{R}}$ имеет конечное число связных компонент. Если группа G связна, то из компактности группы $G_{\mathbf{R}}$ вытекает ее связность.*

В доказательстве нуждается лишь второе утверждение. Группа $G_{\mathbf{R}}$, будучи компактной, целиком состоит из полупростых

элементов. Поэтому произвольный фиксированный ее элемент лежит в некотором (своём) $\mathbb{R}$-определенном торе $T \subset G$. Группа $T_{\mathbb{R}}$ также компактна, и поэтому T изоморфен тору вида $(\mathbf{R}^{(1)}_{\mathbb{C}/\mathbb{R}}(\boldsymbol{G}_m))^d$, где $d = \dim T$ (см. § 2.2, п. 4). Отсюда следует, что $T_{\mathbb{R}}$ можно отождествить с произведением d экземпляров единичной окружности, которое связно. Таким образом, связная компонента $G^0_{\mathbb{R}}$ обязана содержать все группы $T_{\mathbb{R}}$, и поэтому совпадает с $G_{\mathbb{R}}$. Другое доказательство связности группы $G_{\mathbb{R}}$ можно получить, воспользовавшись тем фактом, что компактная линейная группа над $\mathbb{R}$ замкнута в топологии Зариского (см. Шевалле [1], т. 3, с. 296).

Предложение 6. *Пусть G — связная $\mathbb{R}$-простая алгебраическая группа. Тогда любой нецентральный нормальный делитель группы $G_{\mathbb{R}}$ имеет в ней конечный индекс. Если группа $G_{\mathbb{R}}$ компактна, то она проективно проста.*

Доказательство. Согласно теореме 3 любой нецентральный нормальный делитель N группы $G_{\mathbb{R}}$ открыт и поэтому обязан содержать связную компоненту $G^0_{\mathbb{R}}$, которая в силу следствия 1 имеет конечный индекс в $G_{\mathbb{R}}$. Если группа $G_{\mathbb{R}}$ компактна, то $G_{\mathbb{R}} = G^0_{\mathbb{R}}$, и поэтому $N = G_{\mathbb{R}}$.

Продолжим получение следствий из теоремы 6.

Следствие 2. *Пусть $G \times X \to X$ — транзитивное $\mathbb{R}$-определенное действие алгебраической $\mathbb{R}$-группы G на $\mathbb{R}$-многообразии X. Тогда $X_{\mathbb{R}}$ состоит из конечного числа орбит группы $G_{\mathbb{R}}$. Если $X_{\mathbb{R}}$ связно, то имеется в точности одна орбита.*

Доказательство. Для любой точки $x \in X_{\mathbb{R}}$ орбита $G_{\mathbb{R}}x$ открыта в $X_{\mathbb{R}}$ (следствие 2 из предложения 4). Дополнение $X_{\mathbb{R}} \setminus G_{\mathbb{R}}x$ является объединением остальных орбит, и поэтому также открыто. Тем самым $G_{\mathbb{R}}x$ является открыто-замкнутым подмножеством пространства $X_{\mathbb{R}}$ и поэтому содержит связную компоненту последнего. Поэтому число различных орбит не превосходит числа связных компонент $X_{\mathbb{R}}$, которое конечно, и равно единице, если $X_{\mathbb{R}}$ связно.

Замечание. Следствие 2 имеет очевидную когомологическую интерпретацию. А именно, если $x \in X_{\mathbb{R}}$, то X можно отождествить с однородным пространством G/H, где $H = G(x)$ — стабилизатор точки x, и тогда орбиты группы $G_{\mathbb{R}}$ на пространстве $X_{\mathbb{R}}$ взаимно однозначно соответствуют элементам из $\operatorname{Ker}(H^1(\mathbb{R}, H) \to H^1(\mathbb{R}, G))$ (см. § 1.3, п. 2). Поэтому в силу следствия 2 указанное ядро конечно. Рассматривая вложение данной $\mathbb{R}$-группы H в некоторую $\mathbb{R}$-группу G с тривиальными когомологиями (например, при помощи точного $\mathbb{R}$-определенного представления $H \hookrightarrow G = \boldsymbol{GL}_n$), отсюда получаем, что для любой $\mathbb{R}$-группы H множество $H^1(\mathbb{R}, H)$ конечно. В главе VI § 6.4 мы

дадим другое доказательство этого факта, которое работает также в случае неархимедовых локальных полей.

Следствие 3. *Пусть f: $G \to H$ — сюръективный $\mathbb{R}$-определенный морфизм алгебраических групп. Тогда индекс $[H_{\mathbb{R}} : f(G_{\mathbb{R}})]$ конечен. Если группа $H_{\mathbb{R}}$ связна, в частности, если H унипотентна, то гомоморфизм $f_{\mathbb{R}}$: $G_{\mathbb{R}} \to H_{\mathbb{R}}$ сюръективен.*

Доказательство вытекает из следствия 2, если применить его к действию $G \times H \to H$, $(g, h) \to f(g)h$. Связность множества $\mathbb{R}$-точек унипотентной группы H является следствием того обстоятельства, что логарифмическое «усеченное» отображение определяет гомеоморфизм $H_{\mathbb{R}}$ и $L(H)_{\mathbb{R}}$, где $L(H)$ — алгебра Ли группы H (см. § 2.1, п. 8).

Дальнейшие результаты этого параграфа направлены на более точное изучение алгебраической и топологической структуры групп вещественных и комплексных точек редуктивных алгебраических групп. А именно, мы хотим получить для таких групп полярное разложение и разложение Ивасавы. Чтобы прояснить существо дела, мы вначале рассматриваем наиболее простой случай группы $\boldsymbol{GL}_n$. В этой ситуации обсуждаемые разложения легко следуют из хорошо известных фактов линейной алгебры.

Начнем с полярного разложения для группы $GL_n(\mathbb{R})$.

Обозначим через $\boldsymbol{K}$ подгруппу в $GL_n(\mathbb{R})$, состоящую из ортогональных матриц, т. е. матриц $x \in GL_n(\mathbb{R})$, удовлетворяющих соотношению

$$^t x x = E_n, \tag{3}$$

где $^t x$ — транспонированная к x матрица. Ясно, что $\boldsymbol{K}$ совпадает с группой $\mathbb{R}$-точек $O_n(f)_{\mathbb{R}}$ ортогональной группы единичной квадратичной формы $f = x_1^2 + \ldots + x_n^2$. Эта форма анизотропна над $\mathbb{R}$, и поэтому группа $O_n(f)$ также является $\mathbb{R}$-анизотропной (см. предложение 2.14). Но тогда из теоремы 1 вытекает, что группа $\boldsymbol{K} = O_n(f)_{\mathbb{R}}$ компактна. Последний факт легко доказать и непосредственно, выписав возникающие из (3) соотношения на коэффициенты матрицы x. Обозначим, далее, через S множество положительно определенных симметрических матриц из $GL_n(\mathbb{R})$, т. е. $a = (a_{ij}) \in S$, если $a_{ij} = a_{ji}$ и квадратичная форма $f = \sum_{i,j=1}^{n} a_{ij} x_i x_j$ положительно определена. В этих обозначениях имеет место

Предложение 7. *$GL_n(\mathbb{R}) = \boldsymbol{K}S$ и представление справа единственно. Пространство S связно и односвязно.*

Доказательство. Пусть $x \in GL_n(\mathbb{R})$. Тогда $a = {}^t x x \in S$ и, значит, собственные значения $\alpha_1, \ldots, \alpha_n$ линейного преобразования, определяемого a, вещественны и положительны. Из линейной алгебры хорошо известно существование такого $b \in \boldsymbol{K}$, что bab^{-1} является диагональной матрицей $\operatorname{diag}(\alpha_1, \ldots, \alpha_n)$.

Обозначим через c матрицу $b^{-1}db$, где $d = \operatorname{diag}(\sqrt{a_1}, \ldots, \sqrt{a_n})$ (берутся положительные значения корня). Тогда $c \in S$ и ${}^t cc = c^2 = a$. Итак, $a = {}^t xx = {}^t cc$, откуда ${}^t(xc^{-1})(xc^{-1}) = E_n$, т. е. $z = xc^{-1} \in K$. Тем самым $x = zc \in KS$. Если $x = z_1c_1$ — другое представление, то, применяя к равенству

$$zc = z_1c_1 \tag{4}$$

транспонирование, получим

$$cz^{-1} = c_1z_1^{-1}. \tag{5}$$

Перемножая (4) и (5), будем иметь

$$c^2 = c_1^2.$$

Отсюда следует, что $c = c_1$. Это можно доказать разными способами, но нам удобнее всего использовать следующее утверждение, к которому мы будем еще не раз обращаться.

Лемма 3. *Пусть $c \in S$. Тогда для любого целого r замыкание по Зарисскому циклической подгруппы, порожденной c^r, содержит c.*

Доказательство. Как мы уже отмечали, сопряжение при помощи подходящего элемента x приводит c к диагональному виду, так что с самого начала можно считать матрицу c диагональной, т. е. $c = \operatorname{diag}(\gamma_1, \ldots, \gamma_n)$, $\gamma_i > 0$. Если $c \notin \{c^{rn}\}_{n \in \mathbb{Z}}$, то найдется такой характер χ группы диагональных матриц D_n, что $\chi(c^r) = 1$, но $\chi(c) \neq 1$ (см. Борель [8]). Однако $\chi(c) = \gamma_1^{a_1} \ldots \gamma_n^{a_n}$ для подходящих целых a_i, и поэтому $\chi(c) \in \mathbb{R}^{>0}$. Так как $\chi(c^r) = (\chi(c))^r = 1$, то отсюда следует, что $\chi(c) = 1$, — противоречие. Лемма 3 доказана.

Из леммы 3 вытекает, что элементы $c, c_1 \in S$, удовлетворяющие соотношению $c^2 = c_1^2$, обязательно перестановочны. Тогда для $d = cc_1^{-1}$ имеем $d^2 = E_n$, так что собственные значения равны ± 1. Но любое собственное значение d является произведением собственных значений c и c_1^{-1} и поэтому обязано быть положительным. Таким образом, $d = E_n$, $c = c_1$, $z = z_1$, и однозначность разложения доказана. Нам осталось установить связность и односвязность пространства S.

Для этого воспользуемся методом, который в дальнейшем мы применим к произвольной редуктивной группе, а именно, покажем, что экспоненциальное отображение exp индуцирует гомеоморфизм векторного пространства $\mathfrak{s}$ симметрических матриц на S. Из разложения (1) § 3.1 вытекает, что $\exp(X) \in S$ для любой матрицы $X \in \mathfrak{s}$ (сходимость ряда (1) хорошо известна). Приводя любой элемент $c \in S$ к диагональному виду и используя соотношение (2) § 3.1, легко видеть, что отображение $\exp\colon \mathfrak{s} \to S$ сюръективно. Далее, используя теорему об обратной

функции, несложно показать, что exp в действительности осуществляет локальный аналитический изоморфизм $\mathfrak{s}$ и S, так что осталось установить инъективность exp. Для этого заметим, что рассуждения, полностью аналогичные использованным выше, позволяют установить следующий факт: если $c_1, c_2 \in S$ и $c_1^m = c_2^m$ для некоторого целого m, то $c_1 = c_2$. Отсюда следует, что из равенства $\exp(X) = \exp(Y)$ для $X, Y \in \mathfrak{s}$ вытекает равенство

$$\exp\left(\frac{1}{m}X\right) = \exp\left(\frac{1}{m}Y\right),$$

где m — любое целое число. Выбирая m достаточно большим, можно добиться того, что элементы $(1/m)X$, $(1/m)Y$ будут произвольно близки к нулю. Так как exp является локальным изоморфизмом, то $(1/m)X = (1/m)Y$, откуда $X = Y$, что и требовалось. Предложение 7 доказано.

Имеет место также следующий комплексный аналог предложения 7. Обозначим через $\boldsymbol{B}$ подгруппу в $GL_n(\mathbb{C})$, состоящую из унитарных матриц, т. е. матриц, удовлетворяющих соотношению $^*xx = E_n$, где $^*x$ — сопряженно-транспонированная к x матрица. Рассматривая координатную запись последнего соотношения, легко показать, что группа $\boldsymbol{B}$ компактна. Пусть E — множество положительно определенных эрмитовых матриц, т. е. $a = (a_{ij}) \in E$, если $a_{ij} = \bar{a}_{ji}$ (комплексное сопряжение) и эрмитова форма $f = \sum a_{ij}\bar{x}_i x_j$ положительно определена. Тогда справедливо

Предложение 8. *$GL_n(\mathbb{C}) = \boldsymbol{B}E$ и представление справа единственно. Пространство E связно и односвязно.*

Доказательство полностью аналогично доказательству предложения 7. При этом используется следующее обобщение леммы 3:

Лемма 4. *Пусть $e \in E$. Тогда для любого целого r замыкание по Зарисскому подгруппы, порожденной e^r, содержит e.*

Связность и односвязность E доказывается следующим образом. Обозначим через $\mathfrak{e}$ пространство эрмитовых матриц в $M_n(\mathbb{C})$. Тогда экспоненциальное отображение exp осуществляет гомеоморфизм $\mathfrak{e}$ и E.

Разложения, о которых идет речь в предложениях 7 и 8, называются *полярными разложениями*. Мы собираемся установить существование и единственность аналогичных разложений для произвольной редуктивной $\mathbb{R}$-определенной подгруппы $G \subset GL_n(\mathbb{C})$. Для этого надо научиться «хорошо располагать» G в $GL_n(\mathbb{C})$. Точнее, будем говорить, что подгруппа $G \subset GL_n(\mathbb{C})$ является *самосопряженной*, если она инвариантна относительно транспонирования, т. е. если $x \in G$, то $^tx \in G$.

Теорема 7 (Мостов). *Пусть $G \subset GL_n(\mathbb{C})$ — редуктивная $\mathbb{R}$-определенная алгебраическая группа. Существует такая матрица $a \in GL_n(\mathbb{R})$, что группа $a^{-1}Ga$ является самосопряженной.*

Доказательство базируется на следующем факте.

Предложение 9. *Пусть $G \subset GL_n(\mathbb{C})$ — редуктивная $\mathbb{R}$-определенная алгебраическая группа. Тогда существует плотная по Зарисскому компактная подгруппа $K \subset G$, инвариантная относительно комплексного сопряжения.*

Итак, пусть $K \subset G$ — плотная по Зарисскому компактная подгруппа, инвариантная относительно сопряжения. Положим

$$\mathfrak{m} = \int_K {}^*kkdk, \tag{6}$$

где «матричный» интеграл берется по мере Хаара dk группы K (см. § 3.5). Так как группа K инвариантна относительно комплексного сопряжения, то мера dk также инвариантна, откуда следует, что матрица $\mathfrak{m}$ вещественна. Кроме того, матрица ${}^*kk$ — эрмитова положительно определенная, поэтому на самом деле $\mathfrak{m}$ — симметрическая положительно определенная матрица. При доказательстве предложения 7 мы показали, что $\mathfrak{m} = a^2$ для подходящей симметрической положительно определенной матрицы a. Из (6) вытекает, что K лежит в унитарной группе, отвечающей матрице $\mathfrak{m}$, поэтому $a^{-1}Ka$ лежит в группе обычных унитарных матриц B, т. е. ${}^*xx = E_n$ для $x \in a^{-1}Ka$. Таким образом, ${}^tx = {}^*\bar{x} = \bar{x}^{-1} \in K$ для любого $x \in a^{-1}Ka$, где черта означает комплексное сопряжение. Мы показали, что группа $a^{-1}Ka$ инвариантна относительно транспонирования. Поэтому тем же свойством обладает ее замыкание по Зарисскому, т. е. группа $a^{-1}Ga$. Теорема 7 доказана.

Доказательство предложения 9. Группа G представима в виде почти прямого произведения $G = TD$, где T — центральный $\mathbb{R}$-определенный тор, а группа D полупроста. Существование требуемой подгруппы в T практически очевидно: выбрав $\mathbb{C}$-определенный изоморфизм $T \simeq \mathbb{C}^{*d}$, можно взять в качестве K подгруппу S^d, где S — совокупность комплексных чисел с модулем 1; эта подгруппа является единственной максимальной компактной подгруппой в T и поэтому инвариантна относительно всех непрерывных автоморфизмов $\mathbb{C}^*$. Если нам удалось построить подгруппу $K_1 \subset D$ с требуемыми свойствами, то $K_0 = KK_1$ — искомая подгруппа в G. Тем самым можно в дальнейшем считать группу G полупростой. Выберем максимальный $\mathbb{R}$-определенный тор $T \subset G$, и пусть $R = R(T, G)$ — система корней группы G относительно T, $\{X_\alpha\}_{\alpha \in R}$ — соответствующие элементы базиса Шевалле в алгебре Ли $L(G)$ (см. § 2.1, п. 13). Тогда если обозначать через σ инволюцию комплексного сопряжения, то $\sigma(X_\alpha) = c_\alpha X_{\bar{\alpha}}$, где $c_\alpha \in \mathbb{C}$, $\bar{\alpha}$ — сопряженный к α характер тора T. Положим $\tau(X_\alpha) = |c_\alpha| X_{-\alpha}$, где $|c_\alpha|$ — модуль комплексного числа c_α. Несложное вычисление, использующее структурные соотношения для базиса Шевалле, показывает

(см. Теория алгебр Ли. Топология групп Ли//Семинар Софус Ли.—С. 145—146), что τ продолжается до антилинейной инволюции алгебры $L(G)$, которая перестановочна с σ. Обозначим через f форму Киллинга на $L(G)$, (см. § 2.1, п. 3). Путем прямого вычисления легко установить (см. loc. cit.), что $f(X, \tau(X)) < 0$ для любого $X \in L(G)$, $X \neq 0$. Поэтому если обозначить через $\mathfrak{h}$ подпространство (в действительности, $\mathbb{R}$-подалгебру) в $L(G)$ элементов, неподвижных относительно τ, то форма $f(X, X) = f(X, \tau(X))$ на $\mathfrak{h}$ отрицательно определена. Пусть $\boldsymbol{K}$ — подгруппа в G, состоящая из таких g, что $\operatorname{Ad} g$ оставляет $\mathfrak{h}$ инвариантным. Используя $\operatorname{Ad} G$-инвариантность формы f и тот факт, что $\mathfrak{h} \otimes_{\mathbb{R}} \mathbb{C} = L(G)$, несложно показать, что $\operatorname{Ad} \boldsymbol{K}$ является замкнутой подгруппой группы $\mathbb{R}$-точек $\boldsymbol{O}(g)_{\mathbb{R}}$ — ортогональной группы формы $g = f|\mathfrak{h}$. Так как g отрицательно определена, то группа $\boldsymbol{O}(g)_{\mathbb{R}}$ компактна. Поэтому компактна и группа $\boldsymbol{K}$, поскольку Ad имеет конечное ядро. Далее, в силу того, что $\mathfrak{h}$ является подалгеброй, для любого $X \in \mathfrak{h}$ элемент $\exp X$ лежит в $\boldsymbol{K}$. Но $\frac{d}{dt}(\exp(tX))_{t=0} = X$, так что алгебра Ли группы $\boldsymbol{K}$ содержит $\mathfrak{h}$ (отметим, что $\boldsymbol{K}$ является группой Ли над $\mathbb{R}$ согласно теореме Картана). Поэтому из леммы 1 вытекает, что алгебра Ли замыкания $\overline{\boldsymbol{K}}$ группы $\boldsymbol{K}$ в топологии Зарисского должна содержать $\mathbb{C}\mathfrak{h} = L(G)$, откуда $\overline{\boldsymbol{K}} = G$. Наконец, из перестановочности σ и τ вытекает σ-инвариантность $\mathfrak{h}$, поэтому σ-инвариантной будет и группа $\boldsymbol{K}$. Предложение 10 доказано.

Замечание. Утверждение предложения лежит в основе одного технического приема, который принято называть «унитарным трюком Вейля». А именно, работая с алгебраическими группами над полями характеристики нуль, вначале сводят задачу к полю $\mathbb{C}$, а затем оперируют не самой алгебраической группой, а ее плотной компактной подгруппой. Таким путем можно, например, легко установить полную приводимость представлений редуктивных алгебраических групп в характеристике нуль.

Теперь мы в состоянии построить полярное разложение в произвольной редуктивной $\mathbb{R}$-определенной группе G. Пусть $G \subset GL_n(\mathbb{C})$ — матричная реализация G. Согласно теореме 7 без ущерба для общности можно считать группу G самосопряженной. В этом случае полярное разложение для группы $GL_n(\mathbb{R})$ (предложение 7) индуцирует полярное разложение для группы $G_{\mathbb{R}}$.

Более точно, справедливо

Предложение 10. 1) $G_{\mathbb{R}} = (G \cap \boldsymbol{K})(G \cap S)$ *в обозначениях предложения 7. При этом* $\boldsymbol{K}_1 = G \cap \boldsymbol{K}$ — *максимальная компактная подгруппа в* $G_{\mathbb{R}}$, *а пространство* $\boldsymbol{S}_1 = G \cap \boldsymbol{S}$ *связно и одно-*

связно. Следовательно, факторпространство $G_{\mathbb{R}}/\boldsymbol{K}_1$ связно и односвязно.

2) *Любая компактная подгруппа $G_{\mathbb{R}}$ содержится в максимальной компактной подгруппе, а все максимальные компактные подгруппы в $G_{\mathbb{R}}$ сопряжены.*

Доказательство. 1) Пусть $x \in G_{\mathbb{R}}$ и $x = kc$ — полярное разложение в группе $GL_n(\mathbb{R})$; покажем, что $k \in \boldsymbol{K}_1$, $c \in S_1$. Поскольку G самосопряжена, то ${}^t x \in G$, следовательно, $c^2 = {}^t xx \in G$. Используя лемму 3, получаем, что $c \in G$, т. е. $c \in S_1$. Тогда и $k \in \boldsymbol{K}_1$. Любая подгруппа в $G_{\mathbb{R}}$, строго содержащая $\boldsymbol{K}_1$, обязана содержать неединичный элемент из S_1. Но из приводимости любого элемента из S к диагональному виду с положительными коэффициентами вытекает, что неединичный элемент из S не может содержаться в компактной подгруппе. Таким образом, $\boldsymbol{K}_1$ максимальна. Для доказательства связности и односвязности S_1 воспользуемся тем же методом, что и при доказательстве предложения 7. А именно, обозначим через $\mathfrak{s}_1$ подпространство в алгебре Ли $\mathfrak{g}^*$ группы $G_{\mathbb{R}}$, состоящее из симметрических матриц. Мы покажем, что экспоненциальное отображение exp индуцирует гомеоморфизм $\mathfrak{s}_1$ и S_1. При доказательстве предложения 8 мы установили, что exp индуцирует гомеоморфизм $\mathfrak{s}$ и S, поэтому достаточно показать, что $\exp(\mathfrak{s}_1) = S_1$. Включение $\exp(\mathfrak{s}_1) \subset S_1$ очевидно. Пусть теперь $c = \exp X \in S_1$, где $X \in \mathfrak{s}$. Из леммы 3 вытекает, что для любого целого n элемент $\exp(n^{-1}x)$ также лежит в S_1. Поэтому $\exp(\mathbb{Q}X) \subset S_1$, и, следовательно, $\exp(tX) \in S_1$ для любого $t \in \mathbb{R}$. Но тогда

$$X = \frac{d}{dt}\left(\exp(tX)\right)_{t=0} \in \mathfrak{g}^* \cap \mathfrak{s} = \mathfrak{s}_1,$$

и требуемое доказано.

2) Доказательство, подробности которого мы опускаем (см. Хелгасон [1]), проводится по следующей схеме. Пространство $X = G_{\mathbb{R}}/\boldsymbol{K}_1$ наделяется $G_{\mathbb{R}}$-инвариантной метрикой, относительно которой оно становится римановым многообразием отрицательной кривизны. Затем применяется результат Э. Картана, согласно которому любая компактная подгруппа, действующая изометриями на таком многообразии, обязательно имеет неподвижную точку. Итак, если $\boldsymbol{K}' \subset G_{\mathbb{R}}$ — компактная подгруппа, то существует точка $x = g\boldsymbol{K} \in X$, неподвижная относительно $\boldsymbol{K}'$. Последнее означает, что $g^{-1}\boldsymbol{K}'g \subset \boldsymbol{K}$, откуда и следует требуемое. Предложение 10 доказано.

Нам понадобится также комплексный вариант предложения 10. Мы сохраняем предположение о самосопряженности $\mathbb{R}$-определенной редуктивной группы G.

Предложение 11. 1) *$G_{\mathbb{C}} = (G \cap \boldsymbol{B})(G \cap E)$ в обозначениях предложения 8. При этом $\boldsymbol{B}_1 = G \cap \boldsymbol{B}$ — максимальная компактная подгруппа в $G_{\mathbb{C}}$, а экспоненциальное отображение* exp *осуще-*

ставляет гомеоморфизм пространства $\mathfrak{e}_1$ эрмитовых матриц из алгебры Ли $L(G)$ на $E_1 = G \cap E$.

2) *Любая компактная подгруппа группы $G_{\mathbb{C}}$ содержится в максимальной компактной подгруппе, и все максимальные компактные подгруппы сопряжены.*

Доказательство аналогично доказательству предложения 10 (можно также вывести предложение 11 из предложения 10, воспользовавшись конструкцией ограничения основного поля).

Приведем еще одно полезное техническое утверждение.

Лемма 5. *Если $b \in \boldsymbol{B}$, $e \in E$ и $e^{-1}be \in \boldsymbol{B}$, то $eb = be$.*

Доказательство. Имеем ${}^*x = x^{-1}$ для $x \in \boldsymbol{B}$ и ${}^*x = x$ для $x \in E$. Поэтому ${}^*(e^{-1}be) = e^{-1}be = ebe^{-1}$, т. е. b и e^2 перестановочны. Остается сослаться на лемму 4.

Теперь мы в состоянии доказать следующие обобщения теоремы 7.

Теорема 8 (Мостов). *Пусть $G_1 \subset \ldots \subset G_r$ — башня $\mathbb{R}$-определенных редуктивных подгрупп группы $GL_n(\mathbb{C})$. Тогда существует такая матрица $a \in GL_n(\mathbb{R})$, что все группы aG_ia^{-1} являются самосопряженными.*

Доказательство. Анализируя доказательство теоремы 7, мы видим, что достаточно найти максимальные компактные подгруппы $\boldsymbol{K}_i \subset G_{i\mathbb{C}}$, которые плотны по Зарисскому в G_i, инвариантны относительно комплексного сопряжения, и такие, что $\boldsymbol{K}_1 \subset \ldots \subset \boldsymbol{K}_r$. При этом все сводится к доказательству для двух $\mathbb{R}$-групп $H \subset G$ следующего утверждения: любая максимальная компактная подгруппа $B \subset H_{\mathbb{C}}$, инвариантная относительно комплексного сопряжения, содержится в максимальной компактной подгруппе $C \subset G_{\mathbb{C}}$, которая также инвариантна относительно сопряжения. Так как согласно предложению 9 существует плотная по Зарисскому максимальная компактная подгруппа, то в действительности любая максимальная компактная подгруппа автоматически плотна по Зарисскому. Выберем максимальную компактную подгруппу $D \subset G_{\mathbb{C}}$, содержащую B. Из предложения 11 вытекает существование однозначного разложения $G_{\mathbb{C}} = DF$, где $F = \exp(\mathfrak{f})$, $\mathfrak{f}$ — некоторое $\mathbb{R}$-подпространство в алгебре Ли $L(G)$. Обозначим через θ автоморфизм комплексного сопряжения. Тогда $\theta(D)$ — также максимальная компактная подгруппа в $G_{\mathbb{C}}$ и поэтому $\theta(D) = a^{-1}Da$ для подходящего $a = \exp(X)$, $X \in \mathfrak{f}$. Положим $b = \exp(X/2)$, $C = b^{-1}Db$ и покажем, что группа C искомая. Имеем

$$\theta(C) = \theta(b)^{-1}\theta(D)\theta(b) = \theta(b)^{-1}a^{-1}Da\theta(b) = \\ = (\theta(b)^{-1}a^{-1}b)\,C\,(b^{-1}a\theta(b)).$$

Поэтому для доказательства θ-инвариантности C достаточно показать, что $b^{-1}a\theta(b)$ лежит в центре Z группы $G_{\mathbb{C}}$, т. е.

$$b\theta(b)^{-1} = az, \quad \text{где } z \in Z. \tag{7}$$

Так как $\theta^2 = \mathrm{id}$, то

$$D = \theta^2(D) = \theta(a^{-1}Da) = \theta(a)^{-1}a^{-1}Da\theta(a).$$

Представим $a\theta(a)$ в виде $a\theta(a) = df$, где $d \in D$, $f \in F$. Тогда $f^{-1}Df = D$, и поэтому, применяя лемму 5, получаем, что f коммутирует с D, а поскольку D плотно по Зарисскому в G, то $f \in Z$. Обозначим через α автоморфизм G, являющийся композицией θ и сопряжения посредством элемента a. Тогда группа D является α-инвариантной, откуда следует, что F также инвариантно относительно α (достаточно воспользоваться тем обстоятельством, что $F = \exp(\mathfrak{f})$, а $\mathfrak{f}$ является ортогональным дополнением в $L(G)$ относительно формы Киллинга к алгебре Ли $\mathfrak{d}$ группы D как вещественной группы Ли). Поэтому $a\theta(a)a^{-1} \in F$. Но $a\theta(a)a^{-1} = dfa^{-1}$, причем если $f = \exp(Y)$, то $fa^{-1} = \exp(Y - X) \in F$, ибо $f \in Z$. Отсюда следует, что $d = 1$ и $a\theta(a) = f$. Вычислим теперь $\theta(b)$. Положим $t = a\theta(b)a^{-1}$. Так как $t \in F$, то $t = \exp(T)$, где $T \in \mathfrak{f}$. Имеем

$$t^2 = a\theta(a)a^{-1} = \exp 2T = fa^{-1} = \exp(Y - X),$$

откуда $T = (Y - X)/2$. Поэтому T перестановочен с X, так что t перестановочен с a и $\theta(b) = t = \exp((Y - X)/2)$. Отсюда следует, что b перестановочен с $\theta(b)$ и

$$b\theta(b)^{-1} = \exp\left(\frac{X}{2} + \frac{Y - X}{2}\right) = \exp\left(X - \frac{Y}{2}\right) = a\exp\left(-\frac{Y}{2}\right),$$

причем $\exp(-Y/2) \in Z$, что и требовалось. Осталось показать, что $B \subset C$. Имеем $B = \theta(B) \subset \theta(D) = a^{-1}Da$, откуда $aBa^{-1} \subset D$. Применяя лемму 5, получаем, что a перестановочен с B. Так как $b^2 = a$, то из леммы 4 вытекает перестановочность b и B. Окончательно, $B = b^{-1}Bb \subset C$. Теорема 8 доказана.

Переходим к нашей заключительной теме — разложению Ивасавы, суть которого состоит в следующем. Пусть G — определенная над $\mathbb{R}$ редуктивная группа, $H \subset G$ — максимальная связная разрешимая $\mathbb{R}$-разложимая подгруппа. Согласно теореме 1 факторпространство $G_{\mathbb{R}}/H_{\mathbb{R}}$ компактно, так что $H_{\mathbb{R}}$ дополняется в $G_{\mathbb{R}}$ некоторым компактом. Разложение Ивасавы утверждает, что дополнение на самом деле может быть осуществлено при помощи подходящей максимальной компактной подгруппы. Более того, если рассмотреть вместо группы $H_{\mathbb{R}}$ ее связную компоненту, то компоненты соответствующего разложения определены однозначно. Таким образом, группа $G_{\mathbb{R}}$ отличается от компактной группы на некоторую разрешимую группу.

Как обычно, вначале продемонстрируем разложение Ивасавы на примере группы $GL_n(\mathbb{R})$. Для этого обозначим через $\boldsymbol{K}$ подгруппу ортогональных матриц в $GL_n(\mathbb{R})$, через A и U — подгруппы в $GL_n(\mathbb{R})$ соответственно диагональных матриц с положительными коэффициентами и верхних унипотентных матриц.

Предложение 12 (разложение Ивасавы для $GL_n(\mathbb{R})$). *Естественное отображение* φ: $\boldsymbol{K}\times A\times U\to GL_n(\mathbb{R})$, $\varphi(k, a, u)=kau$, *является гомеоморфизмом.*

Доказательство. Зафиксируем ортонормированный базис $e=(e_1, \ldots, e_n)$ пространства $\mathbb{R}^n$, и пусть $g\in GL_n(\mathbb{R})$. Применяя к базису $(ge_1, \ldots, ge_n)$ классический процесс ортогонализации Грама — Шмидта, мы получим такой ортонормированный базис $d=(d_1, \ldots, d_n)$ пространства $\mathbb{R}^n$, что $d_1=\beta_{11}ge_1$, $d_2=\beta_{12}ge_1+\beta_{22}ge_2$, $\ldots$, $d_n=\beta_{1n}ge_1+\ldots+\beta_{nn}ge_n$, причем $\beta_{ii}>0$. Обозначим через b матрицу $\begin{pmatrix}\beta_{11} & \ldots & \beta_{1n}\\ & \ddots & \\ 0 & & \beta_{nn}\end{pmatrix}\in B=AU$, и через k — матрицу перехода от базиса e к базису d. Тогда, очевидно, $g=kb^{-1}$, причем матрица k ортогональна, а матрица b^{-1} принадлежит B. Таким образом, φ сюръективно. Группа $\boldsymbol{K}$ определяется условием ${}^txx=E_n$, откуда следует, что $\boldsymbol{K}\cap B=\{E_n\}$. Учитывая, что B является группой и представление $B=AU$ есть ее разложение в полупрямое произведение (как топологической группы), получаем, что φ является непрерывной биекцией. Непрерывность обратного отображения легко следует из компактности $\boldsymbol{K}$. В самом деле, если $g_m=k_ma_mu_m\xrightarrow[m\to\infty]{}g=kau$ (k, $k_m\in\boldsymbol{K}$; a, $a_m\in A$; u, $u_m\in U$), то в силу компактности $\boldsymbol{K}$ можно считать, что $k_m\xrightarrow[m\to\infty]{}k'\in\boldsymbol{K}$. Тогда $b_m=a_mu_m\xrightarrow[m\to\infty]{}b'=a'u'\in B$, ибо B замкнута. Таким образом, $g=k'a'u'$, откуда $k'=k$, $a'=a$, $u'=u$, т. е.

$$k_m\xrightarrow[m\to\infty]{}k,\quad a_m\xrightarrow[m\to\infty]{}a,\quad u_m\xrightarrow[m\to\infty]{}u,$$

что и требовалось. Предложение 12 доказано.

Представление элемента $g\in GL_n(\mathbb{R})$ в виде $g=k_ga_gu_g$, где $k_g\in\boldsymbol{K}$, $a_g\in A$, $u_g\in U$, мы будем называть *разложением Ивасавы* элемента g, а элементы k_g, a_g и u_g — соответственно его k-, a- и u-компонентами. Наша цель — построить аналогичное разложение внутри произвольной $\mathbb{R}$-определенной редуктивной подгруппы $G\subset GL_n(\mathbb{C})$. Более точно, мы покажем, что, переходя от группы G к сопряженной, можно добиться того, чтобы компоненты разложения Ивасавы в $GL_n(\mathbb{R})$ любого элемента $g\in G_{\mathbb{R}}$ принадлежали $G_{\mathbb{R}}$. Согласно теореме 7 можно с самого начала считать группу G самосопряженной. Тогда алгебра Ли $L(G)$ также инвариантна относительно транспонирования. Обо-

значим через $\mathfrak{h}$ (соответственно, $\mathfrak{p}$) подпространство в $\mathfrak{g} = L(G)_{\mathbb{R}}$, состоящее из кососимметрических (соответственно, симметрических) матриц; ясно, что $\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{p}$. (Это инфинитезимальный аналог полярного разложения из предложения 10.) Обозначим через $\mathfrak{a}$ максимальное абелево подпространство в $\mathfrak{p}$.

Лемма 6. *Существует такой $\mathbb{R}$-разложимый тор $T \subset G$, что $\mathfrak{a} = L(T)_{\mathbb{R}}$. При этом T состоит из симметрических матриц.*

Обозначим через T связную компоненту замыкания по Зарисскому множества $\exp(\mathfrak{a})$. Так как любой элемент из $\mathfrak{p}$ приводится к диагональному виду над $\mathbb{R}$ и $\mathfrak{a}$ — абелева подалгебра в $\mathfrak{g}$, то $\mathfrak{a}$ диагонализируема над $\mathbb{R}$, откуда следует, что T — разложимый над $\mathbb{R}$ подтор в G. По построению $\mathfrak{a}$ состоит из симметрических матриц, поэтому то же самое верно для $\exp(\mathfrak{a})$ и, следовательно, для T. Поэтому $L(T)_{\mathbb{R}} \subset \mathfrak{p}$ и коммутирует с $\mathfrak{a}$, так что в действительности $L(T)_{\mathbb{R}} = \mathfrak{a}$. Лемма 6 доказана.

По построению $T_{\mathbb{R}}$ состоит из симметрических матриц, поэтому для подходящего $b \in \boldsymbol{K}$ тор $bT_{\mathbb{R}}b^{-1}$ содержится в группе диагональных матриц D_n; тогда и $bTb^{-1} \subset D_n$. Поэтому, переходя от группы G к группе bGb^{-1}, что сохраняет ее самосопряженность, ибо $b \in \boldsymbol{K}$, можно считать, что $T \subset D_n$. Обозначим через $R = \{\alpha\}$ множество ненулевых весов тора T в присоединенном представлении на алгебре Ли $L(G)$. В силу $\mathbb{R}$-разложимости T все α определены над $\mathbb{R}$ и мы имеем $\mathbb{R}$-определенное разложение

$$L(G) = L(G)^{\mathrm{T}} \oplus \Big(\bigoplus_{\alpha \in R} \mathfrak{u}_\alpha\Big), \tag{8}$$

где $L(G)^T$ — централизатор T, $\mathfrak{u}_\alpha$ — собственное подпространство веса α. Выберем какое-нибудь упорядочение на пространстве $V = \mathbf{X}(T) \otimes_{\mathbb{Z}} \mathbb{R}$, где $\mathbf{X}(T)$ — группа всех характеров тора T. Легко видеть, что существует такое упорядочение на пространстве $V_0 = \mathbf{X}(D_n) \otimes_{\mathbb{Z}} \mathbb{R}$, что при естественной проекции $V_0 \to V$, которая индуцируется гомоморфизмом $\mathbf{X}(D_n) \to \mathbf{X}(T)$, отвечающим включению $T \subset D_n$, положительные элементы переходят в положительные. Пусть R_0 — система корней группы $GL_n(\mathbb{C})$ относительно D_n (в действительности $R_0 = \{\varepsilon_i - \varepsilon_j \mid i, j = 1, \ldots, n;\ i \neq j\}$, где $\varepsilon_i(\mathrm{diag}(a_1, \ldots, a_n)) = a_i$), $\Pi \subset R_0$ — подсистема простых корней относительно рассматриваемого на V_0 упорядочения (см. Бурбаки [4], гл. VI). Известно, что в группе Вейля $W(R_0)$ системы корней R_0 найдется такой элемент $w \in W(R_0)$, что $w\Pi$ совпадает со стандартной системой простых корней $\Pi_0 = \{\varepsilon_i - \varepsilon_{i+1} \mid i = 1, \ldots, n-1\}$. Так как $W(R_0)$ естественно изоморфна группе W невырожденных мономиальных матриц, у которых ненулевые элементы равны единице, то для подходящего $c \in W$ тор $T' = cTc^{-1}$ обладает свойством: существует такое упорядочение на пространстве $\mathbf{X}(T') \otimes_{\mathbb{Z}} \mathbb{R}$, что положительные корни группы $GL_n(\mathbb{C})$ при ограничении на T'

остаются положительными. Переходя от группы G к группе cGc^{-1}, можно считать, что тор T обладает этим свойством (отметим, что $W \subset \boldsymbol{K}$, и поэтому группа cGc^{-1} остается самосопряженной). Пусть R_+ — множество весов из R, которые положительны относительно рассматриваемого упорядочения на V. Положим $\mathfrak{u} = \sum_{\alpha \in R_+} \mathfrak{u}_\alpha$.

Лемма 7. *$\mathfrak{u}$ — $\mathbb{R}$-определенная подалгебра Ли $L(G)$, нормализуемая T и содержащаяся в алгебре всех верхних нильтреугольных матриц $\mathfrak{u}_n$.*

Доказательство. Ясно, что T нормализует $\mathfrak{u}$ и для $\alpha, \beta \in R_+$ имеем

$$[\mathfrak{u}_\alpha, \mathfrak{u}_\beta] = \begin{cases} 0, & \text{если } \alpha + \beta \notin R_+; \\ \mathfrak{u}_{\alpha+\beta} & \text{в противном случае.} \end{cases}$$

Отсюда следует, что $\mathfrak{u}$ является подалгеброй. Так как $\mathfrak{u}_\alpha$ определены над $\mathbb{R}$, то и $\mathfrak{u}$ определена над $\mathbb{R}$. Для доказательства включения $\mathfrak{u} \subset \mathfrak{u}_n$ достаточно показать, что $\mathfrak{u}_\alpha \subset \mathfrak{u}_n$ для любого $\alpha \in R_+$. Если $X = (x_{ij}) \in \mathfrak{u}_\alpha$ и для некоторых $i \leqslant j$ имеем $x_{ij} \neq 0$, то ограничение на T характера $\varepsilon_j - \varepsilon_i$ диагонального тора D_n совпадает с α. Равенство $i = j$ невозможно, ибо оно влечет $\alpha = 0$. Тогда $\varepsilon_j - \varepsilon_i$ — отрицательный элемент относительно рассматриваемого упорядочения на V_0, поэтому по построению его проекция на V (которая совпадает с α) также должна быть отрицательной, — противоречие. Лемма 7 доказана.

Несложные рассуждения (см., например, Борель [8], § 7) позволяют установить существование $\mathbb{R}$-определенной унипотентной подгруппы $U \subset G$, алгебра Ли которой совпадает с $\mathfrak{u}$ (отметим, что в действительности $U = \exp(\mathfrak{u})$, где exp можно понимать как «полное» либо «усеченное» экспоненциальное отображение (см. § 2.1, п. 8), при этом $U_{\mathbb{R}} = \exp(\mathfrak{u}_{\mathbb{R}})$). Ясно, что U нормализуется тором T и содержится в группе верхних унипотентных матриц U_n. Далее, обозначим через A_1 связную компоненту группы $T_{\mathbb{R}}$ и положим $\boldsymbol{K}_1 = G \cap \boldsymbol{K}$.

Теорема 9 (разложение Ивасавы). *Естественное отображение θ: $\boldsymbol{K}_1 \times A_1 \times U_{\mathbb{R}} \to G_{\mathbb{R}}$ является гомеоморфизмом.*

Доказательство. Установим вначале инфинитезимальный аналог разложения Ивасавы:

$$\mathfrak{g} = \mathfrak{h} \oplus \mathfrak{a} \oplus \mathfrak{u}_{\mathbb{R}} \tag{9}$$

в вышеприведенных обозначениях. Обозначим через τ автоморфизм алгебры $\mathfrak{gl}_n$, определенный формулой $\tau(X) = -{}^tX$, $X \in \mathfrak{gl}_n$. По построению τ индуцирует автоморфизм $\mathfrak{g}$, причем $\mathfrak{h}$ совпадает с подалгеброй неподвижных точек $\mathfrak{g}^\tau$ и $\tau(X) = -X$ для $X \in \mathfrak{a}$. Отсюда следует, что $\tau(\mathfrak{u}_\alpha) = \mathfrak{u}_{-\alpha}$ для любого $\alpha \in R$. Пусть

$X \in (\mathfrak{u}_{-\alpha})_{\mathbb{R}}$, $X = \tau(Y)$, где $Y \in (\mathfrak{u}_{\alpha})_{\mathbb{R}}$. Тогда

$$X = (\tau Y + Y) - Y \in \mathfrak{h} \oplus \mathfrak{a}_{\mathbb{R}}.$$

Обращаясь к (8), мы видим, что для доказательства равенства $\mathfrak{g} = \mathfrak{h} + \mathfrak{a} + \mathfrak{u}_{\mathbb{R}}$ осталось установить, что правая часть (9) содержит подалгебру $\mathfrak{c} = L(G)_{\mathbb{R}}^{\tau}$, совпадающую с централизатором $\mathfrak{a}$ в $\mathfrak{g}$. Поскольку $\mathfrak{a}$ инвариантно относительно τ, то $\mathfrak{c}$ также обладает этим свойством. Любой элемент $X \in \mathfrak{c}$ допускает представление

$$X = \frac{1}{2}(X + \tau X) + \frac{1}{2}(X - \tau X),$$

причем $\frac{1}{2}(X + \tau X) \in \mathfrak{h}$. Но элемент $\frac{1}{2}(X - \tau X)$ лежит в $\mathfrak{p}$ и коммутирует с $\mathfrak{a}$, поэтому в действительности $\frac{1}{2}(X - \tau X) \in \mathfrak{a}$ и $X \in \mathfrak{h} \oplus \mathfrak{a}$. Таким образом, $\mathfrak{g} = \mathfrak{h} + \mathfrak{a} + \mathfrak{u}_{\mathbb{R}}$. Если же $X + Y + Z = 0$, где $X \in \mathfrak{h}$, $Y \in \mathfrak{a}$, $Z \in \mathfrak{u}_{\mathbb{R}}$, то, применяя τ, будем иметь

$$X - Y + \tau Z = 0,$$

откуда $Y = \frac{1}{2}(-Z + \tau Z) \in \mathfrak{a} \cap \left(\sum_{\alpha \in R} \mathfrak{u}_{\alpha}\right) = (0)$. Поэтому $Z = \tau Z \in \left(\sum_{\alpha \in R_+} \mathfrak{u}_{\alpha}\right) \cap \left(\sum_{\alpha \in R_+} \mathfrak{u}_{-\alpha}\right) = (0)$, и (9) доказано. Тогда согласно теореме 2 об обратной функции существуют такие связные окрестности единицы $V \subset \boldsymbol{K}_1$ и $W \subset B = A_1 U_p$, что морфизм-произведение определяет гомеоморфизм $V \times W$ на окрестность единицы в $G_{\mathbb{R}}$. Значит, найдутся такие связные окрестности единицы $V_1 \subset V$, $W_1 \subset W$ и такие непрерывные функции φ: $V_1 \times W_1 \to \boldsymbol{K}_1$, ψ: $V_1 \times W_1 \to B$, что

$$bk = \varphi(b, k)\,\psi(b, k)$$

для всех $k \in V_1$, $b \in W_1$. Используя индукцию, легко показать, что для любого набора $S = \{k_1, \ldots, k_p\}$ элементов из V_1 найдутся такие связная окрестность единицы $W(S) \subset W_1$ и непрерывные функции

$$\varphi^S\colon V_1 \times W(S) \to \boldsymbol{K}_1, \quad \psi^S\colon V_1 \times W(S) \to B,$$

что

$$bk(S)\,k = \varphi^S(b, k)\,\psi^S(b, k)$$

для всех $k \in V_1$, $b \in W(S)$, где $k(S) = k_1 \ldots k_p$. Множество V_1 порождает связную компоненту $\boldsymbol{K}_1^0$ группы $\boldsymbol{K}_1$, поэтому из компактности $\boldsymbol{K}$ вытекает существование конечного числа таких наборов S, что $\boldsymbol{K}_1^0 = \bigcup_S k(S)\,V_1$. Положим $W_2 = \bigcap_S W(S)$. Тогда $W_2 \boldsymbol{K}_1^0 \subset \boldsymbol{K}_1^0 B$. Так как B является связной группой, то W_2

порождает B, и поэтому $B\boldsymbol{K}_1^0 = \boldsymbol{K}_1^0 B$. Но $\boldsymbol{K}_1^0 B$ содержит окрестность единицы в $G_{\mathbb{R}}$ и поэтому порождает связную компоненту $G_{\mathbb{R}}^0$. Поэтому $G_{\mathbb{R}}^0 = \boldsymbol{K}_1^0 B$. Для доказательства равенства $G_{\mathbb{R}} = \boldsymbol{K}_1 B$ остается заметить, что $\boldsymbol{K}_1 G_{\mathbb{R}}^0 = G_{\mathbb{R}}$, ибо согласно предложению 11 $G_{\mathbb{R}} = \boldsymbol{K}_1 S_1$, где S_1 — связное множество. Таким образом, сюръективность θ доказана. Из наших построений вытекает, что представление элемента $g \in G_{\mathbb{R}}$ в виде $g = kau$, где $k \in \boldsymbol{K}_1$, $a \in A_1$, $u \in U_{\mathbb{R}}$ является его разложением Ивасавы в группе $GL_n(\mathbb{R})$, поэтому из однозначности последнего вытекает биективность θ. Доказательство непрерывности обратного отображения ничем не отличается от рассуждений предложения 13. Теорема 9 доказана.

Из теоремы 9 вытекает, что группа $H = TU$ является максимальной связной $\mathbb{R}$-разложимой разрешимой подгруппой в G (и, следовательно, T — максимальный $\mathbb{R}$-разложимый тор, U — максимальная $\mathbb{R}$-определенная унипотентная подгруппа). В самом деле, если $H' \supset H$, то $H'_{\mathbb{R}} = (H' \cap K_1) H_{\mathbb{R}}$ согласно теореме 9, так что пространство $H'_{\mathbb{R}}/H_{\mathbb{R}}$ должно быть компактным, чего, как мы видели при доказательстве теоремы 1, не может быть для связной $\mathbb{R}$-разложимой разрешимой подгруппы H', строго содержащей H. В качестве еще одного следствия (не столько самой теоремы, сколько рассуждений, предшествовавших ее доказательству) отметим

Предложение 13. *Пусть $G \subset GL_n(\mathbb{C})$ — редуктивная $\mathbb{R}$-определенная группа. Существует такая матрица $a \in GL_n(\mathbb{R})$, что для группы $H = aGa^{-1}$ выполняются следующие условия:*

(i) *H самосопряжена;*

(ii) *связная компонента пересечения H с группой диагональных матриц D_n является максимальным $\mathbb{R}$-разложимым тором S в H;*

(iii) *существует такое упорядочение на пространстве $V = \boldsymbol{X}(S) \otimes_{\mathbb{Z}} \mathbb{R}$, что ограничения положительных корней $\varepsilon_i - \varepsilon_j$ $(i < j$, $i, j = 1, \ldots, n)$ группы $GL_n(\mathbb{C})$ на S положительны относительно этого упорядочения и отвечающая этому упорядочению максимальная $\mathbb{R}$-определенная унипотентная подгруппа лежит в группе верхних унипотентных матриц U_n;*

(iv) *компоненты разложения Ивасавы в $GL_n(\mathbb{R})$ любого элемента $g \in H_{\mathbb{R}}$ лежат в $H_{\mathbb{R}}$.*

§ 3.3. Неархимедов случай

Всюду в этом параграфе K обозначает неархимедово локально компактное поле характеристики нуль, т. е. конечное расширение поля p-адических чисел $\mathbb{Q}_p$. Как мы уже отмечали в § 3.1, если G — определенная над K алгебраическая группа,

то группа G_K локально компактна и вполне несвязна в p-адической топологии. Известно (см. Бурбаки [2], гл. III, § 4), что такие локально компактные группы обладают базой окрестностей единицы, состоящей из подгрупп. В рассматриваемом случае существует их явное описание на языке конгруэнц-подгрупп. А именно, пусть $G \subset GL_n(\Omega)$ — некоторая матричная реализация, $\mathcal{O}$ — кольцо целых элементов в K и $\mathfrak{p}$ — максимальный идеал в $\mathcal{O}$. Тогда группа $\mathcal{O}$-точек $G_{\mathcal{O}} = G \cap GL_n(\mathcal{O})$ является «главной» открытой компактной подгруппой в G_K (ее открытость является следствием открытости $\mathcal{O}$ в K, а компактность вытекает из компактности $GL_n(\mathcal{O})$ и замкнутости $G_{\mathcal{O}}$ в $GL_n(\mathcal{O})$). *Конгруэнц-подгруппы* $G_{\mathcal{O}}(\mathfrak{p}^d) \subset G_{\mathcal{O}}$ определяются следующим образом:

$$G_{\mathcal{O}}(\mathfrak{p}^d) = \{g \in G_{\mathcal{O}} \mid g \equiv E_n \pmod{\mathfrak{p}^d}\}, \quad d > 0,$$

и образуют искомую базу окрестностей единицы в G_K. Аппарат теории групп Ли оказывается в данной ситуации менее эффективным, чем в архимедовом случае, и поэтому для получения результатов о строении G_K приходится применять другие соображения.

Ряд важных результатов, относящихся, главным образом, к компактным подгруппам в G, может быть получен при помощи техники решеток и порядков в полупростых алгебрах (см. § 1.5, п. 3). Если $G \subset GL_n(\Omega)$ — определенная над K алгебраическая группа и $L \subset K^n$ — некоторая решетка, то всюду в этой книге через $G_{\mathcal{O}}^L$ будет обозначаться стабилизатор решетки L в группе G, т. е.

$$G_{\mathcal{O}}^L = \{g \in G_K \mid g(L) = L\}.$$

(Это обозначение указывает на то обстоятельство, что $G_{\mathcal{O}}^L$ состоит из матриц, которые в базисе решетки L попадают в $GL_n(\mathcal{O})$.)

Согласно предложению 1.12 любая компактная подгруппа $B \subset GL_n(K)$ содержится в стабилизаторе некоторой решетки $L \subset K^n$. В частности, для компактной подгруппы $B \subset G_K$ найдется такая решетка $L \subset K^n$, что $B \subset G_{\mathcal{O}}^L$, и, значит, любая компактная подгруппа в G_K содержится в некоторой открытой компактной подгруппе. При этом если B — максимальная компактная подгруппа, то $B = G_{\mathcal{O}}^L$. Из предложения 1.12 вытекает также, что в случае группы $G = \boldsymbol{GL}_n$ для максимальных компактных подгрупп справедливы те же фундаментальные факты, что и в архимедовом случае: любая компактная подгруппа содержится в некоторой максимальной компактной подгруппе, а все максимальные компактные подгруппы сопряжены между собой. В связи с этим кажется несколько удивительным тот факт, что переход от $G = \boldsymbol{GL}_n$ даже к группе $H = \boldsymbol{SL}_n$ нарушает эту гармонию.

Предложение 14. *Пусть $H = SL_n$. Тогда для любой решетки $L \subset K^n$ группа $H_{\mathcal{O}}^L$ является максимальной компактной подгруппой в H_K. Любая компактная подгруппа в H_K содержится в некоторой максимальной компактной подгруппе, а все максимальные компактные подгруппы распадаются в n классов сопряженности в H_K.*

Доказательство. Мы предлагаем читателю в качестве упражнения слегка модифицировать доказательство предложений 1.11, 1.12 таким образом, чтобы установить максимальность $H_{\mathcal{O}}^L$ для любой решетки $L \subset K^n$ и, кроме того, показать, что из $H_{\mathcal{O}}^L = H_{\mathcal{O}}^M$ следует пропорциональность решеток L и M. Для доказательства последнего утверждения построим сюръективное отображение φ множества $\mathscr{B}$ максимальных компактных подгрупп группы $SL_n(K)$ на факторгруппу K^*/UK^{*n}, где U — группа v-адических единиц в K, слои которого совпадают с классами сопряженности максимальных компактных подгрупп. Так как порядок K^*/UK^{*n} равен n, то отсюда будет следовать требуемое. Зафиксируем некоторую решетку $L \subset K^n$, и пусть $B \in \mathscr{B}$. Тогда B имеет вид $H_{\mathcal{O}}^M$ для подходящей решетки $M \subset K^n$, и отображение φ определяется следующим образом: если $M = g(L)$, $g \in GL_n(K)$, то $\varphi(g) = (\det g)UK^{*n}$. Так как $H_{\mathcal{O}}^{M_1} = H_{\mathcal{O}}^{M_2}$ влечет $M_2 = \mu M_1$, $\mu \in K^*$, то отображение φ определено корректно, и, очевидно, сюръективно. Предположим теперь, что $\varphi(B_1) = \varphi(B_2)$, где $B_i = H_{\mathcal{O}}^{M_i}$, $M_i \subset K^n$. Из определения φ вытекает, что в этом случае $M_2 = g(M_1)$ для некоторого $g \in GL_n(K)$, такого, что $\det g \in UK^{*n}$, т. е. $\det g = ut^n$, $u \in U$, $t \in K^*$. Выберем элемент s из стабилизатора решетки M_1 со свойством $\det s = u$ и положим $h = t^{-1}gu^{-1}$. Тогда $h \in SL_n(K)$ и $h(M_1) = tM_2$, так что $hB_1h^{-1} = H_{\mathcal{O}}^{h(M_1)} = H_{\mathcal{O}}^{M_2} = B_2$, и, значит, B_1 и B_2 сопряжены в H_K. Обратно, если $B_i = H_{\mathcal{O}}^{M_i}$ $(i = 1, 2)$ связаны соотношением $B_2 = hB_1h^{-1}$, то решетки $h(M_1)$ и M_2 пропорциональны, откуда без труда следует, что $\varphi(B_1) = \varphi(B_2)$. Предложение доказано.

Детальное изучение свойств максимальных компактных подгрупп в неархимедовой ситуации, проведенное Брюа и Титсом [2—4], показывает, что последнее утверждение предложения 14 является частным случаем следующего общего результата: если G — простая односвязная K-группа K-ранга l, то в группе G_K имеется в точности $(l+1)$ класс сопряженности максимальных компактных подгрупп. Мы изложим элементы теории Брюа — Титса в следующем параграфе, а пока дадим независимые элементарные доказательства некоторых первоначальных фактов, из которых, в частности, вытекает, что любая компактная подгруппа группы G_K, где G редуктивна, содержится в некоторой максимальной компактной подгруппе. При этом, как показы-

вает следующее утверждение, требование редуктивности G существенно.

Предложение 15. *Если группа G_K обладает максимальными компактными подгруппами, то группа G редуктивна.*

Доказательство. Рассмотрим разложение Леви $G = HU$ группы G, где $U = R_u(G)$ — унипотентный радикал G, а группа H редуктивна (см. § 2.1, п. 9). Предположим, что $U \neq (1)$. Тогда центр $Z(U)$ также нетривиален, причем «усеченное» логарифмическое отображение индуцирует K-определенный изоморфизм φ: $Z(U) \to V$, где $V = L(Z(U))$ — соответствующая алгебра Ли, $\dim V > 0$. Поскольку U является нормальным делителем в G, то $Z(U)$ также является нормальным делителем, и для любых $g \in G$, $z \in Z(U)$ справедлива формула

$$\varphi(g^{-1}zg) = (\operatorname{Ad} g)\,\varphi(z). \tag{1}$$

Пусть ρ: $G \to GL(V)$ — представление, определяемое присоединенным действием. Если $B \subset G_K$ — максимальная компактная подгруппа, то согласно предложению 1.12 найдется решетка $L \subset V_K$, инвариантная относительно $\rho(B)$. Положим $Z_i = \varphi^{-1}(\pi^{-i}L)$, где $\pi \in K$ — униформизующий элемент. Ясно, что Z_i — компактные подгруппы в $Z(U)_K$, объединение которых совпадает с $Z(U)_K$. Кроме того, из формулы (1) вытекает, что B нормализует все Z_i, так что любое произведение BZ_i также является компактной подгруппой. Используя максимальность B, получаем, что $B = BZ_i$ для любого i. Отсюда $Z(U)_K \subset B$ — противоречие, ибо $Z(U)_K$ некомпактно. Предложение доказано.

Покажем теперь, что если группа G редуктивна, то G_K действительно обладает максимальными компактными подгруппами, причем любая компактная подгруппа в G_K лежит в некоторой максимальной компактной подгруппе.

Предложение 16. *Пусть G — редуктивная K-определенная группа. Тогда*

1) *любая открытая компактная подгруппа группы G_K содержится лишь в конечном числе компактных подгрупп;*

2) *любая компактная подгруппа группы G_K содержится в некоторой максимальной компактной подгруппе.*

Кроме того, если G полупроста, то нормализатор в G_K любой открытой компактной подгруппы компактен.

Доказательство. Пусть $G \subset GL(\Omega)$. Используя вложение $GL_n(\Omega) \to GL_{n+1}(\Omega)$, $A \mapsto \begin{pmatrix} A & 0 \\ 0 & \det^{-1} A \end{pmatrix}$, можно считать, что G замкнута по Зарисскому в $M_n(\Omega)$. Обозначим через A Ω-оболочку $\Omega[G]$ группы G в $M_n(\Omega)$ (т. е. совокупность линейных комбинаций элементов G с коэффициентами из Ω) и через B K-оболочку $K[G_K]$ группы G_K в $M_n(K)$. Поскольку группа G редуктивна, из теоремы 2.4 вытекает, что A и B являются полупростыми алгебрами над Ω и K соответственно. Любая откры-

тая компактная подгруппа $U \subset G_K$ плотна по Зарисскому в G (лемма 2), поэтому $\Omega[U] = A$ и $K[U] = B$. В частности, $P = \mathcal{O}[U]$ является порядком в B. Согласно теореме 1.16 порядок P содержится в конечном числе максимальных порядков $P_1, \ldots, P_r$. Каждое пересечение $P_i \cap G$, очевидно, компактно и замкнуто относительно умножения, так что $U_i = (P_i \cap G) \cap (P_i \cap G)^{-1}$ — компактная подгруппа в G_K. Пусть теперь $W \subset G_K$ — компактная подгруппа, содержащая U. Тогда $\mathcal{O}[W]$ — порядок в B, содержащий P, и поэтому $\mathcal{O}[W] \subset P_i$ для некоторого i. Следовательно, $W \subset P_i \cap G$ и $W = W^{-1} \subset (P_i \cap G)^{-1}$; так что $W \subset U_i$. Мы показали, что любая компактная подгруппа, содержащая U, обязательно содержится в одной из групп U_i. Отсюда следует утверждение пункта 1), ибо в силу открытости U любой индекс $[U_i : U]$ конечен, и поэтому число промежуточных между U и U_i подгрупп также конечно. Выше мы отмечали, что любая компактная подгруппа группы G_K содержится в некоторой открытой компактной подгруппе, в силу чего из утверждения 1) получаем утверждение 2). Пусть теперь группа G полупроста. Рассмотрим присоединенное действие группы G на алгебре A, и пусть

$$G \ni g \xrightarrow{\varphi} i_g \in \operatorname{Aut} A, \quad i_g(x) = gxg^{-1},$$

— соответствующее представление. Ясно, что ядро φ совпадает с центром G и поэтому конечно. Рассмотрим произвольную открытую компактную подгруппу $U \subset G_K$ и обозначим через N ее нормализатор в G_K. Как мы установили выше, $P = \mathcal{O}[U]$ является порядком в алгебре $B = K[G_K]$, так что, выбрав $\mathcal{O}$-базис $x_1, \ldots, x_m$ в P, мы получим Ω-базис алгебры A. Так как для любого $g \in N$, очевидно, имеем $g^{-1}Pg = P$, то коэффициенты матрицы преобразования $\varphi(g)$ в базисе $x_1, \ldots, x_m$ лежат в $\mathcal{O}$. Таким образом, $\varphi(N) \subset \varphi(G)_{\mathcal{O}}$. Из компактности $\varphi(G)_{\mathcal{O}}$ и конечности $\operatorname{Ker} \varphi$ вытекает компактность $\varphi^{-1}(\varphi(G)_{\mathcal{O}})$ и, следовательно, относительная компактность N. С другой стороны, в силу замкнутости U, группа N также замкнута, и поэтому в действительности компактна. Предложение 16 доказано.

К свойствам максимальных компактных подгрупп мы еще вернемся в следующем параграфе, а пока, используя элементарную информацию, содержащуюся в предложении 16, получим некоторые структурные результаты о группе G_K. Наши рассуждения будут базироваться на теории проконечных групп. Так как проконечные группы будут не раз встречаться в дальнейшем, приведем сводку основных определений и их свойств (более подробное изложение читатель может найти у Серра [2] и Бурбаки [2], гл. III, § 7).

Пусть I — фильтрующееся множество, т. е. частично упорядоченное множество с отношением порядка $\leqslant$ таким, что для

любых $i, j \in I$ найдется $k \in I$ со свойством $i \leqslant k$, $j \leqslant k$. (В наших рассуждениях I, как правило, будет совпадать с множеством натуральных чисел $\mathbb{N}$, наделенным обычным порядком.) Проективной системой $\mathcal{G} = (G_i, \varphi_i^j)$ над I называется совокупность объектов (множеств, групп, колец и т. д.) G_i, индексированных элементами множества I, и морфизмов φ_i^j: $G_j \to G_i$ между ними для $j \geqslant i$, причем φ_i^i — тождественное отображение и $\varphi_i^k = \varphi_i^j \circ \varphi_j^k$ для $k \geqslant j \geqslant i$. *Проективным пределом* $\varprojlim G_i$ (более точно, $\varprojlim (G_i, \varphi_i^j)$) называется подмножество в декартовом произведении $\prod_{i \in I} G_i$, состоящее из таких наборов $g = (g_i)$, что $\varphi_i^j(g_j) = g_i$ для всех $j \geqslant i$ из I. Ясно, что $\varprojlim G_i$ наследует тот же тип алгебраической структуры, которой обладают все G_i. Кроме того, если все G_i являются отделимыми топологическими пространствами, а φ_i^j — непрерывными отображениями, то $G = \varprojlim G_i$ замкнуто в $\prod_{i \in I} G_i$. Пусть, в частности, все G_i являются конечными группами, которые мы наделим дискретной топологией, а φ_i^j — гомоморфизмами групп. Тогда проективный предел $G = \varprojlim G_i$ называется *проконечной группой*. Поскольку G является замкнутым подмножеством в произведении $\prod_{i \in I} G_i$, которое компактно, то сама группа G компактна. Кроме того, группа G вполне несвязна. (Это легче всего показать, воспользовавшись ограничениями $\pi_I = p_I|_G$ канонических проекций p_I: $\prod_{i \in I} G_i \to G_I$, конечные пересечения ядер которых образуют фундаментальную систему окрестностей единицы группы G, состоящую из подгрупп.) Обратно, любая компактная вполне несвязная топологическая группа G является проконечной, т. е. представима в виде проективного предела конечных групп. Такое представление можно получить, если известна фундаментальная система $\{N_i\}_{i \in I}$ окрестностей единицы группы G, состоящая из нормальных делителей (доказывается, что такая система существует в любой компактной вполне несвязной группе, см. Кох [1], § 1.2). А именно, естественный гомоморфизм

$$G \to \varprojlim G/N_i, \quad g \mapsto (gN_i)_{i \in I},$$

оказывается изоморфизмом топологических групп. Применим этот результат к группе $G_{\mathcal{O}}$ точек алгебраической K-группы G над кольцом целых $\mathcal{O}$. Так как конгруэнц-подгруппы $G_{\mathcal{O}}(\mathfrak{p}^d)$ (где $\mathfrak{p}$ — идеал нормирования в $\mathcal{O}$, $d > 0$), очевидно, являются нормальными делителями в $G_{\mathcal{O}}$ и образуют базис окрестностей

единицы, то

$$G_{\mathcal{O}} \simeq \varprojlim G_{\mathcal{O}}/G_{\mathcal{O}}(\mathfrak{p}^d). \tag{2}$$

Из этого представления можно сделать определенные выводы о структуре группы $G_{\mathcal{O}}$. Для этого напомним, что *про-p-группой* называется проективный предел конечных p-групп.

Лемма 8. *$G_{\mathcal{O}}(\mathfrak{p})$ — про-p-группа.*

Доказательство. Число p определяется из условия $\mathbb{Q}_p \subset K$, или, эквивалентно, $p \in \mathfrak{p}$. Если $G = \varprojlim G/N$ — представление проконечной группы G в виде проективного предела своих конечных факторов, то для любой замкнутой подгруппы $H \subset G$ имеет место представление $H = \varprojlim H/H \cap N$. Отсюда следует, что для группы $G_{\mathcal{O}}(\mathfrak{p})$ справедливо представление

$$G_{\mathcal{O}}(\mathfrak{p}) \simeq \varprojlim G_{\mathcal{O}}(\mathfrak{p})/G_{\mathcal{O}}(\mathfrak{p}^d).$$

Покажем, что факторгруппы $G_{\mathcal{O}}(\mathfrak{p})/G_{\mathcal{O}}(\mathfrak{p}^d)$ являются p-группами. Достаточно показать, что для любого $d \geqslant 1$ факторгруппа $G_{\mathcal{O}}(\mathfrak{p}^d)/G_{\mathcal{O}}(\mathfrak{p}^{d+1})$ является p-группой. Пусть $x \in G_{\mathcal{O}}(\mathfrak{p}^d)$. Представим x в виде $x = E_n + y$, где $y \equiv 0 \pmod{\mathfrak{p}^d}$. Тогда

$$x^p = E_n + C_p^1 y + \ldots + C_p^{p-1} y^{p-1} + y^p.$$

Так как биномиальные коэффициенты C_p^i делятся на p для $0 < i < p$, то $C_p^i y^i \equiv 0 \pmod{\mathfrak{p}^{d+1}}$ для любого $i \geqslant 1$. Поэтому $x^p \equiv E_n \pmod{\mathfrak{p}^{d+1}}$. Тем самым порядок любого элемента факторгруппы $G_{\mathcal{O}}(\mathfrak{p}^d)/G_{\mathcal{O}}(\mathfrak{p}^{d+1})$ делит p. Лемма доказана.

Следствие. *Порядок любого элемента из $G_{\mathcal{O}}(\mathfrak{p})$ либо бесконечен, либо является степенью p.*

Доказательство. Легко видеть, что замкнутая подгруппа про-p-группы является про-p-группой. Поэтому если порядок элемента $x \in G_{\mathcal{O}}(\mathfrak{p})$ конечен, то порожденная им циклическая подгруппа $H = \langle x \rangle$ должна быть конечной про-p-группой, т. е. обычной p-группой.

Таким образом, группа $G_{\mathcal{O}}$ является конечным расширением про-p-группы $G_{\mathcal{O}}(\mathfrak{p})$. Про-$q$-подгруппы (где q — любое простое число) в теории проконечных групп являются проконечными аналогами q-подгрупп в теории конечных групп и сохраняют многие их свойства. В частности, любая про-q-подгруппа содержится в некоторой максимальной (силовской) про-q-подгруппе, а все последние сопряжены между собой (см. Серр [2]). Что же касается про-p-подгрупп, то в нашей ситуации они играют особую роль. Изучение их свойств позволяет получить важные результаты о структуре группы G_K. Наша ближайшая цель — установить для группы G_K аналог теоремы Силова о сопряженности максимальных про-p-подгрупп (после того как мы уста-

новили существование несопряженных максимальных компактных подгрупп, справедливость такого результата отнюдь не кажется столь бесспорной).

Теорема 10 (Мацумото [1]). *Пусть G — полупростая K-определенная алгебраическая группа, $H \subset G_K$ — открытая подгруппа. Тогда H обладает максимальной открытой про-p-подгруппой S и любая про-p-подгруппа в H содержится в сопряженной к S.*

Доказательство. Подгруппа H, будучи открытой, содержит подходящую конгруэнц-подгруппу $G_{\mathcal{O}}(\mathfrak{p}^d)$. Из леммы 8 вытекает, что $G_{\mathcal{O}}(\mathfrak{p}^d)$ является про-p-группой. Применяя утверждение 1) предложения 16, заключаем, что $G_{\mathcal{O}}(\mathfrak{p}^d)$ содержится в некоторой максимальной про-p-подгруппе $S \subset H$. Пусть теперь $T \subset H$ — некоторая про-p-подгруппа. Покажем, что T содержится в некоторой силовской про-p-подгруппе. Опять обращаясь к утверждению 1) предложения 16, мы видим, что достаточно найти открытую про-p-подгруппу, содержащую T. Для этого заметим, что в силу компактности T индекс $[T: T \cap S]$ конечен, и поэтому среди групп $t^{-1}St$, $t \in T$, имеется лишь конечное число различных. Тогда группа $S_0 = \bigcap_{t \in T} (t^{-1}St)$ открыта и нормализуется группой T, так что группа $T_0 = TS_0$ является искомой. Поэтому при доказательстве того, что T содержится в подгруппе, сопряженной к S, можно считать про-p-подгруппу T силовской. По техническим причинам нам удобнее доказывать не просто сопряженность S и T, а существование такого $x \in H$, что $xTx^{-1} = S$ и $[S : S \cap T] = [S : x(S \cap T)x^{-1}]$. (Отметим, что, воспользовавшись существованием меры Хаара на группе G_K и ее унимодулярностью (см. § 3.5), можно показать, что последнее равенство на самом деле выполняется автоматически.) Рассуждение будем вести индукцией по $n = [S : S \cap T]$. Если $n = 1$, то $S = T$, и доказывать нечего. Пусть теперь $n > 1$. Обозначим через N нормализатор пересечения $S \cap T$ в группе H; согласно предложению 16 N — компактная подгруппа в H и, следовательно, индекс $[N: S \cap T]$ конечен. Покажем, что пересечения $N_1 = N \cap S$ и $N_2 = N \cap T$ строго содержат $S \cap T$. Так как $S \cap T \neq S$, T, то это вытекает из следующего утверждения.

Лемма 9. *Пусть P — про-p-группа, $H \subset P$ — собственная открытая подгруппа. Тогда нормализатор $N_P(H)$ отличен от H.*

Доказательство. Это утверждение хорошо известно для конечных p-групп. Чтобы свести общий случай к конечному, положим $F = \bigcap_{g \in P} (g^{-1}Hg)$. Тогда F — открытый нормальный делитель в P, содержащийся в H. Ясно, что $N_P(H) = \pi^{-1}(N_{P/F}(H/F))$, где π: $P \to P/F$ — естественный гомоморфизм. Но группа P/F конечна, поэтому $N_{P/F}(H/F) \neq H/F$, и, следовательно, $N_P(H) \neq H$. Лемма доказана.

Продолжая доказательство теоремы 10, рассмотрим конечную группу $\bar{N} = N/S \cap T$ и естественный гомоморфизм $\varphi\colon N \to \bar{N}$. Образы $\varphi(N_1)$ и $\varphi(N_2)$ являются p-подгруппами в $\bar{N}$, и поэтому согласно классическим теоремам Силова найдется силовская p-подгруппа $P \subset \bar{N}$, содержащая $\varphi(N_1)$, и такой элемент $\bar{x} \in \bar{N}$, что $\bar{x}\varphi(N_2)\bar{x}^{-1} \subset P$. Прообраз $\varphi^{-1}(P)$ является про-p-подгруппой в H и поэтому содержится в некоторой силовской про-p-подгруппе V. Отметим, что по построению N_1, $xN_2x^{-1} \subset V$, где $x \in N$ — такой элемент, что $\varphi(x) = \bar{x}$. Тогда $[S : S \cap V] < n$ и по предложению индукции $S = yVy^{-1}$, $y \in H$, причем $[S : S \cap V] = [S : y(S \cap V)y^{-1}]$. Рассмотрим группу $T' = (yx)T(yx)^{-1}$. Ясно, что $S \cap T' \supset (yx)N_2(yx)^{-1} \supsetneqq (yx)(S \cap T)(yx)^{-1}$, и, кроме того,

$$\begin{aligned}[S : (yx)(S \cap T)(yx)^{-1}] &= [S : y(S \cap T)y^{-1}] = \\ &= [S : y(S \cap V)y^{-1}]\,[y(S \cap V)y^{-1} : y(S \cap T)y^{-1}] = \\ &= [S : S \cap V]\,[S \cap V : S \cap T] = [S : S \cap T]. \qquad (3)\end{aligned}$$

Таким образом, $[S : S \cap T'] < n$, и опять по предположению индукции найдется $z \in H$ со свойствами $S = zT'z^{-1}$ и $[S : S \cap T'] = [S : z(S \cap T')z^{-1}]$. Тогда $S = (zyx)T(zyx)^{-1}$ и

$$\begin{aligned}[S : (zyx)(S \cap T)(zyx)^{-1}] &= \\ &= [S : z(S \cap T')z^{-1}]\,[z(S \cap T')z^{-1} : (zyx)(S \cap T)(zyx)^{-1}] = \\ &= [S : S \cap T']\,[S \cap T' : (yx)(S \cap T)(yx)^{-1}] = \\ &= [S : (yx)(S \cap T)(yx)^{-1}] = [S : S \cap T]\end{aligned}$$

в силу (3). Теорема 10 доказана.

Замечание. Приведенное в оригинальной работе Мацумото [1] доказательство теоремы 10 содержит методологическую ошибку: используемая в нем индукция по паре индексов $[S : S \cap T]$ и $[T : S \cap T]$ невыполнима. Наше доказательство представляет исправленный вариант рассуждений Мацумото.

Теорема 10 будет не раз применяться в этой книге. В частности, из нее вытекает следующий важный структурный результат.

Предложение 17. *Пусть G — K-простая алгебраическая K-группа. Тогда любой нецентральный нормальный делитель группы G_K имеет в ней конечный индекс.*

Доказательство. Пусть H — нецентральный нормальный делитель группы G_K. Согласно теореме 3, H открыт, поэтому факторпространство G_K/H дискретно, и достаточно установить его компактность. Это вытекает из следующего утверждения:

Предложение 18. *Пусть H — открытый нормальный делитель группы G_K, где G — полупростая K-группа. Тогда существует такая максимальная компактная подгруппа $B \subset G_K$, что $G_K = BH$.*

Доказательство. Пусть $S \subset H$ — силовская про-p-подгруппа, $g \in G_K$. Тогда группа $g^{-1}Sg$ также является силовской про-p-подгруппой в $g^{-1}Hg = H$, следовательно, по теореме 10 $g^{-1}Sg = h^{-1}Sh$ для подходящего $h \in H$. Поэтому $x = gh^{-1} \in N = N_{G_K}(S)$, т. е. $G_K = NH$. Но в силу предложения 16 группа N компактна, и согласно утверждению 1) того же предложения содержится в некоторой максимальной компактной подгруппе, которая и будет искомой.

Замечание. Объединяя предложения 5 и 17, можно сделать следующий вывод: если K — локально компактное поле и G — K-простая алгебраическая K-группа, то любой нецентральный нормальный делитель группы G_K имеет в ней конечный индекс. (Формально мы не рассматривали случай $K = \mathbb{C}$, но здесь, как хорошо известно, группа $G = G_{\mathbb{C}}$ вообще не имеет нецентральных нормальных делителей (см. § 7.2). Можно дать также топологическое доказательство этого факта: любой нецентральный нормальный делитель в $G_{\mathbb{C}}$ открыт и поэтому обязан содержать связную компоненту $G^0_{\mathbb{C}}$, но в силу теоремы 5 $G_{\mathbb{C}}$ связна, т. е. $G_{\mathbb{C}} = G^0_{\mathbb{C}}$.) Значительно сложнее доказать аналогичный результат для односвязных групп над числовыми полями (см. § 7.2 и 9.1).

Наряду с теорией проконечных групп при изучении алгебраических групп над неархимедовыми локальными полями используется метод редукции рассматриваемых объектов по модулю максимального идеала $\mathfrak{p}$. С помощью процедуры редукции данному алгебраическому многообразию X, определенному над полем K, ставится в соответствие алгебраическое многообразие $\underline{X}$, определенное над полем вычетов $k = \mathcal{O}/\mathfrak{p}$. При этом если выполнены некоторые условия гладкости; то точки из $\underline{X}_k$ находятся в биективном соответствии с классами сравнимых по модулю $\mathfrak{p}$ точек из $X_{\mathcal{O}}$. Чтобы не отягощать изложение техническими деталями, мы приведем основные определения и результаты для случая аффинных многообразий. Отметим, что в дальнейшем нам встретятся еще лишь проективные многообразия, для которых рассуждения полностью аналогичны. (В действительности случай произвольных многообразий может быть сведен к аффинным путем рассмотрения конечного аффинного покрытия, см. Вейль [3].)

Определение редукции удобно дать в общей ситуации аффинного алгебраического многообразия $X \subset \mathbb{A}^n$, определенного над полем P, которое является полем частных некоторого кольца $R \subset P$. Пусть $\mathfrak{a}$ — идеал в кольце многочленов $P[x_1, \ldots, x_n]$, состоящий из многочленов, обращающихся в нули на X. *Редукцией* X по модулю максимального идеала $\mathfrak{m} \subset R$ называется подмногообразие $\underline{X}^{(\mathfrak{m})}$ в аффинном пространстве $\mathbb{A}^n$ над уни-

версальной областью, содержащей поле вычетов $k = R/\mathfrak{m}$, определяемое идеалом $\mathfrak{a}^{(\mathfrak{m})}$, который получается редукцией всех многочленов из $\mathfrak{a} \cap R[x_1, \ldots, x_n]$ по модулю $\mathfrak{m}$ (т. е. заменой коэффициентов всех многочленов на их классы вычетов по модулю $\mathfrak{m}$). (Отметим, что в общем случае многообразие $\underline{X}^{(\mathfrak{m})}$ является лишь k-замкнутым в $\mathbb{A}^n$, но, вообще говоря, не является k-определенным. Однако в дальнейшем k будет конечным полем, так что ввиду его совершенности понятия k-замкнутости и k-определенности совпадают.) Несмотря на простоту определения, сама процедура редукции является весьма тонкой и при использовании требует известной осторожности. Например, если $P = \mathbb{Q}$, $R = \mathbb{Z}$, а $X \subset \mathbb{A}^1$ состоит из одной точки $x = p^{-1}$, то $\mathfrak{a} = (px - 1)$, $\mathfrak{a} \cap \mathbb{Z}[x] = (px - 1)\mathbb{Z}[x]$, так что редукция X по модулю p определяется уравнением $\bar{0} \cdot x - \bar{1} = \bar{0}$, т. е. $\underline{X}^{(p)} = \varnothing$.

К сожалению, до сих пор в монографической литературе не существует полного изложения теории редукции алгебраических многообразий, хотя большое число относящихся к ней фактов используются как «хорошо известные». В наши планы также не входило достаточно подробное рассмотрение этих вопросов, ибо оно сопряжено с использованием аппарата коммутативной алгебры в гораздо большем объеме, чем в остальной части книги. Поэтому мы ограничимся основными определениями и результатами, причем ряд фундаментальных фактов (таких, как, например, лемма Гензеля) будет приведен без доказательства. С другой стороны, ниже мы дадим ряд простых, но типичных для теории редукции рассуждений, которые позволят заинтересованному читателю восстановить некоторые опущенные доказательства.

Определим теперь так называемую гладкую редукцию. Пусть, как и выше, $X \subset \mathbb{A}^n$ — аффинное P-определенное многообразие, все неприводимые компоненты которого имеют одну и ту же размерность m, $\underline{X}^{(\mathfrak{m})}$ — редукция X по модулю максимального идеала $\mathfrak{m}$ кольца $R \subset P$. Будем говорить, что точка $x \in \underline{X}^{(\mathfrak{m})}$ является *простой точкой редукции*, если существуют такие полиномы $f_1, \ldots, f_r \in \mathfrak{a} \cap R[x_1, \ldots, x_n]$, $r = n - m$ (где $\mathfrak{a}$ — идеал многочленов из $P[x_1, \ldots, x_n]$, обращающихся в нуль на X), что ранг матрицы Якоби

$$\left(\frac{\partial \bar{f}_i}{\partial x_j}(x)\right)_{\substack{i=1,\ldots,r \\ j=1,\ldots,n}}$$

равен r (здесь и далее черта означает редукцию по модулю $\mathfrak{m}$). Если все точки $\underline{X}^{(\mathfrak{m})}$ простые, то редукция называется *гладкой*.

Отметим, что понятие гладкой редукции является более сильным требованием по сравнению с гладкостью многообразия $\underline{X}^{(\mathfrak{m})}$. Для точек $x=(x_1, \ldots, x_n)$ и $y=(y_1, \ldots, y_n)$ из X_R мы пишем $x \equiv y \pmod{\mathfrak{m}}$, если $x_i \equiv y_i \pmod{\mathfrak{m}}$ для всех $i=1, \ldots, n$. Кроме того, для любой точки $x \in X_R$ соответствующая точка $\bar{x} \in \mathbb{A}_k^n$ попадает в $\underline{X}_k^{(\mathfrak{m})}$, тем самым возникает *отображение редукции* ρ: $X_R \to \underline{X}_k^{(\mathfrak{m})}$, непустые слои которого совпадают с классами сравнимых по модулю $\mathfrak{m}$ точек множества X_R. Возникает вопрос о том, каков образ отображения редукции. Мы не будем обсуждать здесь все аспекты этой проблемы (см. обзор Паршина [1]), ибо для наших целей достаточно следующего результата, который относится к нашей исходной ситуации: K — конечное расширение $\mathbb{Q}_p$, $\mathcal{O}$ — кольцо целых в K и $\mathfrak{p} \subset \mathcal{O}$ — максимальный идеал.

Теорема 11 (лемма Гензеля). *Если $x \in \underline{X}^{(\mathfrak{p})}$ — простая точка редукции, то x лежит в образе отображения редукции. В частности, если редукция $\underline{X}^{(\mathfrak{p})}$ гладкая, то отображение редукции сюръективно.*

Отметим, что в случае гладкой редукции различные неприводимые компоненты многообразия не могут «склеиваться», в частности, если X состоит из конечного числа точек и редукция является гладкой, то отображение редукции инъективно.

Разумеется, редукция гладкого многообразия не обязана быть гладкой. Тем не менее если X — гладкое многообразие, определенное над числовым полем K, то для почти всех неархимедовых нормирований v поля K редукция $\underline{X}^{(v)}$ относительно соответствующего максимального идеала $\mathfrak{p}(v)$ кольца целых $\mathcal{O} \subset K$ также является гладкой.

Аналогичным образом ведет себя при редукции и такое свойство многообразий, как (абсолютная) неприводимость. Кроме того, если исходное многообразие являлось алгебраической группой, то все его редукции — также алгебраические группы, причем соответствующее отображение редукции является гомоморфизмом групп. Оставшаяся часть параграфа посвящена точным формулировкам и частичным доказательствам этих фактов.

Теорема 12 (Э. Нётер). *Пусть X — неприводимое аффинное многообразие размерности m над числовым полем K. Тогда для почти всех $v \in V_f^K$ редукция $\underline{X}^{(v)}$ также является неприводимым многообразием размерности m.*

Сделаем одно замечание, касающееся определения многообразия $\underline{X}^{(v)}$. В качестве исходного можно взять определение $\underline{X}^{(v)}$ как редукции многообразия X относительно максимального идеала $\mathfrak{p}(v)$ кольца целых $\mathcal{O} \subset K$. Возникает вопрос, получим

ли мы то же многообразие $\underline{X}^{(v)}$, если возьмем кольцо $\mathcal{O}'$ S-целых элементов для некоторого подмножества $S \subset V^K$ такого, что $v \notin S$, и проведем редукцию относительно соответствующего максимального идеала $\mathfrak{p}'(v) \subset \mathcal{O}'$. Покажем, что ответ на этот вопрос утвердителен. Для этого рассмотрим идеалы $\mathfrak{b} = \mathfrak{a} \cap \mathcal{O}[x_1, \ldots, x_n]$ и $\mathfrak{b}' = \mathfrak{a} \cap \mathcal{O}'[x_1, \ldots, x_n]$. В силу нетеровости кольца $\mathcal{O}'$ по теореме Гильберта о базисе существует конечная система образующих $f_1, \ldots, f_r$ идеала $\mathfrak{b}'$. Так как $v \notin S$, то для подходящего $a \in \mathcal{O} \setminus \mathfrak{p}(v)$ все полиномы $af_1, \ldots, af_r$ лежат в $\mathcal{O}[x_1, \ldots, x_n]$ и, следовательно, в $\mathfrak{b}$. С учетом того, что $\mathcal{O}/\mathfrak{p}(v) = \mathcal{O}'/\mathfrak{p}'(v)$, отсюда вытекает, что редуцированные идеалы $\mathfrak{b}^{(\mathfrak{p}(v))}$ и $(\mathfrak{b}')^{(\mathfrak{p}'(v))}$ совпадают, т. е. $\underline{X}^{(\mathfrak{p}(v))} = \underline{X}^{(\mathfrak{p}'(v))}$. Тем самым редукция K-определенного многообразия определяется фактически не парой $\mathfrak{p}(v) \subset \mathcal{O}$, а лишь нормированием v, и поэтому обозначение $\underline{X}^{(v)}$ вполне оправдано. Отметим еще один аспект этого замечания. Если $x \in X_K$, то $x \in X_{\mathcal{O}'}$ для кольца S-целых $\mathcal{O}'$ относительно достаточно большого S. Тогда для $v \notin S$ точка x редуцируется в точку $\bar{x}$ многообразия $\underline{X}^{(\mathfrak{p}'(v))}$. Но в силу совпадения $\underline{X}^{(\mathfrak{p}(v))}$ и $\underline{X}^{(\mathfrak{p}'(v))}$ можно считать, что $\bar{x} \in \underline{X}^{(\mathfrak{p}(v))}$. В этой ситуации говорят, что для $v \notin S$ возможна редукция точки x по модулю $\mathfrak{p}(v)$ и результат редукции есть точка $\bar{x}$. Аналогичная терминология применяется к полиномам, регулярным отображениям и т. д.

В дальнейшем важную, хотя внешне и не столь заметную роль будет играть факт совпадения редукции $\underline{X}^{(v)}$ с редукцией $\underline{X}^{(\mathfrak{p}_v)}$ относительно максимального идеала $\mathfrak{p}_v$ в кольце целых $\overline{\mathcal{O}}_v$ соответствующего пополнения K_v (в последнем случае многообразие X рассматривается как K_v-определенное).

Лемма 10. *В описанной ситуации* $\underline{X}^{(v)} = \underline{X}^{(\mathfrak{p}_v)}$.

Доказательство. Положим $\mathfrak{b} = \mathfrak{a} \cap \mathcal{O}[x_1, \ldots, x_n]$, $\mathfrak{b}' = \mathfrak{a}_v \cap \mathcal{O}_v[x_1, \ldots, x_n]$, где $\mathfrak{a}_v$ — идеал полиномов из $K_v[x_1, \ldots, x_n]$, обращающихся в нуль на X. Пусть $f_1, \ldots, f_r$ и $g_1, \ldots, g_s$ — конечные системы образующих идеалов $\mathfrak{b}$ и $\mathfrak{b}'$ соответственно. Так как многообразие X определено над K, то найдутся такие полиномы $h_{ij} \in K_v[x_1, \ldots, x_n]$, что $g_i = \sum_{j=1}^{r} h_{ij} f_j$. Выбирая полиномы $t_{ij} \in K[x_1, \ldots, x_n]$ таким образом, чтобы их коэффициенты были достаточно близки к соответствующим коэффициентам полиномов h_{ij}, мы получим полиномы $g_i' = \sum_{j=1}^{r} t_{ij} f_j$, лежащие в $\mathcal{O}_v[x_1, \ldots, x_n] \cap \mathfrak{a}_v = \mathfrak{b}'$ и обладающие свойством $g_i \equiv g_i' \pmod{\mathfrak{p}_v}$. Далее, можно выбрать такое конечное подмножество $S \subset V_f^K$, $v \notin S$, что коэффициенты полиномов g_i' ле-

жат в кольце S-целых элементов $\mathcal{O}'$. Тогда легко видеть, что $\underline{X}^{(\mathfrak{p}'(v))} = \underline{X}^{(\mathfrak{p}_v)}$ для соответствующего идеала $\mathfrak{p}'(v) \subset \mathcal{O}'$, а тогда и $\underline{X}^{(\mathfrak{p}(v))} = \underline{X}^{(\mathfrak{p}_v)}$.

Тем же методом доказывается следующее утверждение, которое обосновывает независимость редукции относительно почти всех нормирований от поля определения.

Лемма 11. *Пусть L/K — конечное расширение числовых полей. Тогда для любого аффинного K-многообразия X и почти всех $v \in V_f^K$ редукция $\underline{X}^{(v)}$ совпадает с редукцией $\underline{X}^{(w)}$, где w — любое продолжение v на L и X рассматривается как L-многообразие.*

При работе с редукциями многообразий часто оказывается полезной следующая

Лемма 12. *Пусть $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$. Тогда если система*

$$f_i = 0, \quad i = 1, \ldots, r, \tag{4}$$

несовместна, т. е. не имеет решений над K, то для почти всех $v \in V_f^K$ редуцированная по модулю v система

$$\bar{f}_i = 0, \quad i = 1, \ldots, r, \tag{5}$$

также несовместна.

Доказательство. Так как (4) несовместна, то по теореме Гильберта о корнях найдутся такие полиномы $g_1, \ldots, g_r \in K[x_1, \ldots, x_n]$, что $f_1 g_1 + \ldots + f_r g_r = 1$. Тогда для почти всех v коэффициенты многочленов g_i являются v-целыми, и последнее равенство можно редуцировать по модулю v. Получим равенство $\bar{f}_1 \bar{g}_1 + \ldots + \bar{f}_r \bar{g}_r = 1$, из которого следует несовместность системы (5). Лемма доказана.

Упражнение 1. Используя лемму 12, получить доказательство теоремы 12 для основного с бирациональной точки зрения случая гиперповерхности в $\mathbb{A}^n$. Другими словами, показать, что если $f \in K[x_1, \ldots, x_n]$ — абсолютно неприводимый полином, то его редукция $\bar{f}$ по модулю v также абсолютно неприводима для почти всех $v \in V_f^K$. (Указание. Существование разложения $\bar{f} = gh$ можно интерпретировать как наличие решения у некоторой системы полиномиальных уравнений относительно коэффициентов полиномов g и h; с другой стороны, используя лемму 12, можно доказать ее неразрешимость для почти всех v.)

Предложение 19. *Пусть X — гладкое аффинное многообразие над полем алгебраических чисел K, все неприводимые компоненты которого имеют одну и ту же размерность m. Тогда для почти всех $v \in V_f^K$ редукция $\underline{X}^{(v)}$ является гладкой.*

Доказательство. Пусть $X \subset \mathbb{A}^n$, $\mathfrak{a} \subset K[x_1, \ldots, x_n]$ — идеал многочленов, обращающихся в нуль на X, и $\mathfrak{b} = \mathfrak{a} \cap \mathcal{O}[x_1, \ldots, x_n]$, где $\mathcal{O}$ — кольцо целых в K. Выберем конечную систему

образующих $f_1, \ldots, f_l$ идеала $\mathfrak{b}$ и обозначим через $\{D_j\}_{j=1}^{d}$ совокупность всех миноров размера $r \times r$, где $r = n - m$, матрицы Якоби

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \cdots & \cdots & \cdots \\ \frac{\partial f_l}{\partial x_1} & \cdots & \frac{\partial f_l}{\partial x_n} \end{pmatrix}.$$

Поскольку многообразие X является гладким, система

$$f_i = 0, \quad i = 1, \ldots, l,$$
$$D_j = 0, \quad j = 1, \ldots, d,$$

несовместна. Поэтому согласно лемме 12 для почти всех $v \in V_f^K$ редуцированная система также несовместна, т. е. редуцированное многообразие не содержит точек, для которых ранг матрицы Якоби меньше r. Но это как раз и означает, что редукция $\underline{X}^{(v)}$ является гладкой. Предложение 19 доказано.

Упражнение 2. Получить проективный аналог предложения 19.

Нам осталось еще показать, что редукция алгебраической группы является алгебраической группой. Для этого мы предварительно обсудим некоторые факты, связанные с редукцией морфизмов алгебраических многообразий. Пусть P — произвольное поле, и $f\colon X \to Y$ — регулярное P-определенное отображение двух P-определенных многообразий $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$. Тогда в координатах f задается набором многочленов $f_1, \ldots, f_m \in P[x_1, \ldots, x_n]$. Будем говорить, что отображение f определено над подкольцом $R \subset P$, если его можно задать многочленами из $R[x_1, \ldots, x_n]$. В этом случае для любого максимального идеала $\mathfrak{m} \subset R$ определено редуцированное регулярное отображение $\underline{f}^{(\mathfrak{m})} = (\bar{f}_1, \ldots, \bar{f}_m)$. Оказывается, что тем самым мы получаем регулярное отображение $\underline{f}^{(\mathfrak{m})}\colon \underline{X}^{(\mathfrak{m})} \to \underline{Y}^{(\mathfrak{m})}$ соответствующих редукций.

Лемма 13. $\underline{f}^{(\mathfrak{m})}(\underline{X}^{(\mathfrak{m})}) \subset \underline{Y}^{(\mathfrak{m})}$.

Доказательство. Пусть $\mathfrak{a}_X$ и $\mathfrak{a}_Y$ — отвечающие многообразиям X и Y идеалы в кольцах $P[x_1, \ldots, x_n]$ и $P[y_1, \ldots, y_m]$ соответственно, $\mathfrak{b}_X = \mathfrak{a}_X \cap \mathcal{O}[x_1, \ldots, x_n]$, $\mathfrak{b}_Y = \mathfrak{a}_Y \cap \mathcal{O}[y_1, \ldots, y_m]$. Обозначим через $f^*\colon P[y_1, \ldots, y_m] \to P[x_1, \ldots, x_n]$ ассоциированный с f коморфизм, который определяется условием $y_j \mapsto f_j(x_1, \ldots, x_n)$. Тогда включение $f(X) \subset Y$ означает, что $f^*(\mathfrak{a}_Y) \subset \mathfrak{a}_X$. Так как f определено над R, то одновременно $f^*(\mathfrak{b}_Y) \subset \mathfrak{b}_X$. Из последнего включения вытекает аналогичное включение для редукций $(f^*)^{(\mathfrak{m})}(\mathfrak{b}_Y^{(\mathfrak{m})}) \subset \mathfrak{b}_X^{(\mathfrak{m})}$, т. е. включение $\underline{f}^{(\mathfrak{m})}(\underline{X}^{(\mathfrak{m})}) \subset \underline{Y}^{(\mathfrak{m})}$. Лемма доказана.

В отличие от критериев определенности морфизма над полем (см. § 2.4), критериев определенности морфизма над кольцом (а, значит, и возможности его редукции), по-видимому, не существует. Мы будем иметь дело главным образом с морфизмами многообразий $f\colon X \to Y$, определенными над некоторым числовым полем K, и тогда заведомо возможна редукция f относительно почти всех v, которая приводит к регулярному отображению $\underline{f}^{(v)}\colon \underline{X}^{(v)} \to \underline{Y}^{(v)}$. Отсюда, в частности, вытекает, что редукция $\underline{X}^{(v)}$ для почти всех v не зависит от геометрической реализации X как замкнутого по Зарисскому подмножества аффинного пространства. Более точно, если X и Y бирегулярно изоморфны над K, то для почти всех v редукции $\underline{X}^{(v)}$ и $\underline{Y}^{(v)}$ также бирегулярно изоморфны над соответствующим полем вычетов. Кроме того, используя существование редукций морфизмов, можно с помощью аффинного покрытия определить редукцию произвольного многообразия. Укажем в общих чертах как это делается, отсылая за деталями к статье Вейля [4]. Пусть $X = \bigcup_{i=1}^{d} X_i$ — конечное аффинное покрытие произвольного K-многообразия X. Зафиксируем геометрические реализации X_i как замкнутых подмножеств аффинных пространств, т. е. K-определенные изоморфизмы $f_i\colon X_i \to X_i^0$, где X_i^0 замкнуто в $\mathbb{A}^{n_i}$. Положим $Y_{ij} = f_i(X_i \cap X_j) \subset \mathbb{A}^{n_i}$. Тогда возникают K-определенные морфизмы согласования $g_{ij}\colon Y_{ij} \to Y_{ji}$, $i, j = 1, \ldots, d$, причем в терминологии алгебраической геометрии исходное многообразие X получается склейкой многообразий X_i^0 относительно системы $\{Y_{ij}, g_{ij}\}$ (см. Шафаревич [1]). Согласно лемме 13 для почти всех v существует редукция $\underline{g}_{ij}^{(v)}$ всех морфизмов g_{ij}, и тогда, склеивая редукции $(\underline{X}_i^0)^{(v)}$ относительно системы $\{\underline{Y}_{ij}^{(v)}, \underline{g}_{ij}^{(v)}\}$ (выполнимость условий, необходимых для склейки, вытекает из того, что они выполняются для исходных морфизмов g_{ij}), получим многообразие $\underline{X}^{(v)}$, называемое *редукцией* X.

Предложение 20. *Пусть $G \subset \boldsymbol{GL}_n$ — K-определенная алгебраическая группа. Тогда для всех $v \in V_f^K$ редукция $\underline{G}^{(v)}$ является алгебраической группой, определенной над полем вычетов k_v, и отображение редукции $G_{\mathcal{O}} \to \underline{G}_{k_v}^{(v)}$ является гомоморфизмом групп. Кроме того, для почти всех v редукция $\underline{G}^{(v)}$ является гладкой, и тогда соответствующее локальное отображение редукции $G_{\mathcal{O}_v} \to \underline{G}_{k_v}^{(v)}$ сюръективно.*

Доказательство. Пусть $\mu\colon \boldsymbol{GL}_n \times \boldsymbol{GL}_n \to \boldsymbol{GL}_n$, $\mu(x, y) = xy$, — морфизм-произведение, $i\colon \boldsymbol{GL}_n \to \boldsymbol{GL}_n$, $i(x) = x^{-1}$, — морфизм-обращение. Тогда тот факт, что G является алгебраической группой, описывается включениями $\mu(G \times G) \subset G$, $i(G) \subset G$. Так

как μ и i определены над $\mathbb{Z}$, то возможна их редукция для любого v, и по лемме 13 $\underline{\mu}^{(v)}(\underline{G}^{(v)} \times \underline{G}^{(v)}) \subset \underline{G}^{(v)}$, $\underline{i}^{(v)}(\underline{G}^{(v)}) \subset \underline{G}^{(v)}$, т. е. $\underline{G}^{(v)}$ — алгебраическая группа. При этом отображение редукции совпадает с ограничением на $G_{\mathcal{O}}$ отображения $GL_n(\mathcal{O}) \xrightarrow{\rho} GL_n(k_v)$, индуцированного гомоморфизмом $\mathcal{O} \to k_v = \mathcal{O}/\mathfrak{p}(v)$. Но ρ, очевидно, является гомоморфизмом, поэтому отображение редукции — также гомоморфизм. Остается заметить, что поскольку G является гладким многообразием, то в силу предложения 19 редукция $\underline{G}^{(v)}$ является гладкой для почти всех v, и тогда по лемме Гензеля локальное отображение редукции $G_{\mathcal{O}_v} \to \underline{G}^{(v)}_{k_v}$ сюръективно. Предложение 20 доказано.

Предложение 21. *Пусть f: $G \to H$ — K-определенный морфизм алгебраических K-групп. Тогда для почти всех $v \in V_f^K$ возможна редукция f и редуцированный морфизм $\underline{f}^{(v)}$: $\underline{G}^{(v)} \to \underline{H}^{(v)}$ также является морфизмом алгебраических групп.*

Доказательство. Согласно лемме 13 и последующим замечаниям для почти всех $v \in V_f^K$ возможна редукция f, которая дает регулярное отображение $\underline{f}^{(v)}$: $\underline{G}^{(v)} \to \underline{H}^{(v)}$, и надо только установить его мультипликативность. Но мультипликативность f выражается в виде системы полиномиальных тождеств на $G \times G$, редукция которых дает аналогичную систему полиномиальных тождеств на $\underline{G}^{(v)} \times \underline{G}^{(v)}$, что и доказывает требуемое.

Предложение 22. *Пусть G — связная алгебраическая K-группа, H — ее связная K-определенная подгруппа и $X = G/H$. Тогда для почти всех $v \in V_f^K$ редукция $\underline{X}^{(v)}$ совпадает с однородным пространством $\underline{G}^{(v)}/\underline{H}^{(v)}$.*

Доказательство. Рассмотрим естественное действие f: $G \times X \to X$ и его редукцию $\underline{f}^{(v)}$: $\underline{G}^{(v)} \times \underline{X}^{(v)} \to \underline{X}^{(v)}$ для почти всех v. Тогда нам надо показать, что для почти всех v выполняются следующие условия:

1) действие $\underline{f}^{(v)}$ транзитивно;

2) стабилизатор $\underline{G}^{(v)}(\bar{x})$ точки $\bar{x} \in \underline{X}^{(v)}$, которая получается редукцией единичного класса $x = eH$, совпадает с $\underline{H}^{(v)}$.

Исключая из рассуждения конечное число v, можно считать, что редукции $\underline{G}^{(v)}$, $\underline{H}^{(v)}$ и $\underline{X}^{(v)}$ являются гладкими, причем эти многообразия неприводимы и их размерности совпадают соответственно с $d = \dim G$, $t = \dim H$ и $s = \dim X$. Положим $Y = \{(g, y) \in G \times X \mid gy = y\}$ и рассмотрим проекцию π: $Y \to X$. Тогда из теоремы о размерности слоев морфизма вытекает, что условие $\dim \pi^{-1}(y) > t$ определяет замкнутое подмногообразие $Z \subset X$. Так как в нашей ситуации $Z = \varnothing$, то из леммы 12 выте-

кает, что для почти всех v также $\underline{Z}^{(v)} = \varnothing$, т. е. $\underline{X}^{(v)}$ не содержит точек y, для которых $\dim \underline{G}^{(v)}(y) > t$. Из подсчета размерностей и предложения 2.23 вытекает справедливость условия 1). Далее, из теоремы 12 получаем, что для почти всех v стабилизатор $\underline{G}^{(v)}(\bar{x})$ должен быть связным. С другой стороны, он содержит $\underline{H}^{(v)}$ и имеет ту же размерность. Поэтому $\underline{G}^{(v)}(\bar{x}) = \underline{H}^{(v)}$, и предложение доказано.

§ 3.4. Элементы теории Брюа — Титса

Брюа и Титсом в работах [2—4] была построена фундаментальная теория для исследования групп рациональных точек полупростых алгебраических групп над локальными полями. В основе этой теории лежит конструкция в группе точек простой односвязной группы G над локальным полем K некоторой BN-пары, которая оказывается связанной с системой корней аффинного типа. Далее, при помощи BN-пары определяется некоторый симплициальный комплекс $\mathscr{A}$, называемый основой *), на котором действует группа G_K. Этот комплекс оказывается стягиваемым, и использование его свойств позволяет получить информацию о группе G_K и ее подгруппах. (Отметим, что в действительности основа является естественным неархимедовым аналогом симметрического пространства $G_R/\boldsymbol{K}$ по максимальной компактной подгруппе $\boldsymbol{K} \subset G_R$ в архимедовом случае; сравните, в частности, предложение 11.) Пусть, например, $B \subset G_K$ — компактная подгруппа. Доказывается, что естественное действие B на $\mathscr{A}$ обладает неподвижной вершиной. Но стабилизаторы вершин (так называемые *максимальные парахорические подгруппы*) сами компактны, откуда следует, что класс максисальных компактных подгрупп в G_K совпадает с классом максимальных парахорических подгрупп. С другой стороны, парахорические подгруппы допускают описание на языке аффинной системы корней, которое аналогично отмеченному в § 2.1, п. 12 описанию параболических подгрупп, что позволяет определить их классы сопряженности и, в частности, вычислить их количество (см. ниже теорему 13). Тем самым с помощью теории Брюа — Титса мы получаем элегантное решение задачи об описании максимальных компактных подгрупп в G_K. К сожалению, в настоящей книге мы не сможем сколько-нибудь подробно остановиться на теории Брюа — Титса, отсылая читателя к указанным выше оригинальным работам, а также статьям Ивахори — Мацумото [1], Макдональда [1], Сатаке [2], Хидзикаты [2]. Дело в том, что изложение этой теории требует введения целого ряда новых определений (которыми мы в дальнейшем

*) По-французски immeuble; по-английски building.

нигде не будем пользоваться) и фактически связано с построением нескольких самостоятельных «подтеорий», так что объем полного изложения сравним с объемом этой книги. Поэтому мы ограничимся описанием основных объектов (беря, правда, при этом в качестве определений результаты теории) и формулировкой некоторых теорем.

Итак, пусть G — простая односвязная алгебраическая группа, определенная над конечным расширением K поля $\mathbb{Q}_p$. *Подгруппой Ивахори* $B \subset G_K$ называется нормализатор силовской про-p-подгруппы в G_K. Отметим, что из сопряженности силовских про-p-подгрупп (теорема 10) вытекает сопряженность подгрупп Ивахори. Подгруппа $\mathscr{P} \subset G_K$ называется *парахорической*, если она содержит некоторую подгруппу Ивахори. *Основой* $\mathscr{A}$ группы G_K (или группы G над K) называется симплициальный комплекс, вершинами которого служат максимальные собственные парахорические подгруппы группы G_K, причем набор $\{\mathscr{P}_0, \mathscr{P}_1, \ldots, \mathscr{P}_s\}$ таких подгрупп определяет s-симплекс в $\mathscr{A}$, если пересечение $\bigcap_{i=0}^{s} \mathscr{P}_i$ также является парахорической подгруппой. Группа G_K действует на $\mathscr{A}$ посредством сопряжений, причем это действие сохраняет симплициальную структуру, и стабилизаторы симплексов являются собственными парахорическими подгруппами. Иногда под основой понимают также геометрическую реализацию указанного симплициального комплекса. В этом смысле $\mathscr{A}$ является стягиваемым геометрическим комплексом (теорема Соломона — Титса), размерность которого совпадает с K-рангом группы G. В частности, если $\operatorname{rang}_K G = 1$, то построенный комплекс является деревом, и к нему можно применить структурную теорию групп, действующих на деревьях (см. Серр [10]). Отсюда, например, получается, что в этом случае любая дискретная подгруппа $\Gamma \subset G_K$ без кручения является свободной (для $G = \boldsymbol{SL}_2$ эта теорема была получена Ихарой [1]; отметим также, что пример группы $\boldsymbol{SL}_2$ подробно разобран в книге Хамфри [2]).

Перейдем теперь к построению так называемой BN-пары в G_K. Предварительно напомним (см. подробнее Бурбаки [4], гл. IV), что *BN-парой* (или *системой Титса*) в абстрактной группе G называется пара подгрупп B, $N \subset G$ таких, что для некоторого подмножества $R \subset N/B \cap N$ выполняются следующие аксиомы:

1) множество $B \cup N$ порождает G и $H = B \cap N$ является нормальной подгруппой N;

2) множество R порождает группу $W = N/H$ и состоит из элементов порядка 2;

3) $rBw \subset BwB \cup BrwB$ для $r \in R$, $w \in W$;

4) $rBr \not\subset B$ для любого $r \in R$.

Группа $W = N/H$ называется *группой Вейля* пары (B, N). Элементы из W являются классами смежности по H, однако двойной смежный класс BgB не зависит от выбора представителя $g \in w$, где $w \in W$, и поэтому его обычно обозначают через BwB; в этом смысле следует понимать соотношения пунктов 3)—4). Отметим также, что множество R однозначно восстанавливается по B и N, а именно, состоит из таких $w \in W$, что объединение $B \cup BwB$ является подгруппой в G.

Пусть теперь снова G — простая односвязная алгебраическая K-группа, $S \subset G$ — максимальный K-разложимый тор. Обозначим через $N_G(S)$ и $Z_G(S)$ соответственно нормализатор и централизатор тора S и положим $N = N_G(S)_K$,

$$H = \{x \in Z_G(S)_K \mid \chi(x) \in U \quad \forall \chi \in \mathbf{X}(Z_G(S))_K\},$$

где U — группа v-адических единиц в K. Тогда существует такая подгруппа Ивахори $B \subset G_K$, что $B \cap N = H$ и группы B, N образуют BN-пару в G_K. При этом оказывается, что группа Вейля $W = N/H$ совпадает с группой Вейля некоторой аффинной системы корней R ранга $l = \dim S$ (определение аффинной группы Вейля см. в книге Бурбаки [4], гл. VI, § 2). В частности, подмножество $R \subset W$ выделенных образующих состоит из $(l+1)$ элементов $r_1, r_2, \ldots, r_{l+1}$, которые можно занумеровать таким образом, что первые l элементов порождают подгруппу $W_0 \subset W$, изоморфную группе Вейля некоторой обычной приведенной системы корней, ассоциированной с R. Отметим, что группа W_0 совпадает с относительной группой Вейля $W(S, G) = N_G(S)/Z_G(S)$, однако в общем случае система R_0 отлична от относительной системы корней $R(S, G)$, даже если последняя является приведенной. При этом все же каждый корень из R_0 пропорционален некоторому корню из $R(S, G)$, и наоборот. В случае K-разложимой группы G, т. е. когда S — максимальный тор в G, всегда $R_0 = R(S, G)$.

Из общей теории групп с BN-парой вытекает, что любая подгруппа $P \subset G_K$, содержащая B, имеет вид $P_S = BW_SB$, где $S \subset R$ — некоторое подмножество, W_S — подгруппа в W, порожденная S. При этом если подгруппы P_{S_1} и P_{S_2} сопряжены в G_K, то $S_1 = S_2$. Отсюда следует, что полную систему представителей классов сопряженности максимальных собственных парахорических подгрупп образуют подгруппы $\mathscr{P}_i = P_{S_i}$, где $S_i = R \setminus \{r_i\}$, $i = 1, \ldots, l+1$. Так как класс максимальных собственных парахорических подгрупп совпадает с классом максимальных компактных подгрупп, то мы приходим к следующему результату:

Теорема 13. *Пусть G — простая односвязная алгебраическая K-группа, $l = \operatorname{rang}_K G$. Тогда в группе G_K имеется ровно $l+1$ классов сопряженности максимальных компактных подгрупп.*

Из теоремы 13, в частности, вытекает, что в любой полупростой односвязной K-группе число классов сопряженности максимальных компактных подгрупп конечно. В теории Брюа — Титса доказывается, что это утверждение сохраняет силу для произвольной редуктивной K-группы.

Для групп рациональных точек имеется ряд разложений, часть из которых является неархимедовыми аналогами разложений из § 3.2. Из этого комплекса результатов нам понадобится лишь неархимедов аналог разложения Картана, на котором мы остановимся более подробно. Сохраним обозначения, введенные выше. Пусть $\mathbf{K}$ — максимальная компактная подгруппа BW_0B. Известно, что группа W является полупрямым произведением $W = W_0T$, где T — абелева группа, порожденная корнями из R_0; отметим, что T — свободная абелева группа ранга $l = \dim S$. Далее, специальным образом строится подполугруппа $T^+ \subset T$ «положительных» элементов (более точно, в системе R_0 выбирается система простых корней Π_0, ассоциированная с B, и тогда T^+ состоит из таких $t \in T$, что $\langle t, \alpha\rangle \geqslant 0$ для всех $\alpha \in \Pi_0$, где $\langle , \rangle$ — некоторая положительно определенная симметрическая билинейная форма на $T \otimes_{\mathbb{Z}} \mathbb{R}$, инвариантная относительно W_0). Обозначим через ν естественный гомоморфизм $N \to W = N/H$ и положим $Z^+ = \nu^{-1}(T^+)$. Заметим теперь, что если $z_1, z_2 \in Z_G(S)_K$ и $\nu(z_1) = \nu(z_2)$, то $z_1z_2^{-1} \in H$, и поэтому $\mathbf{K}z_1\mathbf{K} = \mathbf{K}z_2\mathbf{K}$. Тем самым для $z \in Z_G(S)_K$ двойной смежный класс $\mathbf{K}z\mathbf{K}$ зависит лишь от $t = \nu(z)$, так что его естественно обозначать через $\mathbf{K}\nu^{-1}(t)\mathbf{K}$. В этих обозначениях справедлива

Теорема 14 (разложение Картана). *$G_K = \mathbf{K}Z^+\mathbf{K}$ и отображение $t \mapsto \mathbf{K}\nu^{-1}(t)\mathbf{K}$ взаимно однозначно отображает T^+ на множество двойных смежных классов $\mathbf{K}\backslash G_K/\mathbf{K}$.*

Пример. Пусть $G = \boldsymbol{SL}_n$, $K = \mathbb{Q}_p$. Легко видеть, что силовская про-p-группа группы $SL_n(\mathbb{Q}_p)$ состоит из матриц $x = (x_{ij}) \in SL_n(\mathbb{Z}_p)$ таких, что $x_{ii} \equiv 1 \pmod p$, $x_{ij} \equiv 0 \pmod p$ для всех $i, j = 1, \ldots, n$, $i > j$. Поэтому соответствующая подгруппа Ивахори $B \subset SL_n(\mathbb{Q}_p)$ описывается следующим образом: $B = \{x = (x_{ij}) \in SL_n(\mathbb{Z}_p) \mid x_{ij} \equiv 0 \pmod p \text{ для } i > j\}$. Эта подгруппа вместе с нормализатором N диагонального тора $S \subset G$ образует описанную выше BN-пару. Выделенную систему образующих $R \subset W = N/B \cap N$ составляют классы следующих матриц:

$$r_1 = \begin{pmatrix} 0 & 1 & & & \\ -1 & 0 & & & 0 \\ & & 1 & & \\ & & & \ddots & \\ & 0 & & & 1 \end{pmatrix}, \ldots,$$

$$r_i = \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & 0 & \\ & & \ddots & & & & & & \\ & & & 0 & 1 & & & & \\ & & & -1 & 0 & & & & \\ & & & & & 1 & & & \\ & & & & & & \ddots & & \\ & 0 & & & & & & \ddots & \\ & & & & & & & & 1 \end{pmatrix}, \ldots, \quad r_n = \begin{pmatrix} 0 & 0 & \ldots & & p^{-1} \\ & 1 & & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & & & 1 & \\ -p & & \ldots & & 0 \end{pmatrix}.$$

Парахорическая подгруппа $\mathscr{P} = BW_0B$, где W_0 порождена $r_1, \ldots, r_{n-1}$, совпадает с группой $SL_n(\mathbb{Z}_p)$. Остальные максимальные собственные парахорические подгруппы имеют вид $\mathscr{P}_i = BW_iB$ для $i = 1, \ldots, n-1$, где W_i порождена $R \setminus \{r_i\}$. Несложно показать, что $\mathscr{P}_i$ совпадает со стабилизатором в $SL_n(\mathbb{Q}_p)$ решетки с базисом $e_1, \ldots, e_{n-i}, pe_{n-i+1}, \ldots, pe_n$, где $e_1, \ldots, e_n$ — стандартный базис пространства $\mathbb{Q}_p$. Читатель без труда проверит, что получаемая таким образом классификация классов сопряженности максимальных компактных подгрупп группы $SL_n(\mathbb{Q}_p)$ совпадает с той, которая была получена при доказательстве предложения 14. Проиллюстрируем, наконец, разложение Картана в $SL_n(\mathbb{Q}_p)$. Как мы видели выше, здесь подгруппа $\mathbf{K}$ совпадает с $SL_n(\mathbb{Z}_p)$. Группа T здесь изоморфна подгруппе в $\mathbb{Z}^n$, состоящей из таких $(a_1, \ldots, a_n) \in \mathbb{Z}^n$, что $\sum_{i=1}^{n} a_i = 0$; при этом систему Π_0 простых корней образуют элементы $\alpha_i = (0, \ldots, 0, 1, -1, 0, \ldots, 0)$, $i = 1, \ldots, n-1$ (сравните с описанием системы корней группы $G = \boldsymbol{SL}_n$ в § 2.1, п. 1.3). Группа Вейля $W_0 \simeq S_n$ действует на T перестановками координат, поэтому инвариантным относительно W_0 будет обычное скалярное произведение. Отсюда следует, что множество T^+ в данном случае состоит из таких $(a_1, \ldots, a_n) \in T$, что $a_1 \leqslant a_2 \leqslant \ldots \leqslant a_n$. Теорема 14 тогда утверждает, что в любом двойном смежном классе $\mathbf{K}g\mathbf{K}$, $g \in SL_n(\mathbb{Q}_p)$, найдется представитель вида $\operatorname{diag}(p^{a_1}, p^{a_2}, \ldots, p^{a_n})$, где $a_1 \leqslant a_2 \leqslant \ldots \leqslant a_n$, причем числа a_i определены однозначно. Поэтому в данном случае теорема 14 фактически сводится к известной теореме об инвариантных множителях для матриц (см., например, Кэртис, Райнер [1], гл. III, § 16): если A — кольцо главных идеалов, то для любой матрицы $X \in M_n(A)$ найдутся такие матрицы $Y_1, Y_2 \in SL_n(A)$, что $Y_1XY_2 = \operatorname{diag}(d_1, \ldots, d_r, 0 \ldots 0)$, где $d_i \in A$, $d_i \neq 0$ и d_i делит d_{i+1} для всех $i = 1, \ldots, r-1$; при этом элементы d_i (называемые *инвариантными множителями* матрицы X) определены однозначно с точностью до умножения на обратимый элемент кольца A.

В оставшейся части параграфа мы с помощью теоремы 14 установим факт компактной определенности группы G_K (этот результат будет использован в § 5.4 для доказательства конечной определенности S-арифметических подгрупп). Для точной формулировки соответствующего утверждения условимся о следующей терминологии. Будем говорить, что подмножество C абстрактной группы Γ является *определяющим*, если оно порождает Γ и любое соотношение в Γ между элементами из C является следствием соотношений вида $ab=c$, где $a, b, c \in C$. Другими словами, это означает, что естественный гомоморфизм $f\colon F(C)\to\Gamma$ свободной группы $F(C)$, порожденной C, сюръективен и его ядро $N=\operatorname{Ker} f$ порождается как нормальный делитель в $F(C)$ элементами вида abc^{-1}, где $a, b, c \in C$. Топологическая группа Γ называется компактно определенной, если существует компактное подмножество $C\subset\Gamma$, которое является определяющим для Γ, рассматриваемой как абстрактная группа.

Теорема 15 (Бер [2]). *Пусть G — редуктивная группа, определенная над неархимедовым локальным полем K. Тогда группа G_K является компактно определенной.*

Доказательство. Легко видеть, что для доказательства компактной определенности топологической группы Γ достаточно найти такое компактное подмножество $C\subset\Gamma$, порождающее Γ как абстрактную группу, что все соотношения в Γ между элементами из C являются следствиями соотношений ограниченной длины (этим замечанием мы будем неоднократно пользоваться в дальнейшем). Разберем вначале случай простой односвязной K-группы G. Здесь доказательство компактной определенности G_K получается из следующего утверждения.

Лемма 14. *Пусть топологическая группа Γ снабжена функцией $|\ |$ («абсолютной величиной»), которая принимает целочисленные значения и обладает следующими свойствами:*

а) $|g|\geqslant 0$, $|1|=0$;
б) $|g_1g_2|\leqslant|g_1|+|g_2|$ *для всех* $g_1, g_2\in\Gamma$;
в) $|g^{-1}|=|g|$ *для всех* $g\in\Gamma$;
г) *множества* $\Gamma_n=\{g\in\Gamma \mid |g|\leqslant n\}$ *компактны.*

Предположим, далее, что существуют неотрицательные целые числа c, d и b, для которых выполняются следующие условия:

(i) *если для $g\in\Gamma$ имеем $|g|>c$, то найдутся такие $g_1, g_2\in\Gamma$, что $g=g_1g_2$ и $|g_1|<c$, $|g_2|<|g|-d$;*

(ii) *если $f, g, h\in\Gamma$ и $fgh=1$, то найдутся такие $g_1, g_2, \ldots, g_t\in\Gamma$, что $g=g_1g_2\ldots g_t$, $|g_i|\leqslant c$ $(i=1, \ldots, t)$, $t\leqslant|g|+b$ и $|fg_1\ldots g_j|\leqslant\max\{|f|, |h|\}+d$ $(j=1, \ldots, t-1)$. Тогда группа Γ является компактно определенной.*

Доказательство. Из г) и (i) вытекает, что Γ_c является компактным порождающим множеством для Γ, поэтому достаточно показать, что все соотношения между элементами Γ_c являются следствиями соотношений ограниченной длины. Мы получим явную оценку для длины «базисных» соотношений:

$$l \leqslant l_0 = \max\left\{3c + b + 3,\ 2\left[\frac{c}{d+1}\right] + 5\right\},$$

где [ ] означает целую часть числа. Поскольку Γ_c вместе с каждым элементом g содержит g^{-1}, а также 1, то достаточно рассмотреть соотношения r вида

$$\prod_{i=1}^{n} g_i = 1 \qquad (g_i \in \Gamma_c).$$

Положим $p_j = \prod_{i=j}^{n} g_i$ и $\|r\| = \max\limits_{1 \leqslant j \leqslant n} \{|p_j|\}$. Покажем вначале, что любое соотношение r является следствием таких соотношений r', что $\|r'\| \leqslant 2c$. Доказательство будем вести индукцией по $\|r\|$. Пусть $\|r\| > 2c$ и j — такой индекс, что $\max\{|p_j|, |p_{j+1}|\} = \|r\|$. Поскольку $|g_j| \leqslant c$, то при этом $\min\{|p_j|, |p_{j+1}|\} > c$, и в силу (i) мы можем найти такие элементы $g'_j, g'_{j+1} \in \Gamma_c$, что

$$|g_j'^{-1} p_j| < |p_j| - d \quad \text{и} \quad |g_{j+1}'^{-1} p_j| < |p_{j+1}| - d.$$

Положим $f = p_j^{-1} g'_j$, $g = g_j'^{-1} g_j g'_{j+1}$, $h = g_{j+1}'^{-1} p_j$. Тогда $fgh = 1$ и $\max\{|f|, |h|\} < \|r\| - d$. Применяя (ii), найдем такие $\bar{g}_1, \ldots, \bar{g}_t \in \Gamma_c$, что $g = \bar{g}_1 \ldots \bar{g}_t$, $t \leqslant |g| + b$ и $|f\bar{g}_1 \ldots \bar{g}_k| \leqslant \max\{|f|, |h|\} + d$ для всех $k = 1, \ldots, t-1$. Так как $|g| \leqslant 3c$, то $t \leqslant 3c + b$. Введем в рассмотрение соотношения

$$r_j\colon\ g_j = g'_j \bar{g}_1 \ldots \bar{g}_t g_{j+1}'^{-1},$$

длина которых не превосходит l_0. Заменим теперь g_j в r правой частью r_j для всех индексов j таких, что $\max\{|p_j|, |p_{j+1}|\} = \|r\|$ (где, естественно, в случае $|p_j| = \|r\|$ для пар $(j-1, j)$ и $(j, j+1)$ выбирается один и тот же элемент g'_j). Тогда для любого $k \leqslant t$ имеем $|\bar{g}_k \ldots \bar{g}_t g_{j+1}'^{-1} p_j| = |f\bar{g}_1 \ldots \bar{g}_{k-1}| < \|r\|$. Таким образом, мы получим соотношение r', которое эквивалентно исходному по модулю соотношений r_j, и для которого $\|r'\| < \|r\|$. Повторяя описанный процесс несколько раз, мы придем к соотношению r_0, для которого $\|r_0\| \leqslant 2c$.

Итак, осталось проанализировать соотношения

$$r\colon\ \prod_{i=1}^{n} g_i = 1$$

со свойством $\|r\| \leqslant 2c$. Тогда для любого j, $1 \leqslant j \leqslant n$, имеем $|p_j| \leqslant 2c$, и поэтому в силу (i) мы можем представить p_j в виде произведения самое большее $\left(\left[\frac{c}{d+1}\right]+2\right)$ множителей из Γ_c. Выразим p_j^{-1} в виде произведения обратных множителей. Подставляя эти выражения в соотношение $g_j = p_j p_{j+1}^{-1}$ для $1 \leqslant j \leqslant n-1$ (соответственно в соотношение $g_n = p_n$ для $j = n$), мы получим соотношения, длина которых ограничена числом $\left(2\left[\frac{c}{d+1}\right]+5\right) \leqslant l_0$. С другой стороны, ясно, что r является следствием этих соотношений. Лемма доказана.

Чтобы построить функцию $|\ |$ на группе $\Gamma = G_K$ с описанными в лемме 14 свойствами, поступим следующим образом. Зафиксируем максимальный K-разложимый тор $S \subset G$ (отметим, что если $S = (e)$, то в силу теоремы 1 группа G_K компактна, и в качестве компактного определяющего множества можно взять $C = G_K$). Сохраним обозначения, введенные выше, в частности, пусть $R(S, G)$ — относительная система корней. Тогда для $\mathfrak{g} = L(G)$ имеем разложение

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \left(\bigoplus_{\alpha \in R(S,\, G)} \mathfrak{g}_\alpha\right),$$

где $\mathfrak{g}_0$ — централизатор $\operatorname{Ad} S$, $\mathfrak{g}_\alpha$ — весовое подпространство относительно $\operatorname{Ad} S$ веса $\alpha \in R(S, G)$. Зафиксируем некоторые решетки $L_0 \subset (\mathfrak{g}_0)_K$, $L_\alpha \subset (\mathfrak{g}_\alpha)_K$ и положим $L = L_0 \oplus \left(\bigoplus_{\alpha \in R(S,\, G)} L_\alpha\right)$. Введем, далее, расстояние между двумя решетками L_1, $L_2 \subset \mathfrak{g}_K$:

$$d(L_1, L_2) = \min\{n \mid \pi^n L_1 \subseteq L_2 \subseteq \pi^{-n} L_1\},$$

где $\pi \in K$ — униформизующий элемент. Наша цель — показать, что для функции $|\ |$ на группе $\Gamma = G_K$, определяемой формулой

$$|g| = d(L, \operatorname{Ad}(g) L),$$

выполняются все требования леммы 14. Выполнимость свойств а) — г) проверяется непосредственно. Отметим только, что для доказательства компактности Γ_n при любом целом $n > 0$ следует заметить, что из ограниченности $|\ |$ на Γ_n вытекает ограниченность, а следовательно, и компактность $\operatorname{Ad}(\Gamma_n)$; с другой стороны, отображение $\Gamma \to \operatorname{Ad}(\Gamma)$ открыто (следствие 1 из предложения 3.3), имеет конечное ядро и поэтому является собственным, т. е. прообраз компакта является компактом.

Для проверки (i), (ii) нам понадобится одно разложение группы G_K, которое является следствием разложения Картана $G_K = \mathbf{K} Z^+ \mathbf{K}$. По построению Z^+ является прообразом относительно канонического гомоморфизма ν: $N \to W = N/H$ полугруппы $T^+ \subset W$, которая определяется как совокупность таких элементов t из абелевой группы T, порожденной корнями из R_0.

что $\langle t, \alpha\rangle \geqslant 0$ для всех α из системы простых корней Π_0. Анализ конструкций из теории Брюа — Титса показывает, что $\nu(S_K) \subset T$. Но $S_K \simeq (K^*)^l \simeq Z^l \times U^l$, где $l = \dim S$, U — группа единиц в K. С другой стороны, из компактности $H = \operatorname{Ker} \nu$ вытекает компактность $\operatorname{Ker}(\nu|S_K)$, а следовательно, включение $\operatorname{Ker}(\nu|S_K) \subset U^l$. Поэтому $\nu(S_K)$ содержит свободную абелеву подгруппу ранга l. Но T сама является свободной абелевой группой ранга l, так что индекс $m = [T : \nu(S_K)]$ конечен. Тогда $\nu(S_K) \supset mT$ и $\nu(S_K) \cap T^+ \supset mT^+$. Мы оставляем читателю в качестве упражнения показать, что полугруппа T^+ конечно порождена. Отсюда вытекает, что полугруппа $\nu(S_K) \cap T^+$ также конечно порождена; положим $S^+ = Z^+ \cap S_K$. Имеем $\nu(S^+) = \nu(S_K) \cap T^+$, поэтому $\nu(S^+) \supset mT^+$, и, следовательно, существует такое конечное подмножество $E \subset Z^+$, что $\nu(ES^+) = T^+$. Тогда $Z^+ = HES^+$ и

$$G_K = \mathbf{K}Z^+\mathbf{K} = \mathbf{K}ES^+\mathbf{K}. \tag{1}$$

Далее, для $s \in S_K$, $\alpha \in R_0$ справедлива формула

$$\langle \nu(s), \alpha\rangle = v(\alpha(s)),$$

где v — нормирование поля K.

Поэтому, учитывая взаимную пропорциональность корней из R_0 и $R(S, G)$, получим, что $v(\alpha(s)) \geqslant 0$ для $s \in S^+$ и всех корней $\alpha \in R(S, G)$, положительных относительно порядка, согласованного с системой простых корней $\Pi_0 \subset R_0$. Отсюда следует, что для $s \in S_0$ значения $|s|$ задаются формулой $|s| = v(\alpha_0(s))$, где $\alpha_0 \in R(S, G)$ — максимальный корень; в частности, если $s = s_1 s_2 (s, s_1, s_2 \in S^+)$, то $|s| = |s_1| + |s_2|$. Как мы видели выше, полугруппа $\nu(S^+)$ является конечнопорожденной, поэтому существует такое целое число $r > 0$, что элементы $s \in S^+$ со свойством $|s| \leqslant r$ порождают S^+ как полугруппу. Введем еще две целочисленные константы, через которые будут выражаться искомые константы c, d и b, удовлетворяющие лемме 14. А именно, из компактности $\mathbf{K}$ и конечности E вытекает существование таких целых c_1, c_2, что $|k| \leqslant c_1$, $|e| \leqslant c_2$ для всех $k \in \mathbf{K}$, $e \in E$.

При доказательстве (i) зафиксируем некоторое целое неотрицательное число d и положим $c = 5c_1 + 2c_2 + r + d$. Если $|g| > c$ и $g = k_1 e s k_2$ — разложение вида (1), то

$$|s| = |e^{-1}k_1^{-1}gk_2^{-1}| > 3c_1 + c_2 + r + d.$$

Существуют такие $s_1, s_2 \in S^+$, что $s = s_1 s_2$ и $3c_1 + c_2 + d < |s_1| \leqslant 3c_1 + c_2 + r + d$. Тогда для $g_1 = k_1 e s_1$ и $g_2 = s_2 k_2$ будем иметь

$$|g_1| \leqslant |s_1| + c_1 + c_2 \leqslant 4c_1 + 2c_2 + r + d \leqslant c,$$

$$|g_2| \leqslant |s_2| + c_1 = |s| - |s_1| + c_1 <$$
$$< |g| + 2c_1 + c_2 + c_1 - (3c_1 + c_2 + d) = |g| - d.$$

Перед тем как переходить к доказательству (ii), сделаем одно замечание. Для элемента $s \in S^+$ из включения $\pi^n \operatorname{Ad}(s) L \subset L$ вытекает включение $\pi^n L \subset \operatorname{Ad}(s) L$. Оказывается, что несколько более слабая импликация выполняется для любого $g \in G_K$. А именно, пусть для $g \in G_K$ имеет место включение $\pi^n \operatorname{Ad}(g) L \subset \subset L$. Выберем разложение $g = k_1 e s k_2$ вида (i). Тогда в силу свойств б), в) функции $|\ |$ имеем $\pi^{n+2c_1+c_2} \operatorname{Ad}(s) \subset L$, откуда $\pi^{n+2c_1+c_2} L \subset \operatorname{Ad}(s) L$, и, наконец, $\pi^{n+4c_1+2c_2} L \subset \operatorname{Ad}(g) L$.

Пусть теперь $f, g, h \in G_K$ удовлетворяют соотношению $fgh = = 1$. Представим g в виде $g = k_1 e s k_2$ и разложим s в произведение $s = s_1 \ldots s_t$, где $s_i \in S^+$ и $|s_i| \leqslant r$. Тогда, положив $g_1 = = k_1 e s_1$, $g_2 = s_2, \ldots, g_{t-1} = s_{t-1}$, $g_t = s_t k_2$, будем иметь

$$|g_t| \leqslant c_1 + c_2 + r \leqslant c = 5c_1 + 2c_2 + r + d$$

(для произвольного выбора d). Кроме того, можно считать, что $t \leqslant |s| \leqslant |g| + b$, где $b = 2c_1 + c_2$. Для $j \in \{1, \ldots, t-1\}$ введем отрезки $u = s_1 \ldots s_j$ и $v = s_{j+1} \ldots s_t$. Тогда из определения L вытекает, что

$$\operatorname{Ad}(u) L \subset \operatorname{Ad}(s) L + L,$$

откуда $\operatorname{Ad}(f k_1 e u) \subset \operatorname{Ad}(f k_1 e s) L + \operatorname{Ad}(f k_1 e) L$, т. е. $\pi^n \operatorname{Ad}(f k_1 e u) L \subset \subset L$ для $n = \max\{|f k_1 e s|, |f k_1 e|\}$. Поэтому из сделанного выше замечания вытекает, что

$$|f k_1 e u| \leqslant \max\{|f k_1 e s|, |f k_1 e|\} + 4c_1 + 2c_2.$$

С другой стороны,

$$|f k_1 e s| \leqslant |f k_1 e s k_2| + |k_2| \leqslant |fg| + c_1 = |h| + c_1$$

и

$$|f k_1 e| \leqslant |f| + |k_1 e| \leqslant |f| + c_1 + c_2.$$

Окончательно мы получаем, что

$$|f g_1 \ldots g_j| \leqslant \max\{|f|, |h|\} + (5c_1 + 3c_2).$$

Полагая тогда $d = 5c_1 + 3c_2$ (в этом случае $c = 10c_1 + 5c_2 + + r$), мы и получим искомые константы c, d и b. Тем самым доказательство компактной определенности группы G_K для простой односвязной K-группы G завершено. Оставшаяся часть рассуждений представляет несложную редукцию к этому случаю.

Прежде всего, любая полупростая односвязная K-группа имеет вид $G = \prod_{i=1}^{d} \mathbf{R}_{L_i/K}(G_i)$, где G_i — простые односвязные группы, определенные над конечными расширениями L_i поля $K (i = 1, \ldots, d)$, так что $G_K \simeq \prod_{i=1}^{d} (G_i)_{L_i}$. Легко видеть, что произведение компактно определенных групп является компактно определенной группой; с другой стороны, согласно доказанному

выше все группы $(G_i)_{L_i}$ являются компактно определенными. Поэтому группа G также компактно определена. Пусть теперь G — произвольная редуктивная K-группа. Тогда $G = DT$ — почти прямое произведение, где группа D полупроста, а T — максимальный центральный тор в G. Обозначим через π: $\tilde{D} \to D$ универсальное K-определенное накрытие и представим тор T в виде почти прямого произведения $T = T_1T_2$, где тор T_1 K-разложим, а тор T_2 K-анизотропен. Положим $H = \tilde{D} \times T_1 \times T_2$ и обозначим через φ изогению $H \to G$, которая получается из π и морфизма-произведения; пусть $F = \operatorname{Ker} \varphi$. Тогда из точной последовательности $1 \to F \to H \xrightarrow{\varphi} G \to 1$ получается точная когомологическая последовательность

$$H_K \xrightarrow{\varphi} G_K \to H^1(K, F),$$

поэтому из предложения 3 и теоремы конечности для когомологий Галуа над локальными полями, которую мы установим в § 6.4, вытекает, что $\varphi(H_K)$ является открытой подгруппой в G_K конечного индекса (для полупростой группы G этот факт также вытекает из предложения 17). Но группа $\varphi(H_K)$ является компактно определенной. В самом деле, по построению $H_K = \tilde{D}_K \times \times (T_1)_K \times (T_2)_K$. Выше мы установили, что группа $\tilde{D}_K$ компактно определена. Из теоремы 1 вытекает, что группа $(T_2)_K$ компактна и, следовательно, и компактно определена. Наконец, $(T_1)_K \simeq \simeq K^{*l} \simeq \mathbb{Z}^l \times U^l$, где $l = \dim T_1$, U — группа единиц в K, откуда с очевидностью получаем компактную определенность группы $(T_1)_K$. Таким образом, группа H_K компактно определена. Без ограничения общности можно считать, что компактное определяющее множество $C \subset H_K$ содержит F_K. Тогда легко показать, что $\varphi(C)$ является компактным определяющим множеством для $\varphi(H_K)$. Поэтому завершает доказательство теоремы

Лемма 15. *Пусть Γ — локально компактная топологическая группа, Δ — ее открытая нормальная подгруппа конечного индекса. Если группа Δ является компактно определенной, то группа Γ также компактно определена.*

Доказательство. Пусть $D \subset \Delta$ — компактное определяющее множество. С самого начала можно предполагать, что D содержит единицу. Кроме того, переходя от D к множеству DD^{-1}, можно считать, что $D = D^{-1}$. Нам достаточно построить компактное подмножество $C \subset \Gamma$, порождающее Γ и обладающее тем свойством, что все соотношения в Γ между элементами C являются следствиями соотношений ограниченной длины. Пусть $\{x_i\}_{i=1}^n$ — некоторая система представителей смежных классов Γ/Δ, содержащая единицу. Положим $C = \bigcup_{i=1}^n x_iD$ и построим базисную систему соотношений между элементами из C. Прежде

всего, поскольку $D \subset C$, можно рассмотреть соотношения вида

$$ab = c \tag{2}$$

для $a, b, c \in D$, выполняющиеся в Δ (по условию эти соотношения определяют группу Δ). Далее, для любых двух индексов $i, j = 1, \ldots, n$ существует единственный индекс $k = k(i, j)$ такой, что $E_{ij} = x_k^{-1}((x_iD)(x_jD)) \subset \Delta$. Ясно, что множество E_{ij} компактно. По построению $\Delta = \bigcup_{m=1}^{\infty} D^m$, где $D^m = D \ldots D$, так что в силу теоремы Бэра (см. Бурбаки [2], гл. IX, § 5, п. 3) существует такое $t \geqslant 1$, что множество D^t является открытым в Δ, и поэтому $\Delta = \bigcup_{m=t}^{\infty} D^m$ есть открытое покрытие Δ. Из компактности E_{ij} тогда вытекает, что $E_{ij} \subset D^{l(i,j)}$ для некоторого целого $l(i, j) \geqslant 1$ (отметим, что $D^{k_1} \subset D^{k_2}$ при $k_1 \leqslant k_2$), т. е. $(x_iD)(x_jD) \subset x_kD^{l(i,j)}$. Положим $l = \max_{i, j = 1, \ldots, n} l(i, j)$ и рассмотрим все выполняющиеся в Γ соотношения вида

$$(x_ia)(x_jb) = x_{k(i,j)}d_1 \ldots d_l, \quad i, j = 1, \ldots, n, \tag{3}$$

где $a, b, d_1, \ldots, d_l \in D$. Для завершения доказательства леммы покажем, что соотношения (2), (3) определяют группу Γ. Действительно, пусть N — нормальный делитель в свободной группе $F(C)$, отвечающий соотношениям (2), (3), $H = F(C)/N$ и $\varkappa$: $F(C) \to H$, δ: $H \to \Gamma$ — соответствующие гомоморфизмы. Положим $L = \varkappa(F(D))$. Тогда в L выполняются соотношения (2), и поэтому ограничение $\delta | L$ является изоморфизмом на Δ. Это показывает, что пересечение $\operatorname{Ker} \delta \cap L$ состоит лишь из единицы. С другой стороны, из выполнимости в H соотношений (3), очевидно, вытекает, что любой элемент из H имеет вид x_ky, где $k = 1, \ldots, n$, $y \in L$. Поэтому $[H : L] \leqslant n = [\Gamma : \Delta]$, откуда $[H : L] = [\Gamma : \Delta]$ и $\operatorname{Ker} \delta = (e)$. Лемма доказана.

§ 3.5. Необходимые сведения из теории меры

В настоящем параграфе собраны используемые в дальнейшем результаты из теории интегрирования на локально компактных топологических группах и связанных с ними пространствах. Отметим, что соображения, связанные с интегрированием, выступают на первый план при изучении аналитических аспектов арифметической теории алгебраических групп (например, при определении чисел Тамагавы) и ее приложений к теории автоморфных функций. С другой стороны, при изложении

материала, который мы избрали для включения в настоящую книгу, эти соображения играют вспомогательную роль (тем не менее без них нельзя обойтись в ряде ключевых моментов, например, при доказательстве теоремы о сильной аппроксимации в гл. VII). По этой причине, а также учитывая то обстоятельство, что теория интегрирования сама по себе является весьма обширной, мы не сочли здесь возможным дать сколько-нибудь подробное ее изложение. В результате настоящий параграф содержит лишь напоминание основных определений из теории меры, формулировки необходимых для дальнейшего фактов и разбор некоторых примеров. Систематическое изложение вопросов, связанных с мерой и интегрированием (включая доказательство приводимых ниже утверждений), читатель может найти в книге Бурбаки [3].

Пусть X — локально компактное топологическое пространство. Напомним, что подмножество $B \subset X$ называется *борелевским*, если оно представимо в виде счетного объединения либо пересечения открытых и замкнутых подмножеств в X (иначе говоря, является элементом σ-алгебры подмножеств в X, порожденной открытыми и замкнутыми подмножествами). Ненулевая мера μ на X называется *борелевской*, если все борелевские подмножества являются μ-измеримыми и $\mu(C) < \infty$ для любого компакта $C \subset X$. Предположим теперь, что на X гомеоморфизмами действует некоторая группа Γ. Тогда мера μ называется Γ-инвариантной, если для любого измеримого подмножества $M \subset X$ и любого $\gamma \in \Gamma$ множество $\gamma(M)$ измеримо и $\mu(\gamma(M)) = \mu(M)$. Наиболее важный для нас пример получается в случае, когда рассматривается локально компактная топологическая группа G, действующая на себе посредством левых либо правых сдвигов. В этом случае (ненулевую) инвариантную борелевскую меру на G называют соответственно *левой* или *правой мерой Хаара*.

Теорема 16. *Пусть G — локально компактная группа. Тогда на G существует единственная с точностью до положительного постоянного множителя левая (правая) мера Хаара.*

(Заметим, что если μ — левая мера Хаара на G, то мера $\hat{\mu}$, задаваемая формулой $\hat{\mu}(X) = \mu(X^{-1})$ для всех таких подмножеств $X \subset G$, что X^{-1} μ-измеримо, является правой мерой Хаара на G. Поэтому утверждения теоремы, касающиеся соответственно левой и правой мер Хаара, эквивалентны.)

Вопрос о конструктивном задании меры Хаара в интересующих нас случаях мы рассмотрим несколько позднее, а сейчас перечислим некоторые свойства, которые имеют место в самой общей ситуации.

Предложение 23. *Пусть G — локально компактная группа, μ — (левая) мера Хаара на ней. Тогда*

(i) *G дискретна в том и только том случае, если $\mu(\{e\}) > 0$;*

(ii) *G компактна в том и только том случае, если $\mu(G) < \infty$.* В частности, если G компактна, то существует единственная (левая) мера Хаара μ на G, для которой $\mu(G) = 1$.

Единственность меры Хаара в теореме 16 позволяет связать с каждым автоморфизмом φ топологической группы G некоторое положительное число, называемое *модулем* φ и обозначаемое $\mathrm{mod}_G\,\varphi$. Более точно, зафиксируем некоторую левую меру Хаара μ на G, и для любого подмножества $X \subset G$ такого, что $\varphi(X)$ является μ-измеримым, положим $\nu(X) = \mu(\varphi(X))$. Поскольку φ переводит борелевские множества в борелевские, а компактные — в компактные, то ν также будет левой мерой Хаара на G. Тогда в силу единственности мы должны иметь $\nu = c\mu$, где $c \in \mathbb{R}$, $c > 0$, и по определению полагаем $\mathrm{mod}_G\,\varphi = c$. Легко видеть, что $\mathrm{mod}_G\,\varphi$ на самом деле не зависит от выбора исходной меры Хаара μ. (Пример: если K_v — локально компактное поле, $a \in K_v^*$, то модуль автоморфизма левого сдвига $x \mapsto ax$ аддитивной группы K_v^+ равен значению $\|a\|_v$ нормализованного нормирования, см. § 1.2, п. 1.)

Для $x \in G$ обозначим через $\Delta_G(x)$ модуль соответствующего внутреннего автоморфизма $\varphi = \mathrm{Int}\,x$: $g \mapsto xgx^{-1}$. Возникающая при этом функция Δ_G: $G \to \mathbb{R}^{>0}$ носит название *модуля группы* G и является непрерывным гомоморфизмом. Если $\Delta_G \equiv 1$, то группа G называется *унимодулярной*. На унимодулярной группе G всякая левая мера Хаара μ одновременно является правой мерой Хаара, более того, $\mu(X) = \mu(X^{-1})$ для любого измеримого подмножества $X \subset G$.

Предложение 24. 1) *Любая абелева группа унимодулярна.* 2) *Модуль любого автоморфизма дискретной либо компактной группы равен единице, так что такие группы унимодулярны.*

Рассмотрим теперь вопрос о построении меры Хаара на различных производных теоретико-групповых объектах, исходя из мер Хаара на участвующих в них группах.

Очевидно, что для построения меры Хаара на конечных прямых произведениях достаточно рассмотреть случай двух сомножителей. Итак, пусть $G = G_1 \times G_2$, где G_i — локально компактные группы с мерами Хаара μ_i. Тогда на G существует единственная мера $\mu = \mu_1 \times \mu_2$ такая, что для любых μ_i-измеримых подмножеств $M_i \subset G_i$ множество $M = M_1 \times M_2$ является μ-измеримым и

$$\mu(M) = \mu_1(M_1)\,\mu_2(M_2), \tag{1}$$

причем эта мера μ оказывается мерой Хаара. Более общо, меру-произведение $\mu = \mu_1 \times \mu_2$ можно определить на любом пространстве вида $X = X_1 \times X_2$, где X_i — локально компактные топологические пространства, снабженные мерами μ_i $(i = 1, 2)$, и при этом сохраняется формула (1). Можно переформулировать (1) на языке интегралов по соответствующим мерам. А именно,

пусть f_i — μ_i-интегрируемая функция на X_i $(i=1,2)$ (т. е. существуют интегралы $\int\limits_{X_i} f_i(x_i)\,d\mu_i(x_i)$). Тогда функция f на $X = X_1 \times X_2$, задаваемая формулой $f(x_1, x_2) = f_1(x_1) f_2(x_2)$, является μ-интегрируемой и

$$\int\limits_X f(x_1, x_2)\,d\mu(x_1, x_2) = \int\limits_{X_1} f_1(x_1)\,d\mu_1(x_1) \int\limits_{X_2} f_2(x_2)\,d\mu_2(x_2).$$

Кроме того, для любой интегрируемой функции f на X имеет место формула

$$\int\limits_X f(x_1, x_2)\,d\mu(x_1, x_2) = \int\limits_{X_1}\left(\int\limits_{X_2} f(x_1, x_2)\,d\mu_2(x_2)\right) d\mu_1(x_1) = \\ = \int\limits_{X_2}\left(\int\limits_{X_1} f(x_1, x_2)\,d\mu_1(x_1)\right) d\mu_2(x_2).$$

Отметим, что распространить определение произведения мер на бесконечное число сомножителей, вообще говоря, нельзя, ибо произведение бесконечного числа локально компактных, но не компактных групп не будет локально компактной группой. Здесь приходится использовать другие конструкции. Одной из них является ограниченное топологическое произведение, формализующее построения, использованные при введении аделей (см. § 1.2).

Определение. Пусть $\{X_\lambda\}_{\lambda\in\Lambda}$ — семейство локально компактных топологических пространств, индексированное счетным множеством индексов Λ. Предположим, что для почти всех $\lambda \in \Lambda$ выделены открытые компактные подмножества $K_\lambda \subset X_\lambda$. Рассмотрим пространство X, элементами которого являются семейства $x = \{x_\lambda\}_{\lambda\in\Lambda}$, где $x_\lambda \in X_\lambda$ и $x_\lambda \in K_\lambda$ для почти всех λ. Введем в X топологию, взяв в качестве фундаментальной системы открытых множеств множества вида $\prod U_\lambda$, где $U_\lambda \subset X_\lambda$ открыто для всех λ и $U_\lambda = K_\lambda$ для почти всех λ. Пространство X с таким образом введенной топологией называется *ограниченным топологическим произведением пространств* X_λ по отношению к выделенным подмножествам K_λ.

Укажем на некоторые простые свойства этой конструкции.

Лемма 16. 1) *Для каждого конечного подмножества $S \subset \Lambda$ такого, что для $\lambda \in \Lambda \setminus S$ подпространство K_λ определено, положим $X_S = \prod\limits_{\lambda\in S} X_\lambda \times \prod\limits_{\lambda\in\Lambda\setminus S} K_\lambda$; тогда X_S открыто в X и топология X индуцирует на X_S топологию прямого произведения.*

2) *Каждое пространство X_S локально компактно и $X = \bigcup\limits_S X_S$, где объединение берется по всем конечным подмножествам*

$S \subset \Lambda$ таким, что для $\lambda \in \Lambda \setminus S$ подпространство K_λ определено; следовательно, пространство X локально компактно.

3) *Если $\{G_\lambda\}_{\lambda \in \Lambda}$ — семейство локально компактных топологических групп и для почти всех λ выделены открытые компактные подгруппы $K_\lambda \subset G_\lambda$, то ограниченное топологическое произведение G групп G_λ по отношению к K_λ является локально компактной топологической группой.*

В силу утверждения 3) на группе G существует некоторая мера Хаара μ; покажем, что ее можно построить, исходя из мер Хаара μ_λ на группах G_λ. Для этого вначале предположим, что меры μ_λ нормализованы таким образом, что $\mu_\lambda(K_\lambda) = 1$ для всех тех λ, что определены подгруппы K_λ. Тогда для любого конечного подмножества $S \subset \Lambda$ такого, что для всех $\lambda \in \Lambda \setminus S$ определены подгруппы K_λ, имеется мера μ_S на группе $G_S = \prod_{\lambda \in S} G_\lambda \times \prod_{\lambda \in \Lambda \setminus S} K_\lambda$, которая фактически является «бесконечным» произведением мер μ_λ. Более точно, ее можно определить, например, как произведение $\mu_1 \times \mu_2$, где μ_1 — обычное конечное произведение мер μ_λ на $\prod_{\lambda \in S} G_\lambda$, а μ_2 — мера Хаара на компактной группе $K_S = \prod_{\lambda \in \Lambda \setminus S} K_\lambda$, нормализованная условием $\mu_2(K_S) = 1$. Легко видеть, что если $S_1 \subset S_2$, то $G_{S_1} \subset G_{S_2}$, и ограничение μ_{S_2} на G_{S_1} совпадает с μ_{S_1}. Поэтому, используя представимость G в виде счетного объединения $G = \bigcup_S G_S$ и свойство счетной аддитивности, можно построить искомую меру μ на группе G, продолжающую меры μ_S. Иногда бывает удобно при определении меры μ на G отказаться от условия $\mu_\lambda(K_\lambda) = 1$, а вместо этого потребовать абсолютную сходимость произведения $\Pi\mu_\lambda(K_\lambda)$ по всем λ, для которых определены K_λ. Тогда построенная выше мера μ заменяется на меру $c\mu$, где $c = \Pi\mu_\lambda(K_\lambda)$.

Рассмотрим теперь вопрос о построении инвариантной меры на факторпространстве $X = G/H$, где G — локально компактная топологическая группа, H — ее замкнутая подгруппа (отметим, что понятие инвариантности здесь, естественно, связывается с действием G на X посредством сдвигов).

Теорема 17. *Для того чтобы на факторпространстве $X = G/H$ существовала ненулевая G-инвариантная борелевская мера β, необходимо и достаточно, чтобы ограничение функции Δ_G на H совпадало с Δ_H; если указанная мера β существует, то она определена однозначно с точностью до положительного множителя.*

В частности, если подгруппа H дискретна в G (это основной случай, который будет нас интересовать в дальнейшем), то инвариантная мера на G/H существует в том и только том случае, если группа G унимодулярна. Отметим также, что фраза

«G/H имеет конечную инвариантную меру (или объем)» означает, что инвариантная мера на G/H существует и объем G/H относительно этой меры конечен.

Можно указать связь «фактормеры» β с мерами Хаара μ и ν на группах G и H соответственно. Это лучше всего сделать на языке интегралов от функций по этим мерам. Итак, рассмотрим интегрируемую на G функцию f и, зафиксировав $g \in G$, положим $\varphi(g) = \int\limits_H f(gh)\,d\nu(h)$. Тогда φ является функцией на G, постоянной на классах смежности по H, и поэтому ее можно рассматривать как функцию на $X = G/H$. С учетом этого имеет место следующая формула:

$$\int\limits_X \left(\int\limits_H f(gh)\,d\nu(h) \right) d\beta(gH) = \int\limits_G f(g)\,d\mu(g). \tag{2}$$

В целом определение меры β, доставляемое формулой (2), не является конструктивным, однако в основном для нас случае дискретной подгруппы H можно свести интегрирование по мере β в факторпространстве G/H к интегрированию по подходящим подмножествам в G относительно исходной меры μ (при этом, правда, приходится наложить на G дополнительное условие существования счетной фундаментальной системы окрестностей единицы, однако это требование заведомо выполнено во всех интересующих нас случаях).

Будем говорить, что подмножество $F \subset G$ является *фундаментальной областью относительно* H, есть ограничение на F канонической проекции π: $G \to G/H$ является биекцией между F и G/H). То же самое можно сформулировать в виде следующих двух условий:

$$\begin{aligned} &1) \qquad G = FH, \\ &2) \qquad F \cap Fh = \varnothing \quad \text{для любого} \quad h \in H,\ h \neq e. \end{aligned} \tag{3}$$

В описанной ситуации всегда существует μ-измеримая фундаментальная область $F \subset G$, причем на самом деле ее можно выделить в любом измеримом подмножестве $\Omega \subset G$ со свойством $\pi(\Omega) = G/H$. Из (2) тогда вытекает формула

$$\int\limits_X f(x)\,d\beta(x) = \int\limits_F f(\pi(g))\,d\mu(g), \tag{4}$$

справедливая для любой интегрируемой на X функции f. Иногда бывает удобно использовать более общее определение фундаментальной области, в котором условие 1) в (3) сохраняется, а условие 2) заменяется на следующее:

2′) для любого $h \in H$, $h \neq e$, пересечение $F \cap Fh$ имеет меру 0.

(Типичный пример этой ситуации возникает в случае, когда имеется замкнутое подмножество $F \subset G$, граница которого имеет меру нуль, накрывающее G/H, и такое, что сдвиги F могут иметь лишь граничные общие точки; см. указанный в § 4.2 классический пример фундаментальной области в $SL_2(\mathbb{R})$ относительно $SL_2(\mathbb{Z})$.) Используя счетность H, легко показать, что и при таком более общем толковании фундаментальной области формула (4) сохраняет силу. Полагая $f \equiv 1$ в (4), получим, что $X = G/H$ имеет конечную инвариантную меру в том и только том случае, если существует измеримая фундаментальная область $F \subset G$ относительно H, имеющая конечную меру, и тогда мера любой фундаментальной области также конечна. Используя возможность выделения фундаментальной области в любом измеримом подмножестве, накрывающем X, можно дать переформулировку этого критерия, которая более удобна в приложениях: мера факторпространства X конечна тогда и только тогда, когда оно накрывается множеством конечной меры.

Пример 1. Пусть $G = \mathbb{R}^n$. Тогда обычная мера Лебега на G является одновременно правой и левой мерой Хаара. Если рассмотреть $x \in GL_n(\mathbb{R})$ как топологический автоморфизм G, то из формулы замены переменных в кратных интегралах вытекает, что $\mathrm{mod}_G\, x = |\det x|$. В частности, преобразования из $SL_n(\mathbb{R})$ являются унимодулярными, т. е. сохраняют меру. Пусть теперь $e_1, \ldots, e_n$ — некоторый базис пространства $\mathbb{R}^n$. Обозначим через H решетку $\mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_n$. Тогда H является дискретной подгруппой в $\mathbb{R}^n$, $F = \{t_1e_1 + \ldots + t_ne_n \mid 0 \leqslant t_i < 1\}$ — соответствующей фундаментальной областью, удовлетворяющей условиям 1), 2), а $F' = \{t_1e_1 + \ldots + t_ne_n \mid 0 \leqslant t_i \leqslant 1\}$ — фундаментальной областью, удовлетворяющей условиям 1), 2′).

Приведенный пример является «нетипичным» в том смысле, что обычно построить в явном виде фундаментальную область, удовлетворяющую условиям 1), 2) или 1), 2′), не удается. По этой причине нам придется прибегнуть в гл. 4, 5 к более общей трактовке фундаментальных множеств — так мы будем называть (замкнутые) подмножества $\Phi \subset G$ со следующими свойствами: $G = \Phi H$ и пересечение $\Phi^{-1}\Phi \cap H$ конечно. Естественно, что имея в распоряжении такое фундаментальное множество, мы не можем точно определить объем $X = G/H$, однако в состоянии сделать качественный вывод о его конечности или бесконечности. В самом деле, если мера Φ конечна, то из сделанных выше замечаний вытекает конечность меры X. Обратно, если мера X конечна, то, выделяя измеримую фундаментальную область $F \subset \Phi$ (см. Бурбаки [3]), мы должны получить включение $\Phi \subset \bigcup Fh$, где h пробегает некоторое конечное подмножество в H, и, значит, мера Φ также конечна. Таким образом, мера G/H конечна в том и только том случае, когда

существует фундаментальное подмножество $\Phi \subset G$ конечной меры.

Отметим одно несложное свойство фактормер: пусть $H_1 \subset \subset H_2$ — две замкнутые подгруппы локально компактной группы G и предположим, что на факторпространстве G/H_1 существует конечная G-инвариантная мера; тогда на факторпространстве G/H_2 также существует конечная G-инвариантная мера. Пользуясь этим утверждением, получаем следующую лемму:

Лемма 17. *Пусть $G = G_1 \times G_2$ — прямое произведение двух локально компактных топологических групп, p_i: $G \to G_i$ — соответствующие проекции и $H \subset G$ — такая замкнутая подгруппа, что на пространстве G/H существует конечная инвариантная мера. Предположим, что группа G_1 некомпактна. Тогда группа $p_2(H)$ недискретна и на факторпространстве $G_2/\overline{p_2(H)}$ по ее замыканию существует конечная инвариантная мера.*

Действительно, если допустить, что группа $p_2(H)$ дискретна, то найдется такая окрестность единицы $U \subset G_2$, что $U^{-1}U \cap \cap p_2(H) = \{e\}$. Тогда множество $G_1 \times U$ инъективно проектируется на G/H и поэтому должно иметь конечную меру. Обозначим через μ_i меру Хаара на G_i $(i = 1, 2)$ и положим $\mu = \mu_1 \times \mu_2$. Тогда $\mu(G_1 \times U) = \mu_1(G_1)\mu_2(U)$, и поскольку $\mu_2(U) \neq 0$ в силу открытости U, мера $\mu_1(G_1)$ должна быть конечной. Но в этом случае группа G_1 компактна (предложение 23) — противоречие. Утверждение о существовании конечной инвариантной меры на факторпространстве $G_2/\overline{p_2(H)}$ вытекает из сделанного выше замечания, если применить его к замкнутым подгруппам $H \subset G_1 \times \times \overline{p_2(H)}$ группы G и заметить, что $G_2/\overline{p_2(H)} \simeq G/(G_1 \times \overline{p_2(H)})$.

Перейдем теперь к явному построению меры Хаара в интересующих нас случаях. Прежде всего укажем на результат, который удобно применять к вещественным алгебраическим группам, используя при этом разложение Ивасавы (см. § 3.2).

Предложение 25. *Пусть G — унимодулярная локально компактная топологическая группа, H, A, U — три замкнутые подгруппы в G с левыми мерами Хаара ν, θ и ω соответственно такие, что морфизм-произведение $H \times A \times U \to G$ является гомеоморфизмом. Предположим, что A нормализует U и группы A, U унимодулярны. Тогда $\mu = \rho(a)\nu(h) \times \theta(a) \times \omega(u)$, где $\rho(a) = = \mathrm{mod}_U(\mathrm{Int}\, a|U)$ $(a \in A)$, является левой мерой Хаара на G.*

(Указанная запись меры μ означает, что мера подмножества $E \subset G$ вычисляется по формуле $\mu(E) = \int\limits_E \rho(a)\, d\nu(h)\, d\theta(a)\, d\omega(u)$.)

Другие примеры явного задания мер Хаара мы получим, интегрируя дифференциальные формы. (Нужные нам сведения о дифференциальных формах (правда, в контексте вещественных многообразий) читатель может найти в любой книге по дифференциальной геометрии, например, у Хелгасона [1].)

Пусть X — n-мерное аналитическое многообразие над полным полем K_v, $x_0 \in X$ и $x_1, \ldots, x_n$ — локальные координаты в окрестности точки x_0. Последнее означает, что x_i — такие аналитические функции, что отображение φ: $x \mapsto (x_1(x), \ldots, x_n(x))$ задает аналитический изоморфизм окрестности точки x_0 на область в K_v^n (т. е. φ является отображением, обратным к некоторой параметризации окрестности точки x_0), или, эквивалентно, дифференциал $d_{x_0}\varphi$ осуществляет изоморфизм касательного пространства $T_{x_0}(X)$ на K_v^n. Дифференциальная форма степени n в окрестности точки x_0 записывается в виде выражения $\omega = f(x)\,dx_1 \wedge \ldots \wedge dx_n$, где f — аналитическая в окрестности точки x_0 функция. Если F: $Y \to X$ — аналитическое отображение двух n-мерных многообразий, $y_0 \in Y$ — такая точка, что $F(y_0) = x_0$, $y_1, \ldots, y_n$ — локальные координаты в окрестности точки y_0, причем в координатах F имеет вид $(y_1, \ldots, y_n) \mapsto (F_1(y_1, \ldots, y_n), \ldots, F_n(y_1, \ldots, y_n))$, то под образом дифференциальной формы ω понимают форму $F^*(\omega) = f(F(y))\,dF_1(y_1, \ldots, y_n) \wedge \ldots \wedge dF_n(y_1, \ldots, y_n)$, где, как обычно, $dF_i(y_1, \ldots, y_n) = \sum_{j=1}^{n} \frac{\partial F_i}{\partial y_j}\,dy_j$.

В частности, определено преобразование локальной дифференциальной формы при замене локальных координат. Теперь можно определить n-мерную дифференциальную форму на всем многообразии X как такое семейство n-мерных локальных дифференциальных форм в окрестности каждой точки X, которое согласовано относительно различных локальных координат в окрестности одной и той же точки. Дифференциальная форма ω на многообразии X называется *инвариантной* относительно аналитического автоморфизма F: $X \to X$, если $F^*(\omega) = \omega$.

В наших дальнейших рассуждениях будут в основном участвовать аналитические многообразия, возникающие из алгебраических многообразий, поэтому мы приведем сейчас алгебраические аналоги соответствующих «аналитических» определений. Пусть X — гладкое n-мерное алгебраическое многообразие, определенное над полем K. Под *K-определенной системой локальных параметров* в окрестности точки $x_0 \in X$ мы будем понимать систему из n определенных в точке x_0 K-рациональных функций $x_1, \ldots, x_n$ таких, что дифференциал $d_{x_0}\varphi$ рационального отображения φ: $X \to \mathbb{A}^n$, φ: $x \mapsto (x_1(x), \ldots, x_n(x))$ является изоморфизмом касательных пространств. Тогда n-мерная *рациональная K-определенная дифференциальная форма* в окрестности точки x_0 записывается в виде выражения $\omega = f(x)\,dx_1 \wedge \ldots \wedge dx_n$, где f — определенная в точке x_0 K-рациональная функция на X. Понятия преобразования дифференциальных форм при рациональных отображениях, дифференциальной формы, определенной на всем многообразии, и инвариантной

дифференциальной формы полностью аналогичны приведенным выше определениям. Отметим, что если X определено над полным полем K_v и $x_0 \in X_{K_v}$, то любую K_v-определенную рациональную дифференциальную форму в окрестности x_0 можно рассматривать и как аналитическую дифференциальную форму на $_{K_v}$ в окрестности x_0.

Пусть теперь G — связная K-определенная алгебраическая группа, $n = \dim G$. Тогда известно, что на G существует ненулевая n-мерная K-определенная рациональная дифференциальная форма ω, инвариантная относительно левых сдвигов (т. е. левоинвариантная форма), причем эта форма определена однозначно с точностью до умножения на ненулевой элемент поля K. Приведем некоторые примеры.

Пример 2. Пусть $G = \boldsymbol{GL}_n$. В качестве системы локальных параметров рассмотрим функции x_{ij} $(i, j = 1, \ldots, n)$, сопоставляющие матрице соответствующий ij-й элемент. Пусть $\omega = f(X)\,dx_{11} \wedge \ldots \wedge dx_{nn}$, где $X = (x_{ij})$, — левоинвариантная дифференциальная форма. Зафиксируем $A = (a_{ij}) \in \boldsymbol{GL}_n$. Тогда левый сдвиг λ_A: $X \mapsto AX = X'$ записывается в координатах следующим образом: $x'_{ij} = \sum_k a_{ik}x_{kj}$. Отсюда следует, что λ_A^* переводит форму $f(X')\,dx'_{11} \wedge \ldots \wedge dx'_{nn}$ в форму

$$f(AX)\,d\left(\sum_k a_{1k}x_{k1}\right) \wedge \ldots \wedge d\left(\sum_k a_{nk}x_{kn}\right) = \\ = f(AX)(\det A)^n\,dx_{11} \wedge \ldots \wedge dx_{nn}.$$

Поэтому из условия инвариантности получаем, что $f(X) = f(AX)(\det A)^n$. Полагая $X = E_n$, будем иметь, что $f(A) = c(\det A)^{-n}$, где $c = f(E_n)$, т. е. $\omega = \frac{c\,dx_{11} \wedge \ldots \wedge dx_{nn}}{(\det(x_{ij}))^n}$. В частности, при $n = 1$ получаем $\omega = c\,dx/x$.

Пример 3. Пусть $G = \boldsymbol{SL}_2$. В качестве системы локальных параметров в окрестности единицы возьмем функции x, y, z, сопоставляющие матрице $X = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in G$ соответствующие компоненты; тогда $t = \frac{1 + yz}{x}$. Будем искать левоинвариантную дифференциальную форму в виде $\omega = f(X)\,dx \wedge dy \wedge dz$. Левый сдвиг на матрицу $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ в этих координатах запишется в виде

$$x' = ax + bz,$$
$$y' = ay + b\,\frac{1 + yz}{x},$$
$$z' = cx + dz.$$

Тогда из условия инвариантности мы должны получить

$$f(X')\,dx' \wedge dy' \wedge dz' =$$
$$= f(AX)\,d(ax+bz) \wedge d\left(ay + b\frac{1+yz}{x}\right) \wedge d(cx+dz) =$$
$$= f(X)\,dx \wedge dy \wedge dz,$$

т. е. $f(AX)\dfrac{ax+bz}{x} = f(X)$.

Замечая, что $ax+bz$ совпадает с элементом, стоящим на позиции (1,1) в матрице AX, получаем, что

$$f(AX)(AX)_{11} = f(X)(X)_{11},$$

откуда ω имеет вид

$$\omega = \frac{c}{x}\,dx \wedge dy \wedge dz.$$

Получим теперь выражение для формы $\omega = \dfrac{1}{x}\,dx \wedge dy \wedge dz$ в другой системе координат. А именно, рассмотрим группу $G_{\mathbb{R}} = SL_2(\mathbb{R})$ и воспользуемся глобальной системой координат на $G_{\mathbb{R}}$, которая доставляется разложением Ивасавы (см. § 3.2). Применительно к нашей ситуации разложение Ивасавы утверждает, что любую матрицу из $G_{\mathbb{R}}$ можно однозначно представить в виде произведения трех матриц, которые соответственно имеют вид

$$\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}, \quad \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \quad (\alpha > 0) \quad \text{и} \quad \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}.$$

Возьмем в качестве (аналитических) координат на $G_{\mathbb{R}}$ величины φ, α и u. Тогда прямое вычисление показывает, что $x = \alpha\cos\varphi$, $y = \alpha u\cos\varphi - \alpha^{-1}\sin\varphi$, $z = \alpha\sin\varphi$ и поэтому $\omega = \alpha\, d\varphi \wedge d\alpha \wedge \wedge du$.

Пример 4 (упражнение для читателя). Пусть U_n — группа n-мерных верхних унипотентных матриц. Показать, что дифференциальная форма $\prod\limits_{i<j} dx_{ij}$ является левоинвариантной дифференциальной формой на U_n. Получить обобщение этого результата на произвольную унипотентную группу.

Перейдем теперь к построению меры, отвечающей дифференциальной форме. Пусть снова X — n-мерное аналитическое многообразие над полем K_v, $x_0 \in X$, $x_1, \ldots, x_n$ — система локальных координат в окрестности точки x_0 и $\omega = f(x)\,dx_1 \wedge \ldots \wedge dx_n$ — n-мерная дифференциальная форма, заданная и отличная от нуля в некоторой окрестности x_0. Тогда на этой окрестности можно определить меру $\mu = |f(x)|_v |dx_1|_v \times \ldots \times |dx_n|_v$ (последнее означает, что $\mu(E) = \int\limits_E |f(x)|_v |dx_1|_v \ldots |dx_n|_v$, где $|dx|_v$ — (аддитивная) мера Хаара на K_v, совпадающая с обычной мерой Лебега, если K есть $\mathbb{R}$ либо $\mathbb{C}$, и нор-

мализованная в v-адическом случае таким образом, чтобы мера кольца целых $\mathcal{O}_v$ равнялась единице). Далее показывается, что эта мера не зависит от выбора системы локальных координат (в архимедовом случае это вытекает из формулы замены переменных в определенном интеграле, а в неархимедовом — из ее v-адического аналога, см. Вейль [4]). Наконец, устанавливается, что если ω — n-мерная дифференциальная форма, определенная на всем многообразии и нигде не обращающаяся в нуль, то локальные меры продолжаются до меры на всем многообразии. Полученную таким образом меру мы будем обозначать через ω_v.

Теорема 18. *Пусть G — K_v-определенная алгебраическая группа, $n = \dim G$ и ω — n-мерная K_v-определенная левоинвариантная дифференциальная форма. Тогда мера ω_v является левой мерой Хаара на G_{K_v}. Группа G_{K_v} унимодулярна в том и только том случае, если форма ω является правоинвариантной.*

Из этой теоремы и приведенных выше примеров получаются явные выражения для мер Хаара. Так, на группе $GL_n(K_v)$ мера Хаара задается интегралом $\int \frac{dx_{11} \ldots dx_{nn}}{|\det(x_{ij})|_v^n}$. В частности, применяя это к $n = 1$, получаем, что для l-мерного разложимого тора $S = \{\mathrm{diag}(\alpha_1, \ldots, \alpha_l)\}$ мера Хаара на S_{K_v} определяется как $\int \frac{d\alpha_1 \ldots d\alpha_l}{\alpha_1 \ldots \alpha_l}$. Для группы n-мерных верхних унипотентных матриц $\boldsymbol{U}_n$ соответственно получаем выражение для меры Хаара группы $\boldsymbol{U}_{nK_v}$ в виде интеграла $\int \prod_{i<j} dx_{ij}$. Поэтому если рассмотреть автоморфизм φ группы $\boldsymbol{U}_{nK_v}$, индуцируемый сопряжением при помощи матрицы $s = \mathrm{diag}(\alpha_1, \ldots, \alpha_n)$, то $\mathrm{mod}\,\varphi = \prod_{i<j} |\alpha_i/\alpha_j|_v$. Этот пример очевидным образом обобщается на максимальные унипотентные K_v-определенные подгруппы в любой редуктивной K_v-определенной группе G. Пусть теперь $G = \boldsymbol{SL}_2$. Тогда для группы $SL_2(\mathbb{R})$ получаем следующее выражение для меры Хаара в координатах, доставляемых разложением Ивасавы: $\int \alpha\, d\varphi\, d\alpha\, du$. Поскольку $\frac{d\alpha}{\alpha}$ является мерой Хаара на группе $A = \{\mathrm{diag}(\alpha, \alpha^{-1}) \mid \alpha \in \mathbb{R}^{>0}\}$, этот результат совпадает с выражением для меры Хаара, получаемым из предложения 25. Наконец, чтобы привести пример p-адического интегрирования, вычислим объем $\omega_p(SL_2(\mathbb{Z}_p))$ относительно меры Хаара ω_p на группе $SL_2(\mathbb{Q}_p)$, отвечающей дифференциальной форме $\omega = \frac{1}{x}\, dx \wedge dy \wedge dz$ из примера 3. Для этого

заметим, что $\omega_p(SL_2(\mathbb{Z}_p)) = [SL_2(F_p)]\,\omega_p(SL_2(\mathbb{Z}_p, p))$, и остается вычислить объем конгруэнц-подгруппы $\Gamma = SL_2(\mathbb{Z}_p, p)$. Но функции x, y, z отображают Γ на $p\mathbb{Z}_p \times p\mathbb{Z}_p \times p\mathbb{Z}_p$, причем на Γ имеем $\left|\frac{1}{x}\right|_p = 1$. Поэтому $\omega_p(\Gamma) = \mu_p(p\mathbb{Z}_p)^3$, где μ_p — мера Хаара на $\mathbb{Q}_p$, нормализованная условием $\mu_p(\mathbb{Z}_p) = 1$. Таким образом, окончательно $\omega_p(\Gamma) = p^{-3}$ и $\omega_p(SL_2(\mathbb{Z}_p)) = p^{-3}[SL_2(F_p)] = p^{-3}p(p^2-1) = 1 - 1/p^2$.

В заключение отметим одно вытекающее из теоремы 18

Следствие. *Пусть G — полупростая K_v-определенная алгебраическая группа. Тогда группа G_{K_v} унимодулярна.*

Действительно, пусть ω — левоинвариантная рациональная K_v-определенная дифференциальная форма на G размерности $n = \dim G$. Обозначим через ρ_g правый сдвиг на элемент $g \in G$. Из перестановочности левых и правых сдвигов вытекает, что форма $\rho_g^*(\omega)$ также будет левоинвариантной, так что в силу единственности ω мы должны иметь соотношение $\rho_g^*(\omega) = \chi(g)\,\omega$, где $\chi(g)$ — ненулевая константа. Далее, нетрудно видеть, что соответствие $g \mapsto \chi(g)$ является рациональным характером G, и поэтому $\chi = 1$, ибо G полупроста. Итак, мы показали, что форма ω является одновременно и правоинвариантной, поэтому унимодулярность G_{K_v} непосредственно вытекает из теоремы 18.

АРИФМЕТИЧЕСКИЕ ГРУППЫ И ТЕОРИЯ ПРИВЕДЕНИЯ

Арифметические группы являются одним из основных объектов исследования арифметической теории алгебраических групп. Их свойства мы будем изучать или использовать во всех последующих главах. Цель настоящей главы — изложить теорию приведения для арифметических групп, которая дает конструкцию фундаментального множества в группе вещественных точек $G_{\mathbb{R}}$ алгебраической $\mathbb{Q}$-группы G относительно группы целых точек $G_{\mathbb{Z}}$. Как следствие, получается ряд основополагающих теоретико-групповых фактов об арифметических подгруппах, в частности, их конечная порожденность и определяемость конечным числом соотношений. Кроме того, мы даем критерии, когда факторпространство $G_{\mathbb{R}}/G_{\mathbb{Z}}$ компактно или имеет конечную меру Хаара. Заключительный параграф главы содержит обсуждение одной открытой проблемы о конечных арифметических группах.

§ 4.1. Арифметические группы

Определение. Пусть $G \subset GL_n(\mathbb{C})$ — алгебраическая линейная группа, определенная над полем рациональных чисел $\mathbb{Q}$. Подгруппа $\Gamma \subset G$ называется *арифметической*, если она соизмерима с $G_{\mathbb{Z}}$, т. е. пересечение $\Gamma \cap G_{\mathbb{Z}}$ имеет конечный индекс как в Γ, так и в $G_{\mathbb{Z}}$ *).

Здесь и далее $G_{\mathbb{Z}}$ обозначает пересечение $G \cap GL_n(\mathbb{Z})$. Можно также рассматривать $G_{\mathbb{Z}}$ как совокупность точек G над кольцом $\mathbb{Z}$ как групповой схемы. А именно, рассмотренное в § 2.1, п. 1 вложение $GL_n(\mathbb{C}) \to GL_{n+1}(\mathbb{C})$ отождествляет $GL_n(\mathbb{C})$ с замкнутым по Зарисскому подмножеством в $M_{n+1}(\mathbb{C}) = \mathbb{C}^{(n+1)^2}$. Тогда множество G так же замкнуто в $M_{n+1}(\mathbb{C})$ и $G_{\mathbb{Z}} = G \cap M_{n+1}(\mathbb{Z})$. Этот прием позволит избежать в дальнейшем громоздких обозначений, включающих $(\det a)^{-1}$. Отметим также, что следуя классической традиции, которая берет свое начало из теории целочисленных автоморфизмов квадратичных форм, мы будем иногда называть $G_{\mathbb{Z}}$ *группой единиц* алгебраической группы G.

---

*) Отметим, что понятие соизмеримости имеет смысл для произвольных подгрупп любой абстрактной группы.

Легко видеть (см. предложение 3), что группы целых точек при рациональных морфизмах могут меняться весьма существенно. Поэтому если G задана как алгебраическая группа преобразований векторного пространства V, то для корректного определения группы целых точек $G_{\mathbb{Z}}$ необходимо фиксировать базис $e_1, \ldots, e_n$ пространства $V_{\mathbb{Q}}$ или, эквивалентно, решетку $L = \mathbb{Z}e_1 + \ldots + \mathbb{Z}e_n$, и тогда $G_{\mathbb{Z}}$ реализуется как стабилизатор $G_{\mathbb{Z}}^L = \{g \in G_{\mathbb{Q}} \mid g(L) = L\}$ решетки L в группе $G_{\mathbb{Q}}$. Тем не менее определяемый через группы целых точек класс арифметических подгрупп обладает свойством инвариантности.

Предложение 1. *Пусть φ: $G \to G'$ — определенный над $\mathbb{Q}$ рациональный изоморфизм линейных алгебраических $\mathbb{Q}$-групп. Тогда если Γ — арифметическая подгруппа в G, то $\varphi(\Gamma)$ — арифметическая подгруппа в G'.*

Доказательство. Отметим вначале следующий элементарный теоретико-групповой факт: отношение соизмеримости на классе всех подгрупп произвольной группы G является отношением эквивалентности (в частности, любые арифметические подгруппы соизмеримы). Отсюда следует, что для доказательства предложения достаточно установить соизмеримость $\varphi(G_{\mathbb{Z}})$ и $G'_{\mathbb{Z}}$. Далее, учитывая, что $[G'_{\mathbb{Z}} : G'_{\mathbb{Z}} \cap \varphi(G_{\mathbb{Z}})] = [\varphi^{-1}(G'_{\mathbb{Z}}) : \varphi^{-1}(G'_{\mathbb{Z}}) \cap G_{\mathbb{Z}}]$, где φ^{-1}: $G' \to G$ — обратный рациональный $\mathbb{Q}$-морфизм, мы видим, что наша задача свелась к доказательству конечности индекса $[\varphi(G_{\mathbb{Z}}) : \varphi(G_{\mathbb{Z}}) \cap G'_{\mathbb{Z}}]$ для произвольного $\mathbb{Q}$-изоморфизма φ. Мы укажем подгруппу $H \subset G_{\mathbb{Z}}$ конечного индекса, образ $\varphi(H)$ которой лежит в $G'_{\mathbb{Z}}$; тогда $\varphi(G_{\mathbb{Z}}) \cap G'_{\mathbb{Z}} \supset \varphi(H)$, так что $[\varphi(G_{\mathbb{Z}}) : \varphi(G_{\mathbb{Z}}) \cap G'_{\mathbb{Z}}] \leqslant [\varphi(G_{\mathbb{Z}}) : \varphi(H)] < \infty$ и требуемое доказано. Оказывается, что такая подгруппа H существует для произвольного рационального $\mathbb{Q}$-морфизма (а не только для $\mathbb{Q}$-изоморфизма).

Лемма 1. *Пусть φ: $G \to G'$ — определенный над $\mathbb{Q}$ рациональный морфизм. Тогда существует такая подгруппа $H \subset G^{\mathbb{Z}}$ конечного индекса, что $\varphi(H) \subset G'_{\mathbb{Z}}$.*

Доказательство. Пусть $G \subset GL_n(\mathbb{C})$, $G' \subset GL_m(\mathbb{C})$. Без ограничения общности можно считать, что G и G' замкнуты по Зарисскому в $M_n(\mathbb{C})$ и $M_m(\mathbb{C})$ соответственно. Тогда φ имеет вид $\varphi((x_{ij})) = (\varphi_{kl}(x_{11}, \ldots, x_{nn}))$ $(i, j = 1, \ldots, n;\ k, l = 1, \ldots, m)$, где φ_{kl} — полиномы с рациональными коэффициентами. Введем новые переменные $y_{ij} = x_{ij} - \delta_{ij}$ (δ_{ij} — символ Кронекера) и положим

$$\psi_{kl}(y_{11}, \ldots, y_{nn}) = \varphi(x_{11}, \ldots, x_{nn}) - \delta_{kl}.$$

Поскольку $\varphi(E_n) = E_m$, то $\psi_{kl}(0, \ldots, 0) = 0$ для $k, l = 1, \ldots, m$, т. е. ψ_{kl} — полиномы без свободного члена. Так как коэффициенты ψ_{kl} рациональны, то найдется такое число d, что все по-

линомы $d\psi_{kl}$ станут целочисленными. Обозначим через H конгруэнц-подгруппу $G_{\mathbb{Z}}(d)$ уровня d, т. е. совокупность матриц из $G_{\mathbb{Z}}$, сравнимых с E_n по модулю d. Тогда $H = G_{\mathbb{Z}} \cap GL_n(\mathbb{Z}, d)$, где $GL_n(\mathbb{Z}, d)$ — конгруэнц-подгруппа уровня d в $GL_n(\mathbb{Z})$. Ясно, что $GL_n(\mathbb{Z}, d)$ совпадает с ядром гомоморфизма редукции $GL_n(\mathbb{Z}) \to GL_n(\mathbb{Z}/d\mathbb{Z})$, который сопоставляет каждой целочисленной матрице матрицу, составленную из вычетов соответствующих элементов по модулю d, и поэтому является нормальным делителем конечного индекса, не превосходящего порядок конечной группы $GL_n(\mathbb{Z}/d\mathbb{Z})$. Отсюда следует, что H является нормальным делителем конечного индекса в $G_{\mathbb{Z}}$. С другой стороны, если $h = (h_{ij}) \in H$, то $\varphi_{kl}(h) = \psi_{kl}(h - E_n) + \delta_{kl} \in \mathbb{Z}$, ибо все элементы $h_{ij} - \delta_{ij}$ кратны d. Таким образом, $\varphi(H) \subset G'_{\mathbb{Z}}$ и все доказано.

Следствие 1. *Пусть Γ — арифметическая подгруппа алгебраической $\mathbb{Q}$-группы G. Тогда для любого $g \in G_{\mathbb{Q}}$ группа $g\Gamma g^{-1}$ также арифметическая.*

Следствие 2. *Пусть $G = HN$ — полупрямое произведение ($N \lhd G$), определенное над $\mathbb{Q}$. Тогда подгруппа $H_{\mathbb{Z}}N_{\mathbb{Z}}$ имеет конечный индекс в группе $G_{\mathbb{Z}}$.*

Действительно, пусть φ: $G \to H$ — рациональный $\mathbb{Q}$-определенный морфизм, задаваемый соответствием φ: $g = hn \mapsto h$. Согласно лемме 1 найдется такая подгруппа $M \subset G_{\mathbb{Z}}$ конечного индекса, что $\varphi(M) \subset H_{\mathbb{Z}}$. Тогда для $m \in M$ имеем $m = \varphi(m)\,(\varphi(m)^{-1}m) \in H_{\mathbb{Z}}N_{\mathbb{Z}}$, так что $M \subset H_{\mathbb{Z}}N_{\mathbb{Z}}$, откуда и следует требуемое.

Введенные при доказательстве леммы 1 конгруэнц-подгруппы $GL_n(\mathbb{Z}, d)$ и $G_{\mathbb{Z}}(d)$ играют в арифметической теории алгебраических групп важную роль. Они будут неоднократно встречаться нам в дальнейшем как в качестве естественного технического средства, так и в качестве самостоятельного объекта исследования (см. § 9.5).

Следует обратить внимание, что в определении арифметической подгруппы не предполагается выполненным включение $\Gamma \subset G_{\mathbb{Q}}$. Более того, некоторые важные классы арифметических подгрупп (например максимальные) заведомо не обладают этим свойством. С другой стороны, арифметические подгруппы, содержащиеся в $G_{\mathbb{Q}}$, допускают естественное описание как подгруппы конечного индекса групп целых точек, отвечающих всевозможным реализациям G. А именно, имеет место следующий «глобальный» аналог предложения 1.12.

Предложение 2. *Пусть $G \subset GL_n(\mathbb{C})$ — определенная над $\mathbb{Q}$ алгебраическая группа, $\Gamma \subset G_{\mathbb{Q}}$ — арифметическая подгруппа. Тогда существует решетка $L \subset \mathbb{Q}^n$, инвариантная относительно Γ. При этом индекс Γ в группе $G_{\mathbb{Z}}^L$ конечен.*

Доказательство. Пусть $e_1, \ldots, e_n$ — стандартный базис пространства $\mathbb{Q}^n$; обозначим через M решетку $\mathbb{Z}e_1 + \ldots + \mathbb{Z}e_n$. Так как по условию индекс $[\Gamma : \Gamma \cap G_{\mathbb{Z}}^M]$ конечен, то среди решеток вида $\gamma(M)$, $\gamma \in \Gamma$, имеется лишь конечное число различных. Отсюда следует, что $\mathbb{Z}$-подмодуль $L \subset \mathbb{Q}^n$, порожденный объединением $\bigcup_{\gamma \in \Gamma} \gamma(M)$, будет конечно порожденным, т. е. является решеткой. При этом, очевидно, $\Gamma \subset G_{\mathbb{Z}}^L$. Далее, группа $G_{\mathbb{Z}}^L$ совпадает с группой целых точек относительно произвольного базиса $w_1, \ldots, w_n$ решетки L, а поэтому арифметична в силу предложения 1. Таким образом, $\Gamma \subset G_{\mathbb{Z}}^L$ — две арифметические подгруппы, так что индекс $[G_{\mathbb{Z}}^L : \Gamma]$ обязан быть конечным. Предложение доказано.

Замечание. Используя лемму 1, можно при помощи тех же рассуждений доказать несколько более общий факт: если ρ: $G \to GL(V)$ — определенное над $\mathbb{Q}$ представление алгебраической $\mathbb{Q}$-группы G, $\Gamma \subset G_{\mathbb{Z}}$ — арифметическая подгруппа, то существует решетка $L \subset V_{\mathbb{Q}}$, инвариантная относительно $\rho(\Gamma)$. При этом можно считать, что L содержит наперед заданный вектор $v \in V_{\mathbb{Q}}$. Согласно предложению 2 группы целых точек $G_{\mathbb{Z}}^L$ доставляют в некотором смысле универсальный пример арифметических подгрупп. Естественно задать вопрос: существуют ли арифметические подгруппы, отличные от $G_{\mathbb{Z}}^L$? Оказывается, существуют, и примеры таких подгрупп можно построить на основе анализа доказательства предложения 1. В самом деле, мы показали, что группы вида $\varphi^{-1}(\varphi(G)_{\mathbb{Z}})$, где φ: $G \to GL_m(\mathbb{C})$ — рациональное $\mathbb{Q}$-определенное представление, обязательно содержат некоторую конгруэнц-подгруппу $G_{\mathbb{Z}}(d)$. В то же время имеются примеры подгрупп конечного индекса, например группы $SL_2(\mathbb{Z})$, которые не обладают этим свойством (см. § 9.5). В этой связи любопытно отметить, что сами конгруэнц-подгруппы $G_{\mathbb{Z}}(d)$ реализуются в качестве $G_{\mathbb{Z}}^L$. Более точно, имеет место следующее утверждение, которое будет играть важную роль в гл. VIII.

Предложение 3. *Пусть $G \subset GL_n(\mathbb{C})$ — алгебраическая $\mathbb{Q}$-определенная группа, ρ: $G \to GL_{2n}(\mathbb{C})$ — представление, задаваемое формулой*

$$a \mapsto \begin{pmatrix} a & 0 \\ 0 & E_n \end{pmatrix}. \tag{1}$$

Тогда для любого натурального d существует такая решетка $L(d) \subset \mathbb{Q}^{2n}$, что $G_{\mathbb{Z}}(d) = \rho^{-1}(\rho(G)_{\mathbb{Z}}^{L(d)})$.

Доказательство. Пусть $e_1, \ldots, e_n, f_1, \ldots, f_n$ — базис пространства $\mathbb{Q}^{2n}$, в котором представление ρ задается форму-

лой (1). Обозначим через $L(d)$ решетку с базисом $e_1 + d^{-1}f_1, \ldots, e_n + d^{-1}f_n, f_1, \ldots, f_n$. Тогда если $g = (g_{ij}) \in G$, то

$$\rho(g)(e_j + d^{-1}f_j) = \sum_{i=1}^{n} g_{ij}e_i + d^{-1}f_j =$$

$$= \sum_{i=1}^{n} g_{ij}(e_i + d^{-1}f_i) - \sum_{\substack{i=1 \\ i \neq j}}^{n} d^{-1}g_{ij}f_i + d^{-1}(1 - g_{jj})f_j.$$

Поэтому $\rho(g) \in \rho(G)_{\mathbb{Z}}^{L(d)}$ в том и только том случае, если $g \in G_{\mathbb{Z}}$ и $g_{ij} \equiv \delta_{ij} \pmod d$ для всех $i, j = 1, \ldots, n$. Последнее означает, что $\rho(G)_{\mathbb{Z}}^{L(d)} = \rho(G_{\mathbb{Z}}^{\sim}(d))$, что и требовалось.

Предложение 3 показывает, что группы целых точек действительно подвержены существенным изменениям при рациональных морфизмах. В связи с этим класс арифметических подгрупп выступает как естественный инвариантный класс, их содержащий. Слабую форму его инвариантности (инвариантность при $\mathbb{Q}$-изоморфизмах) мы уже установили. Но оказывается, что его свойства инвариантности сильнее, чем можно было априори ожидать.

Теорема 1. *Пусть φ: $G \to H$ — сюръективный $\mathbb{Q}$-определенный морфизм алгебраических групп. Если Γ — арифметическая подгруппа в G, то $\varphi(\Gamma)$ — арифметическая подгруппа в H.*

В отличие от предложения 1 здесь доказательство не является элементарным, и мы сможем его провести лишь после изложения теории приведения (см. § 4.4). Прежде чем переходить к этой большой теме, укажем еще на ряд теоретико-групповых следствий теории приведения.

Теорема 2. *Пусть Γ — арифметическая подгруппа $\mathbb{Q}$-определенной алгебраической группы G. Тогда Γ является группой с конечным числом образующих и конечным числом определяющих соотношений.*

Теорема 3. *Пусть G — алгебраическая группа, определенная над $\mathbb{Q}$. Тогда конечные подгруппы группы $G_{\mathbb{Z}}$ образуют конечное число классов сопряженности.*

Доказательство теорем 2 и 3 см. в § 4.4. Там же содержится еще ряд результатов об арифметических подгруппах (теорема плотности Бореля, описание подгруппы соизмеримости).

В заключение настоящего параграфа укажем на некоторые обобщения арифметических подгрупп. Определяя их, мы исходили из группы целых точек $G_{\mathbb{Z}}$, отвечающей некоторой матричной реализации $G \subset GL_n(\mathbb{C})$ алгебраической $\mathbb{Q}$-группы G и рассматривали класс всех подгрупп, с ней соизмеримых. Аналогичное определение можно дать применительно к алгебраическим группам, определенным над произвольным полем K, если фиксировано некоторое подкольцо $\mathcal{O} \subset K$, поле частных которого совпадает с K. Анализ доказательства предложения 1

показывает, что получившийся таким образом класс $\mathcal{O}$-арифметических подгрупп обладает свойством инвариантности при K-изоморфизмах, если выполнено следующее условие:

$$\text{для любого } a \in \mathcal{O} \setminus \{0\} \text{ фактор-кольцо } \mathcal{O}/a\mathcal{O} \text{ конечно.} \quad (2)$$

(Отметим, что из предложения 3 вытекает, что условие (2) является необходимым для инвариантности класса $\mathcal{O}$-арифметических подгрупп, например групп $G = GL_n$, SL_n и т. д.) Наиболее типичные примеры колец со свойством (2) доставляют кольца $\mathcal{O}(S)$, состоящие из S-целых элементов некоторого поля алгебраических чисел (см. § 1.2). Соответствующие арифметические подгруппы носят название S-арифметических. Класс S-арифметических подгрупп гораздо шире класса обычных арифметических групп, однако подгруппы, отвечающие $S = V_\infty^K$, в существенной степени сводятся к арифметическим. В самом деле, здесь кольцо S-целых элементов совпадает с кольцом целых алгебраических чисел $\mathcal{O}$ поля K. Поэтому выбрав $\mathbb{Z}$-базис кольца $\mathcal{O}$ и применив к группе G конструкцию ограничения основного поля, мы получим $\mathbb{Q}$-группу $G' = \mathbf{R}_{K/\mathbb{Q}}G$, для которой $G_{\mathcal{O}} \simeq G'_{\mathbb{Z}}$ (см. § 2.1, п. 2). По этой причине при построении теории приведения мы будем рассматривать основной случай арифметических подгрупп $\mathbb{Q}$-определенной группы G. Распространение полученных результатов на общий случай см. в § 4.7.

§ 4.2. Теория приведения (общая схема). Приведение в группе $GL_n(\mathbb{R})$

В основе получения информации о структуре арифметических подгрупп, об их когомологиях и других свойствах лежит топологический подход, использующий реализацию $G_{\mathbb{Z}}$ как дискретной подгруппы группы вещественных точек $G_{\mathbb{R}}$. Этот аспект теории арифметических групп тесно связан с теорией дискретных подгрупп групп Ли, подробному изложению которой посвящена книга Рагунатана [5]. Здесь мы намерены ограничиться рассмотрением круга вопросов, связанных с построением фундаментального множества в $G_{\mathbb{R}}$ относительно $G_{\mathbb{Z}}$ с определенными свойствами конечности. На этом пути мы получим доказательство теорем 1—3 и ряда других результатов. Кроме того, будут указаны условия, необходимые и достаточные для того, чтобы факторпространство $G_{\mathbb{R}}/G_{\mathbb{Z}}$ было компактным (имело конечный объем в мере Хаара).

Указать явную конструкцию фундаментального множества для произвольной алгебраической группы не представляется возможным, поэтому применяется следующий прием. Вначале рассматривается случай групп $G = GL_n(\mathbb{C})$, $SL_n(\mathbb{C})$, где дается явная конструкция, использующая так называемые области Зи-

геля Σ. Возникает разложение $GL_n(\mathbb{R}) = \Sigma GL_n(\mathbb{Z})$, исходя из которого удается получить аналогичное разложение для произвольной подгруппы $G \subset GL_n(\mathbb{C})$. Формальная часть рассуждений сосредоточена в следующем элементарном утверждении.

Лемма 2. *Пусть $G = \Sigma\Gamma$ — разложение абстрактной группы в произведение некоторого подмножества Σ и подгруппы Γ. Пусть, далее, задано правое действие G на некотором множестве X и $H = G(x)$ — стабилизатор точки $x \in X$. Предположим, что для некоторого $a \in G$ пересечение $(xa\Sigma) \cap x\Gamma$ конечно и равно $\{xb_1, \ldots, xb_r\}$, $b_i \in \Gamma$. Тогда $H = \Omega(\Gamma \cap H)$, где $\Omega = \left(\bigcup_{i=1}^{r} a\Sigma b_i^{-1}\right) \cap H$. Если дополнительно Σ удовлетворяет следующему условию: пересечение $\Sigma^{-1}\Sigma \cap g\Gamma h$ конечно для любых g, h из некоторой подгруппы D, $\Gamma \subset D \subset G$, то пересечение $\Omega^{-1}\Omega \cap \cap g(\Gamma \cap H)h$ также конечно для любых $g, h \in D \cap H$.*

Доказательство получается легкой проверкой.

Таким образом, построение фундаментального множества в $G_{\mathbb{R}}$ относительно $G_{\mathbb{Z}}$ сводится к двум задачам: 1) построению фундаментального множества для группы $GL_n(\mathbb{C})$ и 2) реализации конструкций, обеспечивающих выполнение условий леммы 2. В настоящем параграфе мы выполним первый этап этой программы.

В оставшейся части этого параграфа через G будет обозначаться группа $GL_n(\mathbb{R})$, через $\mathbf{K}$, A, U соответственно — подгруппы ортогональных матриц, диагональных матриц с положительными элементами на диагонали и верхних треугольных матриц с единицами на диагонали (унипотентных матриц). Напомним, что согласно предложению 13 о разложении Ивасавы в G морфизм-произведение индуцирует гомеоморфизм $\mathbf{K} \times A \times \times U \to G$. В дальнейшем компоненты разложения Ивасавы элемента $g \in G$ будем обозначать через k_g, a_g и u_g. При этом будем считать, что элементы $a \in A$, $u \in U$ имеют вид

$$a = \operatorname{diag}(a_1, \ldots, a_n), \qquad u = \begin{pmatrix} 1 & & u_{ij} \\ & \ddots & \\ 0 & & 1 \end{pmatrix}.$$

Определение. *Областью Зигеля в G называется множество $\Sigma_{t,v} = \mathbf{K}A_tU_v$ $(t, v > 0)$, где $A_t = \{a \in A \mid a_i \leqslant ta_{i+1}, \quad i = 1, \ldots \ldots, n-1\}$, $U_v = \{u \in U \mid |u_{ij}| \leqslant v$ для всех $1 \leqslant i < j \leqslant n\}$.*

Компоненты в определении области Зигеля подобраны таким образом, что выполняется следующее свойство, которое мы будем неоднократно использовать в дальнейшем.

Лемма 3. *Для любых $t, v > 0$ множество*

$$\{aua^{-1} \mid a \in A_t,\ u \in U_v\}$$

относительно компактно.

Доказательство. Так как $aua^{-1}=\begin{pmatrix}1 & & f_{ij}\\ & \ddots & \\ 0 & & 1\end{pmatrix}$, где $f_{ij}=$ $=a_i/a_j\cdot u_{ij}$, то $|f_{ij}|=|a_i/a_{i+1}\cdot a_{i+1}/a_{i+2}\cdot\ \ldots\ \cdot a_{j-1}/a_j\cdot u_{ij}|\leqslant t^{j-i}v$, так что рассматриваемое множество содержится в U_{sv}, где $s=\max\limits_{1\leqslant i<j\leqslant n}\{t^{j-i}\}$, и требуемое доказано. В дальнейшем мы будем использовать термины «относительно компактный» и «ограниченный» как синонимы.

Положим $\Gamma=GL_n(\mathbb{Z})$. Тогда справедлива

Теорема 4. *При $t\geqslant 2/\sqrt{3}$, $v\geqslant 1/2$ имеет место разложение $G=\Sigma_{t,v}\Gamma$.*

Доказательство. Зафиксируем ортонормированный базис $e_1, \ldots, e_n$ пространства $\mathbb{R}^n$ и будем обозначать через $\|\ \|$ соответствующую евклидову норму. Определим непрерывную функцию Φ: $G\to\mathbb{R}_{>0}$, положив $\Phi(g)=\|ge_1\|$. Пусть $g\in G$. Тогда множество $g\Gamma e_1$ содержится в решетке $g(\mathbb{Z}e_1+\ \ldots\ +\mathbb{Z}e_n)$, и поэтому для любого $d>0$ лишь конечное число элементов $w\in g\Gamma e_1$ удовлетворяет условию $\|w\|\leqslant d$. По этой причине функция Φ достигает на классе $g\Gamma$ своего положительного минимума. Наша цель — показать, что этот минимум достигается на самом деле в некоторой точке множества $\Sigma_0=\Sigma_{2/\sqrt{3},\,1/2}$; тем самым $g\Gamma\cap\Sigma_0\neq\varnothing$, откуда и будет следовать теорема.

Лемма 4. *Если Φ принимает минимальное значение на смежном классе $g\Gamma$ в точке $g=kau$, то*

1) *существует элемент $\bar u\in U_{1/2}$ такой, что $h=ka\bar u\in g\Gamma$ и $\Phi(h)=\Phi(g)$;*

2) *$a_1/a_2\leqslant 2/\sqrt{3}$.*

Доказательство. Покажем, что $U=U_{1/2}(U\cap\Gamma)$. Пусть $u=\begin{pmatrix}1 & & u_{ij}\\ & \ddots & \\ 0 & & 1\end{pmatrix}\in U$. Прямое вычисление показывает, что

$$\begin{pmatrix}1 & u_{12} & \ldots & u_{1n}\\ & \ddots & \ddots & \vdots\\ & & \ddots & u_{n-1n}\\ 0 & & & 1\end{pmatrix}\begin{pmatrix}1 & \alpha_1 & & 0\\ & \ddots & \ddots & \\ & & \ddots & \alpha_{n-1}\\ 0 & & & 1\end{pmatrix}=\begin{pmatrix}1 & u_{12}+\alpha_1 & & *\\ & \ddots & \ddots & \\ & & \ddots & u_{n-1n}+\alpha_{n-1}\\ 0 & & & 1\end{pmatrix}.$$

Поэтому, подбирая подходящие $\alpha_i \in \mathbb{Z}$, можно добиться, чтобы все элементы $u_{12}, \ldots, u_{ii+1}, \ldots, u_{n-1n}$ по модулю не превосходили 1/2. Дальнейшее рассуждение проводится по индукции. Предположим, что все элементы u_{ij}, где $0 < j - i \leqslant l$, удовлетворяют условию $|u_{ij}| \leqslant 1/2$. Вычисляя матричные элементы произведения

$$m = \begin{pmatrix} 1 & u_{12} & \cdots & u_{1n} \\ & 1 & \ddots & \vdots \\ & & \ddots & \vdots \\ & 0 & & u_{n-1n} \\ & & & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & \cdots & \beta_1 & \cdots & 0 \\ & \ddots & & & & \vdots \\ & & \ddots & & & \beta_{n-(l+1)} \\ & & & \ddots & & \vdots \\ & 0 & & & \ddots & 0 \\ & & & & & 1 \end{pmatrix},$$

получим $m_{ij} = u_{ij}$ при $j - i \leqslant l$ и $m_{ij} = u_{ij} + \beta_i$ при $i = 1, \ldots, n-(l+1)$, $j = i + l + 1$. Таким образом, на $(l+1)$-м шаге мы можем удовлетворить условию $|u_{ij}| \leqslant 1/2$ при $0 < j - i \leqslant l + 1$, поэтому на $(n-1)$-м шаге мы получим матрицу из $U_{1/2}$. Тем самым равенство $U = U_{1/2}(U \cap \Gamma)$ доказано. Для доказательства утверждения 1) теперь достаточно выбрать $\bar{u} \in U_{1/2}$ со свойством $u \in \bar{u}(U \cap \Gamma)$ и заметить, что для $h = ka\bar{u}$ выполняется цепочка равенств

$$\Phi(g) = \|ge_1\| = \|ae_1\| = a_1 = \Phi(h), \tag{1}$$

ибо a-компоненты элементов g и h совпадают.

Переходя к доказательству 2), будем считать, что $g = kau$ и $u \in U_{1/2}$. Положим

$$Z = \left(\begin{array}{cc|c} 0 & 1 & \\ 1 & 0 & 0 \\ \hline & 0 & E_{n-2} \end{array}\right) \in T.$$

Тогда по условию $\Phi(gZ) \geqslant \Phi(g)$. Вычисляя $\Phi(gZ)$, получим

$$gZe_1 = ge_2 = k(a_1u_{12}e_1 + a_2e_2),$$

так что

$$\Phi(gZ)^2 = \|a_1u_{12}e_1 + a_2e_2\|^2 = a_1^2u_{12}^2 + a_2^2 \leqslant \frac{1}{4}a_1^2 + a_2^2,$$

ибо $|u_{12}| \leqslant \frac{1}{2}$. Так как в силу (1) имеем $\Phi(g) = a_1$, то $a_1^2 \leqslant \frac{1}{4}a_1^2 + a_2^2$, откуда $a_1 \leqslant \frac{2}{\sqrt{3}}a_2$. Лемма 4 доказана.

Завершим доказательство теоремы. Из леммы 4 вытекает, что требуемое утверждение справедливо для $n = 2$. Проведем

индукцию по n. Пусть $n \geqslant 3$ и Φ достигает минимума на смежном классе $g\Gamma$ в точке $g = kau$. Положим

$$h = bw \in GL_{n-1}(\mathbb{R}), \quad b = \operatorname{diag}(a_2, \ldots, a_n),$$

$$w = \begin{pmatrix} 1 & u_{23} & \ldots & u_{2n} \\ & \ddots & \ddots & \vdots \\ & & \ddots & \vdots \\ & & & u_{n-1\,n} \\ 0 & & & 1 \end{pmatrix}.$$

По предположению индукции существует элемент $c' \in GL_{n-1}(\mathbb{Z})$ со свойством $hc' = k_0'a'u'$, $a' \in A^{(n-1)}_{2/\sqrt{3}}$, $u' \in U^{(n-1)}_{1/2}$ в очевидных обозначениях. Положим

$$c = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & c' & \\ 0 & & & \end{pmatrix} \in \Gamma, \quad \tilde{k}_0 = k \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & k' & \\ 0 & & & \end{pmatrix} \in \boldsymbol{K},$$

$$\tilde{a} = \operatorname{diag}(a_1, a_1', \ldots, a_{n-1}') \in A.$$

Тогда прямое вычисление показывает, что $gc = \tilde{k}\tilde{a}\tilde{u}$ для подходящего $\tilde{u} \in U$. При этом $ce_1 = e_1$, так что $\Phi(gc) = \|gce_1\| = \|ge_1\| = \Phi(g)$ и точка gc также является точкой минимума для Φ на смежном классе $g\Gamma$. Согласно лемме, можно считать, что $\tilde{u} \in U_{1/2}$ и $a_i/a_1' \leqslant 2/\sqrt{3}$. Но по построению $a' \in A^{(n-1)}_{2/\sqrt{3}}$, так что $a_i'/a_{i+1}' \leqslant 2/\sqrt{3}$ для всех $i = 1, \ldots, n-2$. Поэтому $\tilde{a} \in A_{2/\sqrt{3}}$, и теорема доказана.

Следствие. *Положим* $\Sigma^{(1)}_{t,v} = \Sigma_{t,v} \cap SL_n(\mathbb{R})$. *Тогда* $SL_n(\mathbb{R}) = \Sigma^{(1)}_{t,v} SL_n(\mathbb{Z})$ *для* $t \geqslant 2/\sqrt{3}$, $v \geqslant 1/2$. *При этом справедливо равенство* $\Sigma^{(1)}_{t,v} = (\mathbf{K} \cap SL_n(\mathbb{R}))(A_t \cap SL_n(\mathbb{R}))U_v$.

Доказательство. Пусть $g \in SL_n(\mathbb{R})$ и $g = \sigma h$, где $\sigma \in \Sigma_{t,v}$, $h \in GL_n(\mathbb{Z})$. Если $\det h = 1$, то $\sigma \in \Sigma^{(1)}_{t,v}$, и доказывать нечего. В противном случае $\det h = -1$. Тогда для $x = \operatorname{diag}(1, \ldots, 1, -1)$ имеем $xh \in SL_n(\mathbb{Z})$, $\sigma x^{-1} \in \Sigma^{(1)}_{t,v}$, ибо $x \in \mathbf{K}$ и нормализует множества A_t и U_v, так что $g = (\sigma x^{-1})(xh) \in \Sigma^{(1)}_{t,v} SL_n(\mathbb{Z})$. Разложение для $\Sigma^{(1)}_{t,v}$ вытекает из того, что $\det \mathbf{K} = \pm 1$, $\det U = 1$, а $\det A > 0$.

Изучение дискретных групп преобразований обычно начинается с построения соответствующего фундаментального множества. Напомним, что если Γ действует как дискретная группа преобразований пространства X, то фундаментальной областью для Γ называется открытое подмножество $\Omega \subset X$ такое, что

1) $\overline{\Omega}\Gamma = X$, где $\overline{\Omega}$ — замыкание Ω;

2) $\Omega \cap \Omega\gamma = \varnothing$, если $\gamma \neq e$;

(отметим, что иногда используются и другие определения фундаментальной области). Здесь необходимо сделать следующее замечание. В теории приведения мы всюду будем использовать *правое* действие группы Г, а не левое, как это обычно делается. Причина этого заключена в природе доказательства теоремы 4. От этого неудобства можно было бы избавиться, осуществив замену $x \longmapsto x^{-1}$, однако это ухудшило бы вид фундаментального множества.

Из теоремы 4 вытекает, что внутренность $\Sigma^0_{t,v}$ любой области Зигеля при $t > 2/\sqrt{3}$, $v > 1/2$ удовлетворяет условию 1) из определений фундаментальной области для естественного действия группы Г на G правыми сдвигами. Возникает вопрос, не является ли, например, $\Sigma^0_{2/\sqrt{3},1/2}$ фундаментальной областью в полном смысле слова? Ответ оказывается отрицательным, и это лучше всего увидеть в случае группы $SL_2(\mathbb{R})$, воспользовавшись классическими геометрическими соображениями. Прежде всего отметим, что области Зигеля Σ удовлетворяют условию $\mathbf{K}\Sigma = \Sigma$, поэтому без потери общности можно вместо Σ рассматривать ее образ в факторпространстве $X = \mathbf{K}\backslash G$. Для группы $SL_2(\mathbb{R})$ пространство $SO_2(\mathbb{R})\backslash SL_2(\mathbb{R})$ имеет классическую интерпретацию как верхняя полуплоскость комплексной плоскости. В самом деле, обозначив верхнюю полуплоскость через P, определим на ней действие группы $H = SL_2(\mathbb{R})$ формулой

$$zg = \frac{dz+b}{cz+a}, \quad \text{где} \quad z \in P, \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}).$$

Отметим, что это «правое» действие отличается от традиционного «левого» действия $gz = \frac{az+b}{cz+d}$ (см., например, Серр [7], гл. VII) на инволютивный антиавтоморфизм $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^t \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} d & b \\ c & a \end{pmatrix}$. Прямое вычисление показывает, что для мнимой единицы i

$$ig = \frac{ab+cd}{a^2+c^2} + \frac{i}{a^2+c^2}.$$

Отсюда легко следует, что рассматриваемое действие транзитивно и стабилизатор точки i совпадает с $SO_2(\mathbb{R})$, что и дает требуемое отождествление $SO_2(\mathbb{R})\backslash SL_2(\mathbb{R}) \simeq P$. Несложное вычисление показывает также, что образ в P области Зигеля $\Sigma^{(1)}_{t,v}$ есть $\Omega_{t,v} = \{z \in P \mid \operatorname{Im} z \geqslant 1/t, \ |\operatorname{Re} z| \leqslant u\}$. Рассмотрим также область $D = \{z \in P \mid |z| > 1, \ |\operatorname{Re} z| < 1/2\}$. Покажем, что D, фактически, является фундаментальной областью для действия $SL_2(\mathbb{Z})$ на P. Более точно, поскольку матрица $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in SL_2(\mathbb{Z})$ действует на P тривиально, то для соблюдения усло-

вия 2) из определения фундаментальной области нужно от группы $SL_2(\mathbb{Z})$ перейти к группе $\Gamma = PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm e\}$.

Предложение 4. *D является фундаментальной областью для Γ в P.*

Доказательство. Пусть $z \in P$ — произвольная точка. Покажем, что для некоторого $g \in \Gamma$ элемент $zg \in \overline{D} = \{z \in P \mid |z| \geqslant 1,\ |\operatorname{Re} z| \leqslant 1/2\}$. Прямое вычисление показывает, что если g задается матрицей $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, то

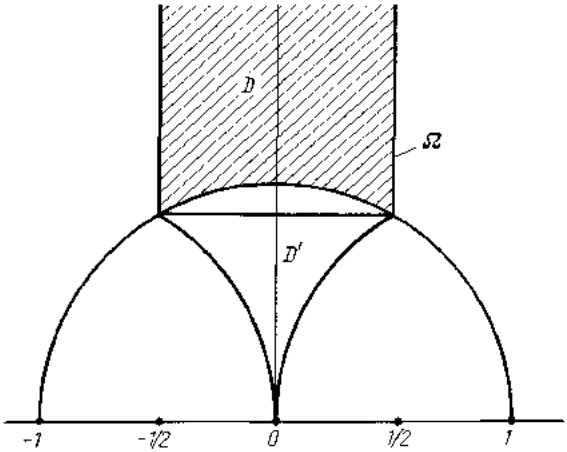
$$\operatorname{Im}(zg) = \frac{\operatorname{Im} z}{|cz + a|^2}. \tag{2}$$

Так как элемент $cz + a$ лежит в решетке $\mathbb{Z} \oplus \mathbb{Z}z$ и, следовательно, $|cz + a|$ ограничен снизу, то найдется матрица $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, для которой $\operatorname{Im}(zg)$ максимально. Кроме того, применяя преобразования, отвечающие матрицам $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, можно добиться, чтобы $|\operatorname{Re}(zg)| \leqslant 1/2$; при этом мнимая часть не изменяется. Покажем, что тогда $z' = zg \in \overline{D}$. По построению $|\operatorname{Re}(z')| \leqslant 1/2$; если же $|z'| < 1$, то для числа $z'' = -1/z'$, которое получается из z' при помощи матрицы $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, имеем $\operatorname{Im} z'' = \frac{\operatorname{Im} z'}{|z''|^2} > \operatorname{Im} z'$, что противоречит выбору z'.

Проверим теперь второе условие из определения фундаментальной области. Пусть $z, zg \in D$, причем g задается матрицей $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Используя симметрию, можно без ограничения общности считать, что $\operatorname{Im}(zg) \geqslant \operatorname{Im}(z)$. Тогда в силу (2) $|cz + a| \leqslant 1$. Так как $\operatorname{Im} z > \sqrt{3}/2$, то $|cz + a| > (\sqrt{3}/2) \cdot |c|$. Заменяя матрицу $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ на $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$, что не изменяет g, можно предполагать, что $c \geqslant 0$. Таким образом, для c имеются лишь следующие возможности: $c = 0, 1$. Если $c = 0$, то $a = \pm 1$, так что g определяется матрицей вида $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. Поэтому $zg = z + b$ и из условия $|\operatorname{Re} z| < 1/2$, $|\operatorname{Re} zg| < 1/2$ получаем, что $b = 0$. Пусть теперь $c = 1$, так что $|z + a| \leqslant 1$. Имеем $|z + a|^2 = |z|^2 + 2a \operatorname{Re} z + a^2$, откуда $2a \operatorname{Re} z + a^2 \leqslant 0$ и $|\operatorname{Re} z| \geqslant \frac{|a|}{2} \geqslant \frac{1}{2}$, если $a \neq 0$, что невозможно. Итак, $a = 0$, и наша матрица имеет вид $\begin{pmatrix} 0 & -1 \\ 1 & d \end{pmatrix}$. Тогда $zg = d - \frac{1}{z}$. Так как $\operatorname{Re}\left(\frac{1}{z}\right) = \frac{\operatorname{Re} z}{|z|^2}$ и $|z|^2 > 1$, то $\left|\operatorname{Re}\left(\frac{1}{z}\right)\right| < |\operatorname{Re} z| < \frac{1}{2}$. Поскольку также $|\operatorname{Re} zg| < \frac{1}{2}$, то $a = 0$ и $zg =$

$= -\frac{1}{z}$. Но $\left|-\frac{1}{z}\right| = |z|^{-1} < 1$ — противоречие. Предложение 4 доказано.

Геометрически области $\Omega = \Omega_{2/\sqrt{3},\,1/2}$ и D (заштриховано) соотносятся следующим образом:



Сравнение Ω и D с учетом предложения 4 позволяет сделать два вывода. Во-первых, границы $t = 2/\sqrt{3}$, $v = 1/2$ в теореме 4 являются наилучшими возможными. Во-вторых, внутренность области Зигеля не является фундаментальной областью, ибо ее сдвиги перекрываются (на рисунке изображен один из сдвигов D', который пересекает Ω). Оказывается, что для областей Зигеля Σ выполняется более слабое условие, суть которого состоит в том, что Σ пересекается лишь с конечным числом своих Γ-сдвигов.

Теорема 5. *Пусть $\Sigma = \Sigma_{t,\,v}$ — область Зигеля в $GL_n(\mathbb{R})$, $x, y \in GL_n(\mathbb{Q})$. Тогда множество $\Sigma^{-1}\Sigma \cap x\Gamma y$ конечно.*

Доказательство будет выведено из одной теоремы Харишчандры, для формулировки которой нам понадобится ряд обозначений. Прежде всего введем функции Φ_i, аналогичные Φ, положив $\Phi_i(g) = \|g(e_1 \wedge \ldots \wedge e_i)\|$, $g \in G$. Здесь $e_1 \wedge \ldots \wedge e_i$ рассматривается как элемент внешней степени $\wedge^i(\mathbb{R}^n)$, на которой $GL_n(\mathbb{R})$ действует естественным образом. Норма вектора берется относительно ортонормированного базиса $e_{j_1} \wedge \ldots \wedge e_{j_i}$ $(j_1 < \ldots < j_i)$ пространства $\wedge^i(\mathbb{R}^n)$. Ясно, что $\Phi_1(g) = \Phi(g)$ и $\Phi_n(g) = |\det g|$. Кроме того, группа $\mathbf{K} = O_n(\mathbb{R})$ действует на $\wedge^i(\mathbb{R}^n)$ ортогональными преобразованиями (упражнение для читателя!); в частности, $\Phi_i(kg) = \Phi_i(g)$ для любого $k \in \mathbf{K}$.

Нам понадобится также ряд обозначений, связанных с разложением Брюа в $G = GL_n(\mathbb{R})$ (см. подробнее § 2.1, п. 10). Пусть D — группа диагональных матриц, W — подгруппа в G, состоящая из матриц, у которых в каждом столбце и каждой строке имеется в точности один ненулевой элемент, равный единице (очевидно, $W \subset \mathbf{K}$). Отметим, что элементы $w = (w_{ij}) \in W$ можно охарактеризовать следующим образом:

$$w_{ij} = \begin{cases} 1, & i = \pi j, \\ 0, & i \neq \pi j, \end{cases}$$

где π — некоторая перестановка индексов $1, \ldots, n$. При этом сопоставление $w \mapsto \pi = \pi(w)$ задает изоморфизм W на симметрическую группу S_n. Произведения WD и $B = DU$ являются полупрямыми, причем первое совпадает с нормализатором D в G, а второе — с группой верхних треугольных матриц. Основной факт (см. теорему 2.5) здесь состоит в том, что $G = \bigcup_{w \in W} UwB$, т. е. $G = UWB = UWDU$. Кроме того, всякий элемент $g \in UwB$ однозначно представим в виде $g = v_g^- w t_g v_g$, где $v_g^- \in U_w = w(w^{-1}Uw \cap U^-)w^{-1}$, U^- — группа нижних унипотентных матриц, $t_g \in D$, $v_g \in U$.

Теорема 6 (Хариш-Чандра). *Пусть $\Sigma = \Sigma_{t,v}$ — область Зигеля в G, $M \subset G$ — такое подмножество, что*

(i) $M = M^{-1}$,

(ii) $\Phi_i(t_m) \geqslant c > 0$ *для всех* $i = 1, \ldots, n$ *и всех* $m \in M$.

Тогда множество $M_\Sigma = \{m \in M \mid \Sigma m \cap \Sigma \neq \varnothing\}$ относительно компактно в G.

Доказательство использует ряд свойств функций Φ_i, которые мы сформулируем в виде следующего утверждения:

Лемма 5. *Пусть $g = k_g a_g u_g = v_g^- w t_g v_g$ — соответственно разложения Ивасавы и Брюа элемента $g \in G$. Тогда*

1) $a_g = a_{w^{-1}v_g^- w t_g}$, *так что*

$$\Phi_i(g) = \Phi_i(w^{-1}v_g^- w) \cdot \Phi_i(t_g) \geqslant \Phi_i(t_g);$$

2) *существует константа $d = d(\Sigma) > 0$ такая, что $\|gx\| \geqslant d\|x\|\Phi_i(g)$ при $g \in \Sigma$, $x \in \wedge^i(\mathbb{R}^n)$ для всех $i = 1, \ldots, n$. В частности, для $g \in \Sigma$, $h \in G$ имеем $\Phi_i(gh) \geqslant d\Phi_i(g)\Phi_i(h)$.*

Доказательство. 1) Имеем

$$\Phi_i(g) = \|g(e_1 \wedge \ldots \wedge e_i)\| = \|a_g(e_1 \wedge \ldots \wedge e_i)\| =$$
$$= \Phi_i(a_g) = a_1 \ldots a_i, \quad a_g = \operatorname{diag}(a_1, \ldots, a_n).$$

Далее, $g = v_g^- w t_g v_g = w w^{-1} v_g^- w t_g v_g = \left(w k_{w^{-1} v_g^- w}\right) \cdot \left(a_{w^{-1} v_g^- w} t_g\right) \times$ $\times \left(t_g^{-1} u_{w^{-1} v_g^- w} t_g v_g\right)$, откуда $a_g = a_{w^{-1} v_g^- w} t_g$. Таким образом, $\Phi_i(g) = \Phi_i(a_g) = \Phi_i\left(a_{w^{-1} v_g^- w}\right) \Phi_i(t_g) = \Phi_i\left(w^{-1} v_g^- w\right) \Phi_i(t_g)$. Наконец, $\Phi_i\left(w^{-1} v_g^- w\right) \geqslant 1$, ибо $w^{-1} v_g^- w \in U^-$, а для любого $u \in U^-$ имеем $u(e_1 \wedge \ldots \wedge e_i) = e_1 \wedge \ldots \wedge e_i + b$, где b — линейная комбинация элементов канонического базиса в $\wedge^i(\mathbb{R}^n)$, отличных от $e_1 \wedge \ldots \wedge e_i$; поэтому $\|u(e_1 \wedge \ldots \wedge e_i)\| \geqslant 1$.

2) Можно считать, что $\|x\| = 1$. Множество таких x компактно, так что компактно и множество

$$\{ux \mid u \in U_v, \|x\| = 1\}.$$

Поэтому существует $\delta_1 > 0$ со свойством: $\|ux\| \geqslant \delta_1$ для всех $u \in U_v$ и всех x таких, что $\|x\| = 1$. Далее, если $f_j = e_{l_1} \wedge \ldots$ $\ldots \wedge e_{l_i}$ $(l_1 < \ldots < l_i)$ — элемент канонического базиса пространства $\wedge^i(\mathbb{R}^n)$, то

$$a_g f_j = a_{l_1} \ldots a_{l_i} f_j = (a_1 \ldots a_i)\left(\frac{a_{l_1}}{a_1} \ldots \frac{a_{l_i}}{a_i}\right) f_j.$$

При этом для любого $k = 1, \ldots, i$ имеем $l_k \geqslant k$, так что если $g \in \Sigma$, то по определению области Зигеля $a_{l_k}/a_k \geqslant t^{k - l_k}$. Таким образом, существует $\delta_2 > 0$ со свойством $\left|\frac{a_{l_1}}{a_1} \ldots \frac{a_{l_i}}{a_i}\right| \geqslant \delta_2$ для любых $l_1 < \ldots < l_i$. Тогда имеем

$$\|gx\| = \|a_g u_g x\| \geqslant \delta_2 \Phi_i(a_g) \|u_g x\| \geqslant \delta_1 \delta_2 \Phi_i(g) = d \Phi_i(g) \|x\|,$$

где $d = \delta_1 \delta_2$, что и требовалось. Применяя доказанное неравенство к вектору $x = h(e_1 \wedge \ldots \wedge e_i)$, мы получим последнее утверждение. Лемма 5 доказана.

Доказательство теоремы Хариш-Чандры базируется на сравнении разложений Ивасавы и Брюа элементов из M_Σ, начало которому положено в лемме 5.

Существенная часть дальнейших рассуждений содержится в следующем утверждении:

Лемма 6. *Если m пробегает M_Σ, то его a-компонента a_m в разложении Ивасавы и компоненты v_m^- и t_m в разложении Брюа образуют относительно компактные множества.*

Доказательство. Пусть $m \in M_\Sigma$, т. е. $xm = y$ для некоторых $x, y \in \Sigma$. Тогда, применяя утверждение 2) предыдущей леммы, будем иметь

$$\Phi_i(x) = \Phi_i((xm) m^{-1}) \geqslant d \Phi_i(xm) \Phi_i(m^{-1}) \geqslant d^2 \Phi_i(x) \Phi_i(m) \Phi_i(m^{-1}),$$

т. е. $\Phi_i(m)\Phi_i(m^{-1}) \leqslant \frac{1}{d^2}$ для всех i и всех $m \in M_\Sigma$. Так как по условию $\Phi_i(m) \geqslant \Phi_i(t_m) \geqslant c$ и $M = M^{-1}$, то функции Φ_i ограничены на M сверху, т. е.

$$0 < c \leqslant \Phi_i(t_m) \leqslant \Phi_i(m) \leqslant b \tag{3}$$

для всех $m \in M_\Sigma$. С другой стороны, как мы видели при доказательстве леммы 5,

$$\Phi_i(m) = \Phi_i(a_m) = a_1 \ldots a_i,$$
$$\Phi_i(t_m) = |t_1 \ldots t_i|,$$

если $a = \operatorname{diag}(a_1, \ldots, a_n)$, $t = \operatorname{diag}(t_1, \ldots, t_n)$. Поэтому из (3) вытекает, что $c \leqslant a_1 \leqslant b$, $cb^{-1} \leqslant a_i \leqslant bc^{-1}$, $i > 1$, т. е. множество $\{a_m \mid m \in M_\Sigma\}$ относительно компактно. Аналогичные рассуждения доказывают относительную компактность множества $\{t_m \mid m \in M_\Sigma\}$. Наконец, согласно утверждению 1) предыдущей леммы, $a_m = a_{w^{-1}v_m^- w} t_m$, так что множество $\{a_{w^{-1}v_m^- w} \mid m \in M_\Sigma \cap \cap UwB\}$ относительно компактно. Поэтому множество элементов вида $(w^{-1}v_m^- w)\, u^{-1}_{w^{-1}v_m^- w} = k_{w^{-1}v_m^- w}\, a_{w^{-1}v_m^- w}$ также относительно компактно. С другой стороны, $w^{-1}v_m^- w \in U^-$, и мы оставляем читателю в качестве упражнения показать, что морфизм-произведение задает гомеоморфизм $U^- \times U$ на замкнутое подмножество в G. Поэтому $w^{-1}v_m^- w$, а следовательно, и v_m^- пробегает относительно компактное множество. Лемма 6 доказана.

Доказательство теоремы Хариш-Чандры. В силу конечности W достаточно установить относительную компактность всех множеств $M_\Sigma \cap UwB$, $w \in W$. Поэтому в дальнейших рассуждениях будем считать w фиксированным; пусть $\pi = \pi_w$ — отвечающая w перестановка индексов $1, \ldots, n$. Возможны два случая:

1) существует $\lambda < n$ со свойством $\pi(\{1, \ldots, \lambda\}) = \{1, \ldots, \lambda\}$,

2) для любого $\lambda < n$ найдется $j \in \{1, \ldots, \lambda\}$, для которого $\pi(j) > \lambda$.

В первом случае w, а следовательно, и весь класс UwB попадает в группу

$$P_\lambda = \left(\begin{array}{c|c} GL_\lambda(\mathbb{C}) & * \\ \hline 0 & GL_{n-\lambda}(\mathbb{C}) \end{array} \right),$$

которых $x, y \in \Sigma$. Без ограничения общности можно считать, что поэтому достаточно установить относительную компактность множества $M_\Sigma \cap P_\lambda$. Далее, если $m \in M_\Sigma \cap P_\lambda$, то $xm = y$ для не-$x \in AU \subset P_\lambda$; тогда и $y \in P_\lambda$. Таким образом,

$$M_\Sigma \cap P_\lambda = \{m \in M \mid (\Sigma \cap P_\lambda)\, m \cap (\Sigma \cap P_\lambda) \neq \varnothing\}.$$

Предположим теперь, что теорема Хариш-Чандры доказана для групп $GL_r(\mathbb{R})$, где $r < n$ (отметим, что случай $n = 1$ тривиален), и разберем случай 1) в размерности n. Разложение Леви (теорема 2.3) группы P_λ имеет вид $P_\lambda = SR$, где

$$S = \left(\begin{array}{c|c} GL_\lambda(\mathbb{C}) & 0 \\ \hline 0 & GL_{n-\lambda}(\mathbb{C}) \end{array} \right)$$

— максимальная редуктивная подгруппа,

$$R = \left(\begin{array}{c|c} E_\lambda & * \\ \hline 0 & E_{n-\lambda} \end{array} \right)$$

— унипотентный радикал. Обозначим через π, π_1 и π_2 естественные проекции P_λ на S, $GL_\lambda(\mathbb{C})$ и $GL_{n-\lambda}(\mathbb{C})$ соответственно. Положим также $\rho(x) = \pi(x)^{-1}x$. Так как группа $\mathbf{K} = O_n(\mathbb{R})$ определяется уравнением ${}^t g = g^{-1}$, то, очевидно,

$$\mathbf{K} \cap P_\lambda = \mathbf{K} \cap S = \left(\begin{array}{c|c} O_\lambda(\mathbb{R}) & 0 \\ \hline 0 & O_{n-\lambda}(\mathbb{R}) \end{array} \right).$$

Далее, $AU \subset P_\lambda$, и поэтому если $g = k_g a_g u_g$ — разложение Ивасавы элемента $g \in P_\lambda$, то $k_g \in P_\lambda$, так что

$$k_g = \left(\begin{array}{c|c} k_{\pi_1(g)} & 0 \\ \hline 0 & k_{\pi_2(g)} \end{array} \right), \qquad a_g = \left(\begin{array}{c|c} a_{\pi_1(g)} & 0 \\ \hline 0 & a_{\pi_2(g)} \end{array} \right).$$

При этом если $a \in A_t^{(n)}$, то $\pi_1(a) \in A_t^{(\lambda)}$, $\pi_2(a) \in A_t^{(n-\lambda)}$. Используя непрерывность π, вследствие чего любое множество вида $\pi(U_u)$ компактно, легко показать, что множества $\pi_1(\Sigma \cap P_\lambda)$ и $\pi_2(\Sigma \cap P_\lambda)$ содержатся в подходящих областях Зигеля $\Sigma_1 \subset GL_\lambda(\mathbb{R})$, $\Sigma_2 \subset GL_{n-\lambda}(\mathbb{R})$. Очевидно также, что $\pi_i(M_\Sigma \cap P_\lambda) \subset (M_i)_{\Sigma_i}$, где $M_i = \pi_i(M \cap P_\lambda)$. Нетрудно видеть, что для любого $g \in P_\lambda$ компонента t_g в разложении Брюа в $GL_n(\mathbb{C})$ имеет вид $t_g = \left(\begin{array}{c|c} t_{\pi_1(g)} & 0 \\ \hline 0 & t_{\pi_2(g)} \end{array} \right)$. Отсюда следует, что множества M_1 и M_2 удовлетворяют условиям теоремы Хариш-Чандры. В самом деле, выполнимость первого условия очевидна. Столь же очевидна выполнимость второго условия для M_1. Покажем, что оно выполняется также и для M_2. Для $m \in M \cap P_\lambda$ имеем $\Phi_\lambda(m) = |\det \pi_1(m)|$, так что $\Phi_\lambda(m^{-1}) = \Phi_\lambda(m)^{-1}$. По условию $\Phi_\lambda(m)^{-1} = \Phi_\lambda(m^{-1}) \geqslant c$. Поэтому остается заметить, что функции $\Phi'_1, \ldots, \Phi'_{n-\lambda}$, построенные аналогично Φ_i, но для группы $GL_{n-\lambda}(\mathbb{R})$, связаны с исходными функциями Φ_i соотношениями $\Phi'_i = \dfrac{\Phi_{\lambda+i}}{\Phi_\lambda}$, откуда и следует требуемое. По предположению

индукции множества $(M_i)_{\Sigma_i}$ относительно компактны, поэтому множество $\pi(M_\Sigma \cap P_\lambda)$ также относительно компактно. Осталось установить относительную компактность множества $\rho(M_\Sigma \cap P_\lambda)$. Итак, пусть $m \in M_\Sigma \cap P_\lambda$, т. е. $xm = y$ для некоторых x, $y \in \Sigma \cap P_\lambda$. Тогда $\pi(x)\rho(x)\pi(m)\rho(m) = \pi(y)\rho(y)$, откуда $\rho(m) = \pi(m)^{-1}\rho(x)^{-1}\pi(m)\rho(y)$. Так как x, y брались из области Зигеля, то $\rho(x)$, $\rho(y)$ пробегают относительно компактные множества. Учитывая, что относительную компактность множества $\{\pi(m) \mid m \in M_\Sigma \cap P_\lambda\}$ мы уже установили, отсюда получаем требуемое утверждение.

Переходим к рассмотрению второго случая. Пусть $xm = y$ для некоторых $m \in M \cap UwB$, x, $y \in \Sigma$, причем можно считать, что $\det x = 1$. Подставляя разложения Ивасавы для x, y и разложение Брюа для m, будем иметь

$$k_y a_y u_y = k_x a_x u_x v_m^- w t_m v_m = (k_x w)\, c w^{-1} a_x w t_m v_m^-, \tag{4}$$

где $c = w^{-1} a_x u_x v_m^- a_x^{-1} w$. Подставляя в (4) разложение Ивасавы элемента c и приравнивая a-компоненты, получим

$$a_y = a_c\,(w^{-1} a_x w)\, a_{t_m}. \tag{5}$$

Заметим здесь, что элемент c, а значит, и его a-компонента a_c пробегает относительно компактное множество. Это следует из того, что u_x и v_m^- пробегают относительно компактные подмножества (u_x — по определению области Зигеля, v_m^- — согласно лемме 6) с учетом леммы 3. Опять в силу леммы 6 множество элементов вида a_{t_m} относительно компактно, поэтому согласно (5) множество $\{a_y^{-1} w^{-1} a_x w\}$ ограничено. Но если $a_x = \operatorname{diag}(a_1, \ldots, a_n)$, $a_y = \operatorname{diag}(b_1, \ldots, b_n)$, то $a_y^{-1} w^{-1} a_x w = \operatorname{diag}(b_1^{-1} a_{\pi(1)}, \ldots, b_n^{-1} a_{\pi(n)})$, где π — отвечающая w перестановка индексов $1, \ldots, n$. Таким образом, найдутся такие $\alpha, \beta > 0$, не зависящие от x, y, что

$$\alpha < b_i^{-1} a_{\pi(i)} < \beta \quad \text{для всех} \quad i = 1, \ldots, n. \tag{6}$$

Из (6) вытекает, что для любых i, j выражения $b_i^{-1} b_j a_{\pi(i)} a_{\pi(j)}^{-1}$ ограничены сверху. Если теперь $i < j$, то ввиду $a_y \in A_t$ выражения $b_i b_j^{-1}$ ограничены сверху, и, следовательно, найдется константа $\gamma > 0$ со свойством

$$a_{\pi(i)} a_{\pi(j)}^{-1} < \gamma \quad \text{для всех} \quad i < j. \tag{7}$$

Покажем теперь, что выражения $a_k^{-1} a_{k+1}$ ограничены для всех $k = 1, \ldots, n-1$. По условию найдется $i \leqslant k$ такое, что $\pi(i) \geqslant k+1$. Очевидно также, что найдется $j > k$ со свойством

$\pi(j) \leqslant k$. Тогда $i < j$ и $\pi(j) \leqslant k < k+1 \leqslant \pi(i)$. Имеем

$$a_{\pi(j)}^{-1} a_{\pi(i)} = (a_{\pi(j)}^{-1} a_{\pi(j)+1}) \cdots (a_{\pi(i)-1}^{-1} a_{\pi(i)}),$$

причем поскольку $a_x \in A_t$, все выражения $a_t^{-1} a_{t+1}$ ограничены снизу. Поэтому из (7) вытекает, что $a_k^{-1} a_{k+1}$ ограничено сверху (равно, как и снизу). Таким образом, элементы $\varphi(a_x)$, где $\varphi\colon A \to \mathbb{R}^* \times \ldots \times \mathbb{R}^*$ — отображение, определяемое формулой

$$\varphi(\operatorname{diag}(a_1, \ldots, a_n)) = (a_1 a_2^{-1}, a_2 a_3^{-1}, \ldots, a_{n-1} a_n^{-1}),$$

заполняют ограниченное подмножество. Так как x выбирался из $SL_n(\mathbb{R})$ и, следовательно, $a_x \in A \cap SL_n(\mathbb{R})$, а ограничение $\varphi|_{A \cap SL_n(\mathbb{R})}$ инъективно и, значит, является собственным, то a_x также заполняют относительный компакт. Возвращаясь к (7), теперь легко вывести и ограниченность a_y. Отсюда следует, что элементы $x = k_x a_x u_x$ и $y = k_y a_y u_y$ лежат в относительно компактных множествах. Поэтому $m = x^{-1} y$ также пробегает относительный компакт. Теорема Хариш-Чандры доказана.

Доказательство теоремы 5. Положим $M = (x\Gamma y) \cup (x\Gamma y)^{-1}$, где $\Gamma = GL_n(\mathbb{Z})$. Множество M, очевидно, замкнуто и дискретно в G; более того, коэффициенты матриц из M имеют ограниченные знаменатели. Поэтому для доказательства конечности соответствующего множества M_Σ (что и утверждает теорема) достаточно установить его относительную компактность. Последнее будет следовать из теоремы Хариш-Чандры, если мы проверим ее условия. Условие 1) выполняется по построению. Для проверки условия 2) сделаем одно предварительное замечание.

Пусть $g = ub$, где $u \in U^-$, $b = \begin{pmatrix} b_{11} & & * \\ & \ddots & \\ 0 & & b_{nn} \end{pmatrix}$. Тогда для любого $i = 1, \ldots, n$ имеем

$$(g_{kl})_{1 \leqslant k, l \leqslant i} = (u_{kl})_{1 \leqslant k, l \leqslant i} (b_{kl})_{1 \leqslant k, l \leqslant i},$$

откуда $\det(g_{kl})_{1 \leqslant k, l \leqslant i} = b_{11} \ldots b_{ii}$. Пусть теперь $m = v_m^- w t_m v_m \in M$. Тогда матрица $w^{-1} m$ имеет ограниченные знаменатели. С другой стороны, $w^{-1} m = w^{-1} v_m^- w t_m v_m$ и $w^{-1} v_m^- w \in U^-$. Из сделанного выше замечания вытекает, что $\Phi_i(t_m) = |t_1 \ldots t_i|$ совпадает с абсолютной величиной главного $(i \times i)$-минора матрицы $w^{-1} m$, т. е. является рациональным числом с ограниченным знаменателем, откуда и следует выполнимость условия 2) в теореме Хариш-Чандры. Теорема 5 полностью доказана.

Подвести итоги настоящего параграфа удобнее всего, используя понятие фундаментального множества, которое является модификацией (в действительности — ослаблением) обсуждавшегося выше понятия фундаментальной области.

Определение. Подмножество $\Omega \subset G$ называется *фундаментальным множеством* для Γ, если

(F0) $\mathbf{K}\Omega = \Omega$, где $\mathbf{K} = O_n(\mathbb{R})$;

(F1) $\Omega\Gamma = G$;

(F2) для любого $g \in GL_n(\mathbb{Q})$ множество $\{\gamma \in \Gamma \mid \Omega g \cap \Omega\gamma \neq \varnothing\}$ конечно.

На первый взгляд, было бы более естественным вместо условия (F2) требовать выполнение более слабого условия:

(F2)′ множество $\{\gamma \in \Gamma \mid \Omega \cap \Omega\gamma \neq \varnothing\}$ конечно.

Однако условие (F2) имеет ряд технических преимуществ. В частности, оно дает возможность, исходя из фундаментального множества Ω для группы Γ, строить фундаментальное множество для любой подгруппы Γ' в $GL_n(\mathbb{Q})$, соизмеримой с Γ. Достаточно положить $\Omega' = \bigcup_{\xi} \Omega\xi$, где ξ пробегает множество представителей $\Gamma'/\Gamma \cap \Gamma'$.

Результаты настоящего параграфа можно переформулировать следующим образом.

Теорема 7. *Область Зигеля $\Sigma_{t,v}$ при $t \geqslant 2/\sqrt{3}$, $v \geqslant 1/2$ является фундаментальным множеством для $\Gamma = GL_n(\mathbb{Z})$ в $GL_n(\mathbb{R})$.*

Следствие. *Для любой арифметической подгруппы $\Gamma \subset GL_n(\mathbb{Q})$ существует открытое фундаментальное множество.*

Легко видеть, что в качестве открытого фундаментального множества для $\Gamma = GL_n(\mathbb{Z})$ можно взять внутренность $\Sigma^0_{t,v}$ области Зигеля для $t > 2/\sqrt{3}$, $v > 1/2$. Используя это множество, можно при помощи указанной выше конструкции построить открытое фундаментальное множество для произвольной арифметической подгруппы.

§ 4.3. Приведение в произвольных группах

В этом параграфе мы реализуем второй шаг намеченной в § 4.2 программы и тем самым установим существование фундаментального множества для произвольной связной алгебраической $\mathbb{Q}$-группы G. При этом, как показывает следующее утверждение, можно ограничиться случаем редуктивной группы.

Лемма 7. 1) *Пусть N — унипотентная $\mathbb{Q}$-определенная группа. Тогда в N найдется такое открытое относительно компактное подмножество U, что $N_{\mathbb{R}} = UN_{\mathbb{Z}}$ и для любых n, $m \in N_{\mathbb{Q}}$ множество $U^{-1}U \cap (nN_{\mathbb{Z}}m)$ конечно.*

2) *Пусть $G = HN$ — разложение Леви связной $\mathbb{Q}$-группы G, где H — максимальная редуктивная $\mathbb{Q}$-определенная подгруппа в G, $N = R_u(G)$ — унипотентный радикал. Предположим, что подмножество $\Sigma \subset H_{\mathbb{R}}$ удовлетворяет условиям:* а) $H_{\mathbb{R}} = \Sigma H_{\mathbb{Z}}$, *и* б) *для любых g, $h \in H_{\mathbb{Q}}$ множество $\Sigma^{-1}\Sigma \cap (gH_{\mathbb{Z}}h)$ конечно. Тогда если $U \subset N_{\mathbb{R}}$ — фундаментальное множество из п. 1), то мно-*

жество $\Omega = \Sigma U$ *удовлетворяет условиям:* α) $G_{\mathbb{R}} = \Omega G_{\mathbb{Z}}$, β) *для любых* $x, y \in G_{\mathbb{Q}}$ *множество* $\Omega^{-1}\Omega \cap (xG_{\mathbb{Z}}y)$ *конечно.*

Доказательство. 1) Достаточно установить компактность факторпространства $N_{\mathbb{R}}/N_{\mathbb{Z}}$. Тогда, используя элементарное топологическое рассуждение (см., например, Бурбаки [2], гл. 3), можно построить открытое относительно компактное множество со свойством $N_{\mathbb{R}} = UN_{\mathbb{Z}}$. При этом конечность пересечения $U^{-1}U \cap (nN_{\mathbb{Z}}m)$ является следствием дискретности и замкнутости $nN_{\mathbb{Z}}m$. Утверждение о компактности $N_{\mathbb{R}}/N_{\mathbb{Z}}$ легко доказывается при помощи индукции по $r = \dim N$ (ср. доказательство леммы 4). Если $r = 1$, то $N \simeq \mathbb{C}^+$, причем при этом изоморфизме $N_{\mathbb{R}} \simeq \mathbb{R}$, $N_{\mathbb{Z}} \simeq a\mathbb{Z}$ $(a \in \mathbb{Q})$ так, что $N_{\mathbb{R}}/N_{\mathbb{Z}} \cong \mathbb{R}/a\mathbb{Z}$ — одномерный компактный тор. Пусть теперь $r > 1$. Так как факторгруппа $N/[N, N]$ является абелевой унипотентной группой, то логарифмическое отображение осуществляет $\mathbb{Q}$-определенный изоморфизм $N/[N, N] \xrightarrow{\sim} \mathbb{C}^l$, $l = \dim N/[N, N]$ (при этом ввиду нильпотентности N заведомо $l \geqslant 1$). Отсюда следует существование $(r-1)$-мерного $\mathbb{Q}$-определенного нормального делителя $M \lhd N$ и одномерной $\mathbb{Q}$-определенной подгруппы $L \subset N$ таких, что $N = LM$ — полупрямое произведение над $\mathbb{Q}$. По предположению индукции пространства $L_{\mathbb{R}}/L_{\mathbb{Z}}$ и $M_{\mathbb{R}}/M_{\mathbb{Z}}$ компактны, и поэтому существуют такие компакты $A \subset L_{\mathbb{R}}$ и $B \subset M_{\mathbb{R}}$, что $L_{\mathbb{R}} = AL_{\mathbb{Z}}$, $M_{\mathbb{R}} = BM_{\mathbb{Z}}$. Покажем, что компакт $C = AB$ удовлетворяет условию $N_{\mathbb{R}} = CN_{\mathbb{Z}}$. В самом деле, пусть $n = lm \in N_{\mathbb{R}} = L_{\mathbb{R}}M_{\mathbb{R}}$. Тогда для подходящих $a \in A$, $z \in L_{\mathbb{Z}}$ имеем равенство $l = az$, а для подходящих $b \in B$, $x \in M_{\mathbb{Z}}$ равенство $zmz^{-1} = bx$. Тогда $n = lm = azm = azmz^{-1}z = abxz$, причем $xz \in N_{\mathbb{Z}}$. Доказательство 1) завершено.

2) Доказательство свойства α) получается при помощи рассуждений, аналогичных тем, которые мы использовали в конце доказательства п. 1). Установим справедливость β). Согласно следствию 2) из предложения 1 группа $H_{\mathbb{Z}}N_{\mathbb{Z}}$ имеет конечный индекс в $G_{\mathbb{Z}}$. Поэтому, рассматривая разложение на правые или левые смежные классы по $H_{\mathbb{Z}}N_{\mathbb{Z}}$, мы видим, что β) эквивалентно конечности пересечения $\Omega^{-1}\Omega \cap (xH_{\mathbb{Z}}N_{\mathbb{Z}}y)$ для произвольных $x, y \in G_{\mathbb{Q}}$. Так как $G_{\mathbb{Q}} = H_{\mathbb{Q}}N_{\mathbb{Q}}$, то $x = ab$, $y = cd$, где $a, c \in H_{\mathbb{Q}}$, $b, d \in N_{\mathbb{Q}}$. Пусть $h \in H_{\mathbb{Z}}$, $n \in N_{\mathbb{Z}}$. Тогда

$$\Sigma Uxhny = \Sigma Uabhncd = \Sigma(ahc)U'g,$$

где $U' = (ahc)^{-1}Uabhc$ — компакт, содержащийся в $N_{\mathbb{R}}$, $g = cnc^{-1}d \in N_{\mathbb{R}}$. Поэтому условие $\Sigma U \cap \Sigma U(xhny) \neq \varnothing$ эквивалентно паре условий:

$$\Sigma \cap \Sigma(ahc) \neq \varnothing, \tag{1}$$

$$U'g \cap U \neq \varnothing. \tag{2}$$

Согласно б) существует лишь конечное число элементов h, удовлетворяющих (1). Конечность числа возможных $n = c^{-1}(gd^{-1})c$ вытекает из (2), относительной компактности множества $(U')^{-1}U$ и того факта, что элемент g в (2) принадлежит замкнутому дискретному множеству $cN_{\mathbb{Z}}c^{-1}d$. Лемма 7 доказана.

Итак, всюду ниже будем предполагать, что группа G редуктивна. Стратегию построения фундаментального множества в этом случае мы уже обсуждали (см. лемму 2): если $G \subset GL_n(\mathbb{C})$, то нужно: 1) определить (правое) действие GL_n на некотором множестве X такое, что стабилизатор подходящей точки $x \in X$ совпадает с G; 2) найти $a \in GL_n(\mathbb{R})$ со свойством: пересечение $xa\Sigma \cap xGL_n(\mathbb{Z})$ конечно, где Σ — область Зигеля в $GL_n(\mathbb{R})$. Тогда мы получим для G фундаментальную область вида $\Omega = \left(\bigcup_{i=1}^{r} a\Sigma b_i^{-1}\right) \cap G$, где $b_i \in GL_n(\mathbb{Z})$. Естественно в качестве X взять векторное пространство V, для которого имеется $\mathbb{Q}$-определенное представление ρ: $GL_n(\mathbb{C}) \to GL(V)$ и вектор $v \in V_{\mathbb{Q}}$ со свойством: $G = \{g \in GL_n(\mathbb{C}) \mid v\rho(g) = v\}$. Существование таких ρ и v обеспечивается усиленной теоремой Шевалле (см. теорему 2.15); при этом орбита $v\rho(GL_n)$ замкнута в топологии Зарисского. Тогда, выбирая $a \in GL_n(\mathbb{R})$ таким образом, чтобы группа $a^{-1}Ga$ была самосопряженной, т. е. инвариантной относительно транспонирования (см. теорему 3.7), мы видим, что конечность нужного нам пересечения вытекает из следующего утверждения:

Предложение 5. *Пусть ρ: $GL_n(\mathbb{C}) \to GL(V)$ — представление, определенное над $\mathbb{Q}$, L — решетка в пространстве $V_{\mathbb{Q}}$. Если $v \in V_{\mathbb{R}}$ — точка, стабилизатор $G = \{g \in GL_n(\mathbb{C}) \mid v\rho(g) = v\}$ которой является самосопряженной группой, а орбита $v\rho(GL_n(\mathbb{C}))$ замкнута в топологии Зарисского, то для любой области Зигеля $\Sigma \subset GL_n(\mathbb{R})$ пересечение $v\rho(\Sigma) \cap L$ конечно.*

Доказательство. Выберем в пространстве $V_{\mathbb{Q}}$ базис, состоящий из собственных векторов относительно $\rho(D_n)$ (D_n — группа диагональных матриц), и определим на $V_{\mathbb{R}}$ евклидову норму (которую будем обозначать через $\|v\|$, $v \in V_{\mathbb{R}}$), считая этот базис ортонормированным. Для характера $\mu \in \mathbf{X}(\rho(D_n))$ пусть $V_\mu = \{v \in V \mid gv = \mu(g)v \quad \forall g \in \rho(D_n)\}$ — весовое пространство веса μ; условимся в дальнейшем рассматривать лишь ненулевые подпространства. Тогда пространства V_{μ_1} и V_{μ_2} для $\mu_1 \neq \mu_2$ являются взаимно ортогональными и $V = \oplus_\mu V_\mu$ — ортогональная прямая сумма. Обозначим через π_μ ортогональную проекцию V на V_μ. Так как V_μ определены над $\mathbb{Q}$, то $\mathbb{Z}$-подмодуль в L, порожденный пересечениями $L \cap V_\mu$, имеет конечный индекс в L. Тогда для подходящего целого m справедливо включение $\pi_\mu(mL) \subset L$, и, следовательно, $\pi_\mu(L) \subset \frac{1}{m} L$ — ре-

шетка в пространстве V_μ. Поэтому существует такая константа $c_1 > 0$, что для всех $w \in L$ и всех μ имеем $\|\pi_\mu(w)\| \geqslant c_1$, если только $\pi_\mu(w) \neq 0$.

Пусть теперь $x = k_x a_x u_x \in GL_n(\mathbb{R})$. Положим $y_x = xa_x^{-1}$, $z_x = xa_x^{-2}$ и будем писать vx вместо $v\rho(x)$. В силу леммы 4.3 множество элементов вида $a_x u_x a_x^{-1}$, где $x \in \Sigma$, относительно компактно. Так как $y_x = k_x a_x u_x a_x^{-1}$, то отсюда следует существование константы $c_2 > 0$ такой, что $\|vy_x\| \leqslant c_2$ для всех $x \in \Sigma$. Покажем, что множество $\Delta = \{vz_x \mid x \in \Sigma,\ vx \in L\}$ также ограничено. Имеем $\pi_\mu(vy_x) = \pi_\mu(vxa_x^{-1}) = \mu(a_x)^{-1}\pi_\mu(vx)$ и аналогично $\pi_\mu(vz_x) = \mu(a_x)^{-2}\pi_\mu(vx)$. Поэтому

$$\|\pi_\mu(vz_x)\| = \frac{\|\pi_\mu(vy_x)\|^2}{\|\pi_\mu(vx)\|} \leqslant \frac{c_2^2}{c_1} = c.$$

Так как орбита $vGL_n(\mathbb{C})$ замкнута в V в топологии Зарисского, то орбита $vGL_n(\mathbb{R})$ замкнута в $V_\mathbb{R}$ в евклидовой топологии (см. доказательство следствия 2 из теоремы 3.6). Поэтому множество

$$W = \{w \in vGL_n(\mathbb{R}) \mid \|\pi_\mu(w)\| \leqslant c \text{ для всех } \mu\}$$

компактно, и, следовательно, найдется такой компакт $U \subset \mathrm{GL}_n(\mathbb{R})$, что $W = vU$. Так как $\Delta \subset W$, то $\{z_x \mid vz_x \in \Delta\} \subset G_\mathbb{R}U$. Но $z_x = k_x a_x u_x a_x^{-2} = k_x a_x^{-1} a_x^2 u_x a_x^{-2}$, поэтому если $x \in \Sigma = \Sigma_{t,b}$, то $a_x^2 \in A_t^2$, так что множество $\{a_x^2 u_x a_x^{-2} \mid x \in \Sigma\}$ относительно компактно. Поэтому $k_x a_x^{-1} \in G_\mathbb{R}U_1$ для подходящего компакта U_1. Применяя преобразование θ: $g \mapsto {}^t g^{-1}$ и учитывая, что k_x — ортогональная, а a_x — диагональная матрица, получим $k_x a_x \in G_\mathbb{R}\theta(U_1)$, так что $x = k_x a_x u_x \in GU_2$, где $U_2 = \theta(U_1)U$ — компактное множество. Таким образом, множество $v\Sigma \cap L$ содержится в vU_2 и, следовательно, является одновременно компактным и дискретным, т. е. конечным. Предложение 5 доказано.

Этим завершается построение фундаментального множества в произвольной редуктивной группе. Сформулируем полученные результаты в виде следующей теоремы.

Теорема 8 (Борель, Хариш-Чандра [2]). *Пусть $G \subset GL_n(\mathbb{C})$ — редуктивная алгебраическая $\mathbb{Q}$-группа, $\Sigma = \Sigma_{t,v}$ $(t \geqslant 2/\sqrt{3},\ v \geqslant 1/2)$ — область Зигеля в группе $GL_n(\mathbb{R})$. Тогда найдутся $a \in GL_n(\mathbb{R})$, $b_1, \ldots, b_r \in GL_n(\mathbb{Z})$ такие, что множество $\Omega = \left(\bigcup_{i=1}^{r} a\Sigma b_i\right) \cap G$ обладает следующими свойствами:*

0) $\mathbf{K}\Omega = \Omega$ *для подходящей максимальной компактной подгруппы* $\mathbf{K}$ *группы* $G_\mathbb{R}$;

1) $\Omega G_\mathbb{Z} = G_\mathbb{R}$;

2) *для любых* $x, y \in G_\mathbb{Q}$ *множество* $\Omega^{-1}\Omega \cap xG_\mathbb{Z}y$ *конечно.*

В доказательстве нуждается лишь пункт 0). Для этого вспомним, что элемент $a \in GL_n(\mathbb{R})$ выбирался исходя из условия: группа $a^{-1}Ga$ должна быть самосопряженной. Но тогда группа $a^{-1}Ga \cap O_n(\mathbb{R})$ является максимальной компактной подгруппой в $a^{-1}G_{\mathbb{R}}a$ (см. предложение 3.10), поэтому $\mathbf{K} = G \cap \cap (aO_n(\mathbb{R})a^{-1})$ — максимальная компактная подгруппа в $G_{\mathbb{R}}$. По построению область Зигеля Σ удовлетворяет условию $O_n(\mathbb{R})\Sigma = \Sigma$, откуда с очевидностью следует 0).

Результаты этого параграфа, как и предыдущего, можно переформулировать более кратко, используя понятие фундаментального множества. Его определение в общей ситуации вполне аналогично определению, которое мы привели в предыдущем параграфе для случая группы $GL_n(\mathbb{C})$, и выглядит следующим образом.

Определение. Пусть G — алгебраическая $\mathbb{Q}$-группа, $\Gamma \subset G_{\mathbb{Q}}$ — ее арифметическая подгруппа. Подмножество $\Omega \subset G_{\mathbb{R}}$ называется *фундаментальным множеством* для Γ, если

(F0) $\mathbf{K}\Omega = \Omega$ — для подходящей максимальной компактной подгруппы $\mathbf{K} \subset G_{\mathbb{R}}$;

(F1) $\Omega\Gamma = G_{\mathbb{R}}$;

(F2) для любых $x, y \in G_{\mathbb{Q}}$ множество $\Omega^{-1}\Omega \cap (xG_{\mathbb{Z}}y)$ конечно.

С учетом леммы 7 и отсутствия компактных подгрупп в унипотентных группах из теоремы 8 получаем

Следствие. *Пусть G — связная $\mathbb{Q}$-группа, $\Gamma \subset G_{\mathbb{Q}}$ — ее арифметическая подгруппа. Тогда в $G_{\mathbb{R}}$ существует открытое фундаментальное множество для Γ.*

Это следствие лежит в основе получения структурных теорем для арифметических групп (см. § 4.4). При этом выявляется важность всех трех условий (F0)—(F2). В частности, условия (F1) и (F2) гарантируют конечную порожденность Γ. Условие (F0) означает, что образ Ω в симметрическом пространстве $X = \mathbf{K}\backslash G_{\mathbb{R}}$ является фундаментальным множеством для индуцированного действия Γ на X, откуда с учетом односвязности X будет вытекать наличие у Γ конечного числа соотношений.

Еще одно применение теории приведения состоит в доказательстве следующей теоремы конечности для орбит арифметических групп.

Теорема 9. *Пусть ρ: $G \to GL(V)$ — определенное над $\mathbb{Q}$ представление редуктивной $\mathbb{Q}$-группы G, $\Gamma \subset G_{\mathbb{Q}}$ — арифметическая подгруппа и $L \subset V_{\mathbb{Q}}$ — Γ-инвариантная решетка. Если $X = v\rho(G)$ — замкнутая в топологии Зарисского орбита группы G, то пересечение $X \cap L$ состоит из конечного числа орбит группы Γ.*

Доказательство. Пусть $G \subset GL_n(\mathbb{C})$. Рассмотрим вначале один частный случай, когда представление ρ получается ограничением $\mathbb{Q}$-определенного представления π: $GL_n(\mathbb{C}) \to GL(V)$, причем орбита $Y = v\pi(GL_n(\mathbb{C}))$ замкнута по Зарисскому, а ста-

билизатор v относительно π лежит в G, т. е. совпадает со стабилизатором H точки v относительно ρ. Множество $X_{\mathbb{R}}$ распадается в объединение конечного числа орбит относительно группы $G_{\mathbb{R}}$ (см. следствие 2 из теоремы 3.6), т. е. $X_{\mathbb{R}} = \bigcup_i v_i\rho(G_{\mathbb{R}})$. При доказательстве теоремы имеет смысл рассматривать только такие i, что $v_i\rho(G_{\mathbb{R}}) \cap L \neq \varnothing$; тогда можно считать, что $v_i \in L$. Таким образом, достаточно показать, что $v\rho(G_{\mathbb{R}}) \cap L$ состоит из конечного числа орбит группы Γ. При этом можно без ограничения общности считать, что $\Gamma = G_{\mathbb{Z}}$, а решетка L инвариантна относительно группы $\rho(GL_n(\mathbb{Z}))$ (см. предложение 2). Согласно теореме 8 найдутся $a \in GL_n(\mathbb{R})$, $b_i \in GL_n(\mathbb{Z})$ такие, что

$$G_{\mathbb{R}} = \left(\left(\bigcup_i (a\Sigma b_i)\right) \cap G\right) G_{\mathbb{Z}} \tag{3}$$

для подходящей области Зигеля $\Sigma \subset GL_n(\mathbb{R})$. При этом в качестве a можно взять произвольный элемент из $GL_n(\mathbb{R})$, для которого группа $a^{-1}Ga$ является самосопряженной. Поэтому в силу теоремы 3.8 можно выбрать a таким образом, что группа $a^{-1}Ha$ также является самосопряженной. Из (3) вытекает, что достаточно установить конечность пересечения $v\rho(a\Sigma b \cap G_{\mathbb{R}}) \cap L$, где $b \in GL_n(\mathbb{Z})$. Так как L инвариантна относительно $\rho(GL_n(\mathbb{Z}))$, то последнее эквивалентно конечности пересечения $w\rho(\Sigma) \cap L$, где $w = v\rho(a)$. Но по построению стабилизатор w, равный $a^{-1}Ha$, является самосопряженным, поэтому требуемая конечность вытекает из предложения 5.

Общий случай сводится к только что рассмотренному. Поскольку орбита X замкнута, то стабилизатор H точки v в G является редуктивной группой. Поэтому согласно усиленной теореме Шевалле (теорема 2.15) найдутся $\mathbb{Q}$-определенное представление π: $GL_n(\mathbb{C}) \to GL(W)$ и точка $w \in W_{\mathbb{Q}}$, стабилизатор которой относительно π совпадает с H, а орбита $Y = w\pi(GL_n(\mathbb{C}))$ замкнута по Зарисскому. При этом из предложения 2 вытекает, что w содержится в $\rho(GL_n(\mathbb{Z}))$-инвариантной решетке $M \subset W_{\mathbb{Q}}$. Орбита $X' = w\pi(G)$ также замкнута, ибо факторотображение π: $GL_n(\mathbb{C}) \to Y$, $\pi(g) = wg$ открыто. Таким образом, множество $X' \cap M$ является объединением конечного числа орбит группы Γ. Более того, переходя от решетки M к решетке $\frac{1}{d}M$ $(d \in \mathbb{Z})$, которая также удовлетворяет требованию $\rho(GL_n(\mathbb{Z}))$-инвариантности, мы видим, что для любого $d \in \mathbb{Z}$ множество $X' \cap \left(\frac{1}{d}M\right)$ является объединением конечного числа орбит группы Γ. Осталось перейти от орбиты X' к орбите X. Для этого заметим, что X и X' являются различными реализациями однородного пространства G/H, т. е. существует $\mathbb{Q}$-определенный G-эквивариантный изоморфизм φ: $X \to X'$. Так как X замкнуто в V, то

относительно координат, определяемых базисами решеток L и M соответственно, изоморфизм φ задается полиномами $P_i(x_1, \ldots, x_r)$, $1 \leqslant i \leqslant s$, с рациональными коэффициентами. Тогда если d — общий знаменатель этих коэффициентов, то $\varphi(X \cap L) \subset X' \cap \left(\frac{1}{d} M\right)$, поэтому из конечности числа орбит группы $G_{\mathbb{Z}}$ в $X' \cap \left(\frac{1}{d} M\right)$ и G-эквивариантности φ вытекает конечность числа орбит $G_{\mathbb{Z}}$ в $X \cap L$. Теорема 9 доказана.

В заключение этого параграфа приведем одну переформулировку условия (F2) из определения фундаментального множества, которая будет использована нами в следующей главе при построении теории приведения для групп аделей.

Лемма 8. *Условие* (F2) *для множества* $\Omega \subset G_{\mathbb{R}}$ *эквивалентно следующему*:

(F2)′ *для любых* x, $y \in G_{\mathbb{Q}}$ *и любого* $r \in \mathbb{Z}$ *пересечение* $\Omega^{-1}\Omega \cap xG_r y$, *где* $G_r = \{g \in G_{\mathbb{Q}} \mid rg,\ rg^{-1} \in M_n(\mathbb{Z})\}$, *конечно.*

В самом деле, для доказательства импликации (F2) $\Rightarrow$ (F2)′ достаточно показать, что множество G_r содержится в объединении конечного числа смежных классов по группе $G_{\mathbb{Z}}$. Но если $g \in G_r$, то для решетки $g(\mathbb{Z}^n)$ имеют место включения

$$r\mathbb{Z}^n \subset g(\mathbb{Z}^n) \subset r^{-1}\mathbb{Z}^n.$$

Так как число решеток, промежуточных между $r\mathbb{Z}^n$ и $r^{-1}\mathbb{Z}^n$, конечно, то для решеток вида $g(\mathbb{Z}^n)$, $g \in G_r$, имеется лишь конечное число возможностей. Заметив, что из $g(\mathbb{Z}^n) = h(\mathbb{Z}^n)$ следует, что $h^{-1}g \in G_{\mathbb{Z}}$, мы и получаем для G_r требуемое включение $G_r \subset \bigcup_i g_i G_{\mathbb{Z}}$, где система представителей g_i выбрана таким образом, чтобы решетки $g_i(\mathbb{Z}^n)$ пробегали все возможные промежуточные решетки между $r\mathbb{Z}^n$ и $r^{-1}\mathbb{Z}^n$ вида $g(\mathbb{Z}^n)$, $g \in G_r$. Обратная импликация (F2)′ $\Rightarrow$ (F2) очевидна.

§ 4.4. Теоретико-групповые свойства арифметических групп

В этом параграфе мы установим справедливость основополагающих фактов из § 4.1 об абстрактных свойствах арифметических групп. Изящество и относительную краткость их доказательств можно рассматривать как своеобразную компенсацию за усилия, потраченные на построение теории приведения.

Теорема 2. *Пусть* Γ — *арифметическая подгруппа* $\mathbb{Q}$-*определенной алгебраической группы* G. *Тогда* Γ *является группой с конечным числом образующих и конечным числом определяющих соотношений.*

Доказательство. Для доказательства конечной определенности Γ достаточно установить конечную представимость ее подгруппы конечного индекса, поэтому можно предполагать, что G

связна и $\Gamma \subset G_{\mathbf{R}}$. Мы будем работать с пространством $X = \mathbf{K}\backslash G_{\mathbf{R}}$, где $\mathbf{K}$ — максимальная компактная подгруппа в $G_{\mathbf{R}}$. Согласно предложению 3.10 пространство X связно и односвязно. Если Σ — открытое фундаментальное множество для Γ в $G_{\mathbf{R}}$ (см. § 4.3, следствие из теоремы 8), то в силу условия $\mathbf{K}\Sigma = \Sigma$ образ Σ в X, который мы обозначим через Ω, удовлетворяет следующим двум условиям:

(i) $\Omega\Gamma = X$;

(ii) множество $\Delta = \{\delta \in \Gamma \mid \Omega\delta \cap \Omega \neq \varnothing\}$ конечно.

(Мы рассматриваем естественное действие Γ на X правыми сдвигами.) Мы покажем, что конечная определенность Γ является автоматическим следствием связности, локальной связности и односвязности X, открытости Ω и условий (i), (ii). Поэтому тот же результат имеет место для произвольной группы преобразований любого топологического пространства X, если выполняются указанные предположения (отметим, что Бер [1] доказывает это при несколько более слабых предположениях, а именно, вместо открытости Ω требуется, чтобы Ω лежало во внутренности множества $\Omega\Delta$).

Лемма 9. Δ — *система образующих для* Γ.

Доказательство. Пусть Γ_0 — подгруппа, порожденная Δ. Тогда из (i) вытекает, что $X = (\Omega\Gamma_0) \cup (\Omega(\Gamma \setminus \Gamma_0))$. При этом если $\Omega\gamma \cap \Omega\delta \neq \varnothing$, где $\gamma \in \Gamma_0$, то $\delta\gamma^{-1} \in \Delta$, следовательно, $\delta \in \Gamma_0$. Это рассуждение показывает, что множества $\Omega\Gamma_0$ и $\Omega(\Gamma \setminus \Gamma_0)$ не пересекаются. Так как оба они являются открытыми, а пространство X — связным, то в действительности $\Omega(\Gamma \setminus \Gamma_0) = \varnothing$, т. е. $\Gamma = \Gamma_0$. Лемма доказана.

Перейдем к построению множества определяющих соотношений для Γ. Обозначим через F свободную группу, построенную на множестве $\bar{\Delta}$, элементы которого находятся во взаимно однозначном соответствии с элементами Δ относительно биекции $\bar{\delta} \mapsto \delta$, φ: $F \to \Gamma$ — определяемый этой биекцией гомоморфизм. Часть соотношений для Γ составляют так называемые локальные соотношения, т. е. соотношения вида

$$\bar{\delta}_1\bar{\delta}_2\,(\overline{\delta_1\delta_2})^{-1} = e, \tag{1}$$

где δ_1, δ_2 пробегают совокупность таких элементов из Δ, что $\delta_1\delta_2 \in \Delta$. Для того чтобы понять их роль, обозначим через L нормальный делитель в F, порожденный левыми частями локальных соотношений. Ясно, что $\varphi(\bar{\delta}_1\bar{\delta}_2(\overline{\delta_1\delta_2})^{-1}) = 1$, так что $\varphi(L) = 1$. Пусть N — нормальный делитель в F, содержащий L и содержащийся в $K = \operatorname{Ker}\varphi$. Рассмотрим факторгруппу $H = F/N$ и естественные гомоморфизмы σ: $F \to H$, θ: $H \to \Gamma$ так, что $\theta \circ \sigma = \varphi$. Далее, наделив H дискретной топологией, введем пространство S, которое является факторпространством

произведения $\Omega \times H$ относительно следующего отношения:

$(x_1, h_1) \sim (x_2, h_2)$, если существует такой $\delta \in \Delta$,

$$\text{что } x_2 = x_1\delta, \ h_1 = \sigma(\bar{\delta}) h_2.$$

Оказывается, что соотношения (1) как раз и обеспечивают тот факт, что $\sim$ является отношением эквивалентности, и требуемая факторизация возможна. В самом деле, рефлексивность $\sim$ очевидна ($1 \in \Delta$), симметричность является следствием того обстоятельства, что вместе с любым δ множество Δ содержит также δ^{-1} (ибо $\Omega\delta \cap \Omega \neq \varnothing \Leftrightarrow \Omega \cap \Omega\delta^{-1} \neq \varnothing$), причем $\sigma(\bar{\delta})^{-1} = \sigma(\bar{\delta}^{-1})$ в силу локальных соотношений. Докажем транзитивность $\sim$. Если $(x_1, h_1) \sim (x_2, h_2)$ и $(x_2, h_2) \sim (x_3, h_3)$, то найдутся такие $\delta_1, \delta_2 \in \Delta$, что

$$x_2 = x_1\delta_1, \quad h_1 = \sigma(\bar{\delta}_1) h_2,$$
$$x_3 = x_2\delta_2, \quad h_2 = \sigma(\bar{\delta}_2) h_3.$$

Тогда $x_3 = x_1\delta_1\delta_2$, так что $\delta_1\delta_2 \in \Delta$ и $h_1 = \sigma(\bar{\delta}_1)\sigma(\bar{\delta}_2) h_3 = \sigma(\overline{\delta_1\delta_2}) h_3$ в силу локальных соотношений.

Обозначим через α: $\Omega \times H \to S$ соответствующее фактор-отображение, а через β: $\Omega \times \Gamma \to X$ — отображение-произведение. Если $(x_1, h_1) \sim (x_2, h_2)$, то $x_2 = x_1\delta$, $h_1 = \sigma(\bar{\delta}) h_2$ для некоторого $\delta \in \Delta$, следовательно,

$$\beta(x_1, \theta(h_1)) = x_1\theta(h_1) = (x_1\delta)\theta(\sigma(\bar{\delta})^{-1} h_1) = x_2\theta(h_2) = \beta(x_2, \theta(h_2)),$$

так что существует единственное непрерывное отображение p: $S \to X$, превращающее следующую диаграмму в коммутативную:

$$\begin{tikzcd} \Omega \times H \arrow[r, "(\mathrm{id}, \theta)"] \arrow[d, "\alpha"] & \Omega \times \Gamma \arrow[d, "\beta"] \\ S \arrow[r, "p"] & X \end{tikzcd} \tag{2}$$

Лемма 10. *Отображение p является накрытием, кратность которого равна* $[\operatorname{Ker}\theta]$.

Доказательство. Положим $\Psi = \alpha(\Omega \times \{e\})$. Тогда прообраз

$$\alpha^{-1}(\Psi) = \bigcup_{\delta \in \Delta} (\Omega \cap \Omega\delta, \ \sigma(\bar{\delta})^{-1})$$

является открытым подмножеством в $\Omega \times H$, следовательно, Ψ открыто в S. Ограничение $p|_\Psi$ инъективно и осуществляет гомеоморфизм $\Psi \xrightarrow{\sim} \Omega$. В самом деле, если $p(\alpha(x_1, e)) = p(\alpha(x_2, e))$, то из коммутативности (2) получаем $x_1 = x_2$. Покажем, что

$$p^{-1}(\Omega) = \bigcup_h \Psi h,$$

где объединение берется по $h \in \operatorname{Ker}\theta$, причем сдвиги Ψh попарно не пересекаются. (Здесь и ниже мы рассматриваем индуцированное действие H на S; отметим в связи с этим полезное соотношение $p(xh) = p(x)\theta(h)$). Если $p(\alpha(x, h)) = y \in \Omega$, то $x\theta(h) = y \in \Omega$. Следовательно, $\theta(h) = \delta \in \Delta$, т. е. $g = \sigma(\bar{\delta})^{-1}h \in \operatorname{Ker}\theta$. Но тогда по построению $(x, h) \sim (y, g)$, что и требовалось. Наконец, если $\alpha(x, e) = \alpha(y, h)$, где $h \in \operatorname{Ker}\theta$, то $h \in \Delta$, и так как ограничение $\varphi|_{\Delta}$ инъективно, то $h = e$. Лемма доказана.

Если Ω связно, то пространство S также связно. Действительно, $S = \bigcup_{h \in H} \Psi h$, и поэтому ввиду связности Ψ достаточно показать, что любой сдвиг Ψh соединяется с Ψ цепочкой $\Psi_0 = \Psi$, $\Psi_1 = \Psi h_1, \ldots, \Psi_m = \Psi h_m$, $h_m = h$ попарно перекрывающихся сдвигов. Для $h = \sigma(\bar{\delta}_1 \ldots \bar{\delta}_d)$ достаточно положить $h_1 = \sigma(\bar{\delta}_d)$, $h_2 = \sigma(\bar{\delta}_{d-1}\bar{\delta}_d), \ldots, h_{m-1} = \sigma(\bar{\delta}_2 \ldots \bar{\delta}_d)$, $h_m = \sigma(\bar{\delta}_1 \ldots \bar{\delta}_d)$. Из односвязности X тогда вытекает биективность p, следовательно, и тривиальность $\operatorname{Ker}\theta$, построенных для $N = L$. Таким образом, если фундаментальное множество Ω связано, то для определимости Γ достаточно локальных соотношений.

В общем случае приходится работать со связными компонентами Ω, множество которых мы обозначим через $\{\Omega_i\}_{i \in I}$. Отметим, что в силу локальной связности X и открытости Ω все Ω_i также открыты в X. Зафиксируем одну компоненту $X^0 = \Omega_0$ и обозначим через $X^{(1)}$ объединение $\bigcup_{i, \gamma} \Omega_i\gamma$ по парам $(i, \gamma) \in I \times \Gamma$ таким, что $\Omega_i\gamma \cap \Omega_0 \neq \varnothing$. Пусть множества $X^{(1)}, \ldots, X^{(k)}$ уже построены. Положим тогда $X^{(k+1)} = \bigcup_{i, \gamma} \Omega_i\gamma$, где объединение берется по таким парам, что $\Omega_i\gamma \cap X^{(k)} \neq \varnothing$. Множество $X' = \bigcup_{k=0}^{\infty} X^{(k)}$, очевидно, открыто в X. Его дополнение является объединением множества вида $\Omega_i\gamma$, и поэтому также открыто. Действительно,

$$X = \Omega\Gamma = \bigcup_{\substack{i \in I \\ \gamma \in \Gamma}} \Omega_i\gamma,$$

при этом, если $\Omega_{i_1}\gamma_1 \cap \Omega_{i_2}\gamma_2 \neq \varnothing$, где $\Omega_{i_1}\gamma_1 \subset X^{(k)}$, то $\Omega_{i_2}\gamma_2 \subset X^{(k+1)} \subset X'$. Из связности X вытекает, что $X' = X$, т. е. любой сдвиг $\Omega_i\gamma$ можно соединить с Ω_0 цепочкой попарно перекрывающихся сдвигов связных компонент Ω. Рассмотрим, в частности, $\Omega_0\delta$, $\delta \in \Delta$. Тогда найдется последовательность $\{\Omega_{i_j}\gamma_j\}_{j=0}^{m}$ такая, что $i_0 = i_m = 0$, $\gamma_0 = 1$, $\gamma_m = \delta$ и $\Omega_{i_j}\gamma_j \cap$

$\bigcap \Omega_{i_{j+1}}\gamma_{j+1} \neq \varnothing$ для всех $j=0, \ldots, m-1$. Построим по индукции такие элементы $\omega_j \in F$, что $\varphi(\omega_j)=\gamma_j$ для всех $j=0, \ldots, m$. Для этого положим $\omega_0=e$. Если элементы $\omega_0, \ldots, \omega_k$ уже построены, то положим $\omega_{k-1}=\bar{\delta}_k\omega_k$, где $\delta_k=\gamma_{k+1}\gamma_k^{-1} \in \Delta$. Обозначим через N нормальный делитель в F, порожденный левыми частями соотношений (1) и соотношений

$$\bar{\delta}^{-1}\omega_m=e \tag{3}$$

для всех $\delta \in \Delta$.

Лемма 11. $N=K$, *следовательно,* Γ *конечно определена.*

Доказательство. Положим $\Psi_i=\alpha(\Omega_i \times \{e\})$. Утверждается, что для любого $\delta \in \Delta$ и соответствующих элементов w_j, построенных выше, имеем

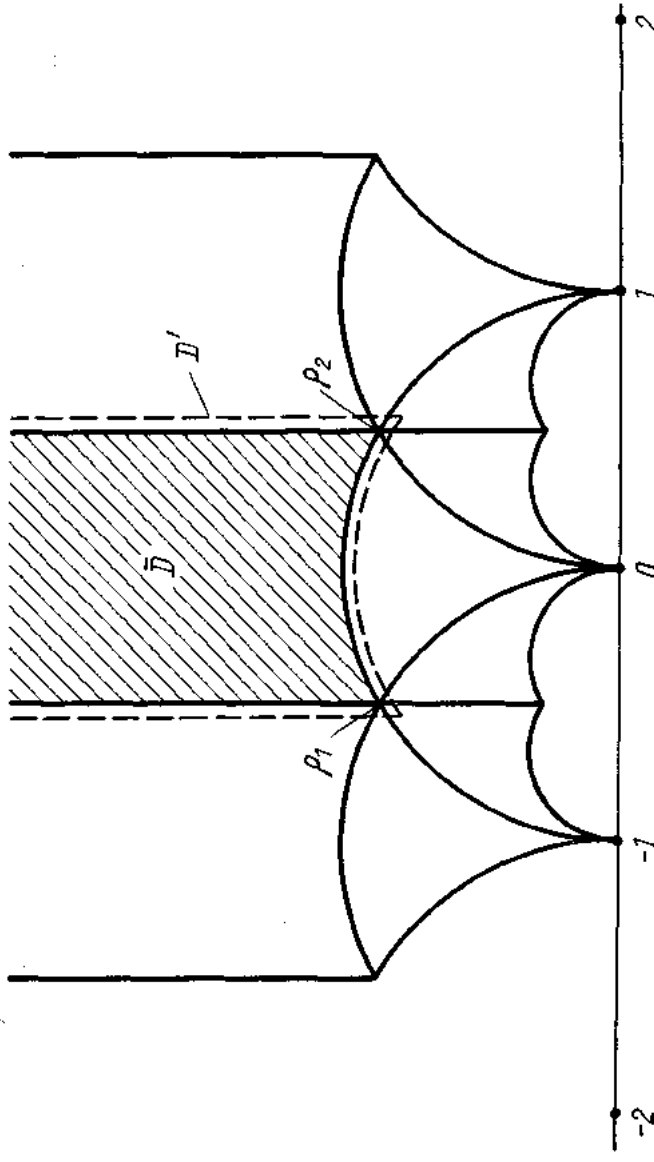
$$\Psi_{i_j}\sigma(w_j) \cap \Psi_{i_{j+1}}\sigma(w_{j+1}) \neq \varnothing. \tag{4}$$

Действительно, пусть $x_j\gamma_j=x_{j+1}\gamma_{j+1} \in \Omega_{i_j}\gamma_j \cap \Omega_{i_{j+1}}\gamma_{j+1}$. Тогда $\delta_j=\gamma_{j+1}\gamma_j^{-1} \in \Delta$ и $x_j=x_{j+1}\delta_j$, $\sigma(w_{j+1})=\sigma(\bar{\delta}_j)\sigma(w_{j+1})$, откуда и следует (4). Обозначим через Φ объединение множеств $\Psi_{i_j}\sigma(w_j)$, построенных для всех $\delta \in \Delta$. Так как любая цепочка $\Psi_{i_j}\sigma(w_j)$ начинается с Ψ_0, то Φ связно. Пусть Y — связная компонента пространства S, содержащая Φ. Для любого $\delta \in \Delta$ имеем $\Psi_0\sigma(\bar{\delta})=\Psi_{i_m}\sigma(w_m) \subset \Phi$, так что $\Phi \cap \Phi\sigma(\bar{\delta}) \neq \varnothing$, и поэтому $Y\sigma(\bar{\delta})=Y$. Так как элементы $\sigma(\bar{\delta})$, $\delta \in \Delta$, порождают H, то $Yh=Y$ для любого $h \in H$. Используя локальную связность S, легко показать, что ограничение $P|_Y$: $Y \to X$ также является накрытием. Отображение $P|_Y$ биективно в силу односвязности X; с другой стороны, все множества $\Psi_0 h$, $h \in \operatorname{Ker}\theta$, лежат в Y, не пересекаются (см. доказательство леммы 10) и дают в образе Ω_0. Следовательно, $\operatorname{Ker}\theta=\{e\}$, и лемма доказана.

Таким образом, доказательство теоремы 2 завершено.

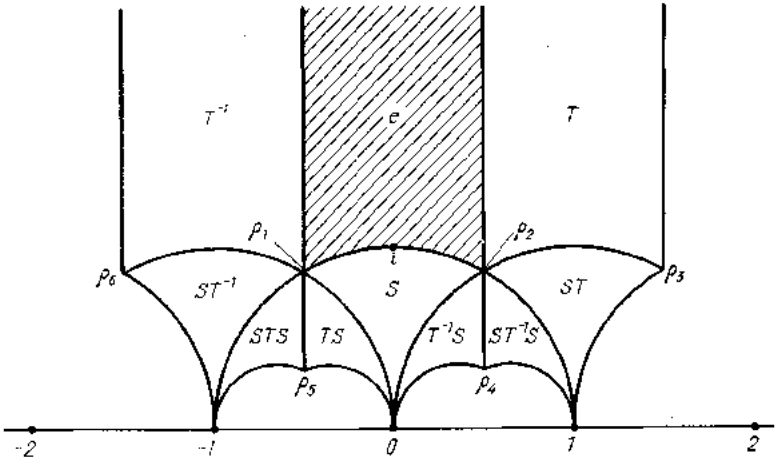
Доказательство теоремы 2 в принципе позволяет строить явное задание арифметической группы образующими и соотношениями, если известна ее «хорошая» фундаментальная область. В этой связи разберем классический пример группы $SL_2(\mathbb{Z})$.

Пример (образующие и соотношения для $SL_2(\mathbb{Z})$). Как мы уже знаем (см. § 4.2), пространство $X=SO_2(\mathbb{R})\backslash SL_2(\mathbb{R})$ можно отождествить с верхней полуплоскостью P. Группа $\Gamma=PSL_2(\mathbb{Z})=SL_2(\mathbb{Z})/\{\pm e\}$ действует на P справа с фундаментальной областью $D=\{z \in P \mid |z|>1, |\operatorname{Re} z|<1/2\}$ (предложение 4). Замыкание $\bar{D}$ удовлетворяет условиям (i) и (ii), выделенным при доказательстве теоремы 2, но не является открытым в P. Тем не менее рассмотрим множество $\Delta=\Delta_{\bar{D}}=\{\delta \in \Gamma \mid \bar{D} \cap \bar{D}\delta \neq \varnothing\}$. Сдвиги $\bar{D}$ на элементы множества Δ изображены на следующем рисунке:


D'
P_2
$\bar{D}$
P_1
2
1
0
-1
-2

Ясно, что если перейти от $\bar{D}$ к «чуть-чуть» большей области D', то $\Delta_{D'} = \{\delta \in \Gamma \mid D' \cap D'\delta\}$ будет совпадать с Δ. С другой стороны, к D' применимо доказательство теоремы. Отсюда следует, что Δ является системой образующих для Γ, а все соотношения есть следствия локальных соотношений. Из рисунка видно, что $[\Delta] = 10$, поэтому если мы попытаемся «в лоб» применить метод, указанный при доказательстве теоремы 10, то нам придется работать с 10 образующими и анализировать $10 \times 10 = 100$ локальных соотношений. Для сокращения этой процедуры мы применим дополнительные геометрические соображения. Вспомним, что P является моделью геометрии Лобачевского, прямыми в которой служат прямые, перпендикулярные оси Ox, и полуокружности с центрами на Ox. Тем самым $\bar{D}$ является неевклидовым треугольником с двумя конечными вершинами (ρ_1, ρ_2) и одной вершиной на бесконечности. При этом Γ действует на P изометриями, так что сдвиги $\bar{D}\gamma$, $\gamma \in \Gamma$ также являются треугольниками, которые в совокупности образуют симплициальное разбиение P, т. е. два треугольника либо не пересекаются, либо имеют общую сторону, либо общую вершину. Доказательство симплициальности действия Γ вытекает из того, что соседние с $\bar{D}$ треугольники действительно пересекаются с $\bar{D}$ требуемым образом (см. рисунок). Тогда, слегка видоизменяя доказательство первой части теоремы, можно показать, что Γ порождается теми γ, для которых $\bar{D}$ и $\bar{D}\gamma$ имеют общую сторону (можно также заметить, что подгруппа, порожденная такими γ, содержит Δ, см. ниже). В данном случае множество таких γ состоит из трех элементов: $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ (преобразование, отвечающее матрице $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$), $T^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$ и $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Геометрически преобразование T является параллельным переносом на единицу вдоль оси Ox, а S — композицией инверсии относительно окружности $|z| = 1$ и симметрии относительно оси Oy. Используя это описание, легко показать, что соседние с $\bar{D}$ треугольники могут быть получены из $\bar{D}$ путем преобразований, указанных на следующем ниже рисунке (с. 227).

Локальные соотношения, введенные при доказательстве теоремы 2, имеют вид $\bar{\delta}_1\bar{\delta}_2 = \bar{\delta}_3$, где $\delta_3 = \delta_1\delta_2$ и $\delta_1, \delta_2, \delta_3 \in \Delta$. Проанализируем вначале локальные соотношения, в которых либо δ_1, либо δ_2 совпадает с S. Несложный перебор вариантов показывает, что все они являются следствием соотношения $S^2 = e$. Прежде чем переходить к общему случаю, сделаем одно замечание. Если ρ_1 и ρ_2 — конечные вершины треугольника $\bar{D}$, то для любого $\delta \in \Delta$ имеем $\{\rho_1, \rho_2\}\delta \cap \{\rho_1, \rho_2\} \neq \varnothing$, что является следствием условия $\bar{D}\delta \cap \bar{D} \neq \varnothing$ и симплициальности действия Γ. Так как $\rho_1 S = \rho_2$, $\rho_2 S = \rho_1$, то для любого $\delta \in \Delta$ выполняется следующее условие: $S\delta$, $\delta S \in \Delta$ и либо δ, либо $S\delta$ и δS стаби-



лизируют одну из точек ρ_1, ρ_2. Покажем теперь, что по модулю соотношений, содержащих S, любое локальное соотношение сводится к соотношению, в котором δ_1 и δ_2 стабилизируют одну из вершин. В самом деле, пусть $\delta_1\delta_2 = \delta_3$ и $\delta_1, \delta_2, \delta_3 \in \Delta$. Домножая при необходимости δ_3 на S, можно считать, что $\rho_1\delta_3 = \rho_1$ (или $\rho_2\delta_3 = \rho_2$, что разбирается аналогично). Если $\rho_1\delta_2 = \rho_1$, то $\rho_1\delta_1 = \rho_1$, и все доказано. Покажем, что случай $\rho_2\delta_2 = \rho_2$ не реализуется. Достаточно установить, что при этих условиях

$$\{\rho_1, \rho_2\}\left(\delta_3\delta_2^{-1}\right) \cap \{\rho_1, \rho_2\} = \varnothing.$$

Ясно, что элемент $\delta_3\delta_2^{-1}$ не может стабилизировать ни одну из вершин, поэтому надо доказать невозможность соотношений

$$\rho_1\left(\delta_3\delta_2^{-1}\right) = \rho_2, \tag{5}$$

$$\rho_2\left(\delta_3\delta_2^{-1}\right) = \rho_1. \tag{6}$$

Если выполняется (5), то $\rho_1 = \rho_1\delta_3 = \rho_2\delta_2 = \rho_2$, — противоречие. Если же выполняется (6), то $\rho_2\delta_3 = \rho_1\delta_2$, но легко проверить, что множество $\{\rho_1\delta \mid \rho_2\delta = \rho_2\}$ состоит из точек ρ_1, ρ_3, ρ_4 и не пересекается с множеством $\{\rho_2\delta \mid \rho_1\delta = \rho_1\}$, которое состоит из точек ρ_2, ρ_5, ρ_6.

Итак, пусть $\delta_1\delta_2 = \delta_3$ и $\rho_1\delta_3 = \rho_1$, но $\rho_1\delta_2 \neq \rho_1$. Тогда перепишем соответствующее локальное соотношение в виде $(\delta_1 S)(S\delta_2) = \delta_3$. Так как $\rho_2\delta_2 \neq \rho_2$, то $\rho_1(S\delta_2) = \rho_1$ и $\rho_1(\delta_1 S) = \rho_1$. Таким образом, можно считать, что все δ_1, δ_2, δ_3 стабилизируют одну из точек ρ_1, ρ_2.

Лемма 12. *Стабилизатор точки* ρ_1 (*соответственно*, ρ_2) *в* Γ *является циклической группой третьего порядка, порожденной* TS (*соответственно*, ST).

Доказательство. Если g задается матрицей $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, то $zg = \frac{dz+b}{cz+a}$. Тогда условие $\rho_1 g = \rho_1$ переписывается в виде $c\rho_1^2 + (a-d)\rho_1 - b = 0$. Но $\rho_1 = \frac{-1+\sqrt{3}\,i}{2}$, и минимальный полином ρ_1 над $\mathbb{Q}$ имеет вид $t^2+t+1=0$. Поэтому если $a, b, c, d \in \mathbb{Z}$ и $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1$, то либо $b = c = a - d = 0$, что соответствует тождественному преобразованию, либо $b = \pm 1$, $c = \mp 1$, $a - d = \mp 1$, что соответствует матрицам $\pm\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, $\pm\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$. Остается заметить, что

$$TS = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}, \quad (TS)^2 = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}.$$

Вычисление стабилизатора ρ_2 получается из соотношения $\rho_1 S = \rho_2$. Лемма доказана.

Из леммы 12 вытекает, что локальные соотношения, в которых все буквы стабилизируют одну из вершин, сводятся к соотношению $(ST)^3 = e$. Таким образом, группа $PSL_2(\mathbb{Z})$ задается образующими S, T и соотношениями $S^2 = (ST)^3 = e$. Соответственно группа $SL_2(\mathbb{Z})$ задается образующими S, T, U и соотношениями $S^2 = (ST)^3 = U$ и $U^2 = e$.

Даже из приведенного примера ясно, что теорема 2 не снимает проблемы нахождения явного задания арифметических групп образующими и соотношениями. Большое число примеров явного задания (арифметических) групп образующими и соотношениями см. в книге Кокстера, Мозера [1]. С точки зрения теории алгебраических групп представляет интерес явное задание группы целых точек $G_{\mathbb{Z}}$ группы Шевалле G, найденное Бером [4]. А именно, если G — односвязная почти простая группа Шевалле, построенная по системе корней R, то $G_{\mathbb{Z}}$ порождается образующими x_α $(\alpha \in R)$ и, в случае $R \neq A_1$, определяется следующими соотношениями:

$$[x_\alpha, x_\beta] = \prod_{i,\, i>0} x_{i\alpha+j\beta}^{N_{ij}^{\alpha,\beta}}, \qquad (x_\alpha^{-1} x_{-\alpha} x_\alpha^{-1})^4 = 1,$$

где в первом соотношении α, β пробегают все корни $(\beta \neq -\alpha)$, а во втором α — некоторый длинный корень, $[x_\alpha, x_\beta]$ — коммутатор элементов x_α, x_β, $N_{ij}^{\alpha,\beta}$ — некоторые целые числа (более полную информацию о которых можно почерпнуть из леммы 15 книги Стейнберга [2]). В случае $R = A_1$, т. е. $G = SL_2$, первое из соотношений меняется на такое:

$$x\ x_{-\alpha}^{-1} x_\alpha = x_{-\alpha}^{-1} x_\alpha x_{-\alpha}^{-1}.$$

Если $G = \boldsymbol{SL}_n$, то результат Бера дает хорошо известную порождаемость группы $SL_n(\mathbb{Z})$ элементарными матрицами. В связи с этим следует упомянуть результат Картера и Келлера [1], согласно которому любой элемент из $SL_n(\mathbb{Z})$ можно представить в виде произведения элементарных матриц, число которых не превышает некоторой константы (результат остается верным при замене $\mathbb{Z}$ на кольцо целых $\mathcal{O}$ поля арифметических чисел). О. И. Тавгень [3] обобщил результат Картера и Келлера на произвольные группы Шевалле ранга, большего 1 (при этом вместо элементарных матриц появляются «корневые» образующие x_α). Отметим, что в случае $G = \boldsymbol{Sp}_{2n}$, $n \geqslant 3$, аналогичное утверждение получил К. Х. Закирьянов [1]. Однако им использовалась более широкая система образующих и, кроме того, ошибочно утверждалось, что $Sp_4(\mathbb{Z})$ не имеет ограниченной порождаемости относительно элементарных симплектических матриц.

Вообще, абстрактную конечно порожденную группу Γ назовем *группой ограниченной ширины*, если найдется такое конечное порождающее множество $X \subset \Gamma$, что любой элемент $g \in \Gamma$ представим в виде $g = x_1^{\alpha_1} \ldots x_t^{\alpha_t}$, где $x_i \in X$, $\alpha_i \in \mathbb{Z}$, а число t ограничено константой, не зависящей от g.

Проблема. Какие арифметические группы являются группами ограниченной ширины?

Из работы Тавгеня [3] следует, что это, например, арифметические группы вида $G_{\mathbb{Z}}$, где G — группы Шевалле ранга, большего 1. С другой стороны, там же показано, что группы $SL_2(\mathbb{Z})$, $SL_2(\mathcal{O}_d)$, где $\mathcal{O}_d$ — кольцо целых мнимого квадратичного поля $\mathbb{Q}(\sqrt{-d})$, $d > 0$, не имеют ограниченной ширины. Сопоставление этих фактов с полученными к настоящему времени результатами по конгруэнц-проблеме (см. § 9.5) наводит на мысль о том, что среди арифметических подгрупп простых односвязных алгебраических групп ограниченную ширину имеют те и только те группы, для которых положительно решается конгруэнц-проблема (т. е. соответствующее конгруэнц-ядро конечно). Кажется вероятным, что дальнейшее развитие этих соображений может привести к новому подходу к конгруэнц-проблеме.

Чтобы завершить обсуждение образующих и соотношений арифметических групп, нам остается еще раз обратить внимание читателя на тот факт, что эту тему можно рассматривать с точки зрения общей теории дискретных групп преобразований, которой посвящен обзор Винберга, Шварцмана [1]. Стоит также подчеркнуть, что многие группы, изучаемые этой теорией (в частности, дискретные группы, порожденные отражениями, группы с симплициальной фундаментальной областью (ср. приведенный выше пример)) оказываются неарифметическими.

Наш следующий результат восходит к классическим работам Жордана (см. Делоне и др. [1]), где установлена конечность числа несопряженных конечных подгрупп группы $SL_n(\mathbb{Z})$.

Теорема 3. *Пусть G — связная алгебраическая группа, определенная над $\mathbb{Q}$. Тогда конечные подгруппы группы $G_{\mathbb{Z}}$ образуют конечное число классов сопряженности.*

Доказательство. Положим $\Gamma = G_{\mathbb{Z}}$ и будем использовать применительно к этому случаю обозначения, введенные при доказательстве теоремы 2. В частности, $\mathbf{K}$ — максимальная компактная подгруппа в $G_{\mathbb{R}}$, $X = \mathbf{K}\backslash G_{\mathbb{R}}$ и $\Omega \subset X$ — такое подмножество, что: 1) $X = \Omega\Gamma$; 2) множество $\Delta = \{\delta \in \Gamma \mid \Omega\delta \cap \Omega \neq \varnothing\}$ конечно. Пусть $\Theta \subset \Gamma$ — конечная подгруппа. В силу того, что любая компактная подгруппа группы $G_{\mathbb{R}}$ сопряжена подгруппе группы $\mathbf{K}$ (предложение 3.10), найдется $g \in G_{\mathbb{R}}$ со свойством $g\Theta g^{-1} \subset \mathbf{K}$. Последнее означает, что точка $x = \mathbf{K}g \in X$ неподвижна относительно преобразований из Θ. Представим x в виде $x = x_0\gamma$, где $x_0 \in \Omega$, $\gamma \in \Gamma$. Тогда точка x_0 неподвижна относительно группы $\gamma\Theta\gamma^{-1}$ так, что $x_0 \in \Omega \cap \Omega\delta$ для любого $\delta \in \gamma\Theta\gamma^{-1}$, и, значит, $\gamma\Theta\gamma^{-1} \subset \Delta$. Таким образом, любая конечная подгруппа в Γ сопряжена подгруппе, содержащейся в конечном множестве Δ. Теорема 3 доказана.

Замечание. Используя теорему 9, можно дать другое доказательство теоремы 3, в духе доказательства предложения 3.5 (см. также доказательство теоремы 5.10).

Теперь мы в состоянии доказать инвариантность класса арифметических подгрупп при произвольных сюръективных морфизмах.

Теорема 1. *Пусть φ: $G \to H$ — сюръективный $\mathbb{Q}$-определенный морфизм $\mathbb{Q}$-определенных алгебраических групп. Если Γ — арифметическая подгруппа в G, то $\varphi(\Gamma)$ — арифметическая подгруппа в H.*

Доказательство. Достаточно показать, что группа $\varphi(G_{\mathbb{Z}})$ арифметична в H, причем, выбирая подходящую реализацию H, можно считать, что $\varphi(G_{\mathbb{Z}}) \subset H_{\mathbb{Z}}$ (см. замечание после предложения 2). Тогда в доказательстве нуждается конечность индекса $[H_{\mathbb{Z}} : \varphi(G_{\mathbb{Z}})]$. Сведем общий случай к случаю, когда группа G является либо редуктивной, либо унипотентной. Пусть $G = CU$ — разложение Леви группы G, где $U = R_u(G)$ — унипотентный радикал G, а группа C редуктивна. Положим $D = \varphi(C)$, $V = \varphi(U)$; тогда $H = DV$ — разложение Леви группы H. Если предположить, что индексы $[D_{\mathbb{Z}} : \varphi(C_{\mathbb{Z}})]$ и $[V_{\mathbb{Z}} : \varphi(U_{\mathbb{Z}})]$ конечны, то элементарное рассуждение (ср. доказательство леммы 7) позволяет установить конечность индекса $[D_{\mathbb{Z}}V_{\mathbb{Z}} : \varphi(C_{\mathbb{Z}}U_{\mathbb{Z}})]$. С другой стороны, индекс $[H_{\mathbb{Z}} : \varphi(G_{\mathbb{Z}})]$ конечен в силу следствия 2 из предложения 1. Поэтому конечен индекс $[H_{\mathbb{Z}} : \varphi(C_{\mathbb{Z}}U_{\mathbb{Z}})]$ и тем более — индекс $[H_{\mathbb{Z}} : \varphi(G_{\mathbb{Z}})]$.

Пусть вначале группа G унипотентна. Тогда факторпространство $G_{\mathbb{R}}/G_{\mathbb{Z}}$ компактно (лемма 7). Так как в силу следствия 3 из теоремы 3.6 $H_{\mathbb{R}}=\varphi(G_{\mathbb{R}})$, то пространство $H_{\mathbb{R}}/\varphi(G_{\mathbb{Z}})$ компактно. С другой стороны, факторпространство $H_{\mathbb{Z}}/\varphi(G_{\mathbb{Z}})$ замкнуто и дискретно в $H_{\mathbb{R}}/\varphi(G_{\mathbb{Z}})$, откуда и получается требуемая конечность индекса $[H_{\mathbb{Z}}:\varphi(G_{\mathbb{Z}})]$.

Осталось рассмотреть случай редуктивной группы G. Здесь конечность нужного нам индекса является следствием теоремы 9. В самом деле, пусть $H\subset GL_n(\mathbb{C})$. Используя при необходимости вложение $GL_n(\mathbb{C})\to GL_{n+1}(\mathbb{C})$: $A\longmapsto\begin{pmatrix} A & 0\\ 0 & (\det A)^{-1}\end{pmatrix}$, можно считать, что H замкнута по Зарисскому в $M_n(\mathbb{C})$. Определим действие G на $V=M_n(\mathbb{C})$ формулой $Ag=A\varphi(g)$, где справа стоит обычное произведение матриц. Тогда $H=E_n\varphi(G)$ является замкнутой орбитой группы G, и, согласно теореме 9, $H_{\mathbb{Z}}$ является объединением конечного числа орбит группы $G_{\mathbb{Z}}$. Но эти орбиты, как нетрудно видеть, совпадают со смежными классами $H_{\mathbb{Z}}\backslash\varphi(G_{\mathbb{Z}})$, откуда и следует конечность индекса $[H_{\mathbb{Z}}:\varphi(G_{\mathbb{Z}})]$. Теорема доказана.

Приведенные результаты являются первыми шагами в направлении изучения абстрактных свойств арифметических групп. В последующих главах мы расскажем о более глубоких фактах, касающихся, в частности, нормального строения арифметических групп. Отметим, однако, что их получение сопряжено с использованием гораздо более сложной техники.

Перед формулировкой теоремы плотности выделим классы полупростых групп, которые принципиально различаются по своим арифметическим свойствам и которые будут участвовать в формулировке многих теорем этой книги.

Определение. Говорят, что $\mathbb{Q}$-определенная алгебраическая группа G имеет *компактный тип*, если группа вещественных точек $G_{\mathbb{R}}$ компактна. Пусть теперь группа G полупроста. Тогда G имеет *некомпактный тип*, если группа $G^i_{\mathbb{R}}$ некомпактна для любого $\mathbb{Q}$-простого сомножителя G^i группы G. Если G не принадлежит ни к одному из указанных выше типов, то говорят, что G имеет *смешанный тип*.

Теорема 10 (теорема плотности; см. Борель [5]). *Пусть G — полупростая $\mathbb{Q}$-определенная группа некомпактного типа. Тогда замыкание в топологии Зарисского любой арифметической подгруппы $\Gamma\subset G$ совпадает с G.*

Доказательство. Если мы докажем теорему для $\mathbb{Q}$-простых групп, то замыкание $\overline{\Gamma}$ должно содержать $\overline{\Gamma\cap G^i}=G^i$ для любого $\mathbb{Q}$-простого сомножителя G^i группы G. Тогда $\overline{\Gamma}\supset\prod_i G^i=$ $=G$, что и требовалось. Для рассмотрения случая $\mathbb{Q}$-простой группы G нам понадобится один факт, в справедливости

которого мы убедимся в следующем параграфе:

если G — полупростая $\mathbb{Q}$-группа с некомпактной группой $G_{\mathbb{R}}$, то группа $G_{\mathbb{Z}}$ бесконечна. (7)

(Отметим, что верно и обратное утверждение, ибо если группа $G_{\mathbb{R}}$ компактна, то группа $G_{\mathbb{Z}}$, являясь дискретной подгруппой, обязана быть конечной.)

Заметим теперь, что если $\Gamma_1 \subset \Gamma_2$ — подгруппы группы G и индекс $[\Gamma_2 : \Gamma_1]$ конечен, то для их замыканий $\overline{\Gamma}_i$ индекс $[\overline{\Gamma}_2 : \overline{\Gamma}_1]$ также конечен. В самом деле, если $\Gamma_2 = \bigcup_{i=1}^{d} \Gamma_1 \gamma_i$, то $\overline{\Gamma}_2 = \bigcup_{i=1}^{d} \overline{\Gamma}_1 \gamma_i$, т. е. $[\overline{\Gamma}_2 : \overline{\Gamma}_1] \leqslant d$. Отсюда следует совпадение связных компонент $(\overline{\Gamma}_1)^0 = (\overline{\Gamma}_2)^0$. Более общо, если подгруппы Γ_1 и Γ_2 соизмеримы, то

$$(\overline{\Gamma}_1)^0 = (\overline{\Gamma_1 \cap \Gamma_2})^0 = (\overline{\Gamma}_2)^0.$$

Завершим теперь доказательство теоремы. Без ограничения общности можно считать, что $\Gamma \subset G_{\mathbb{Z}}$. Тогда из (7) и сделанного выше замечания вытекает, что замыкание $H = \overline{\Gamma}$ является алгебраической $\mathbb{Q}$-группой положительной размерности. Для любого $g \in G_{\mathbb{Q}}$ группа $g\Gamma g^{-1}$ является арифметической (следствие 1 из предложения 4.1), т. е. соизмерима с Γ. Поэтому $H^0 = (\overline{\Gamma})^0 = (\overline{g\Gamma g^{-1}})^0 = gH^0g^{-1}$. Таким образом, H^0 нормализуется группой $G_{\mathbb{Q}}$. Так как нормализатор $N_G(H^0)$ является замкнутой подгруппой, а $G_{\mathbb{Q}}$ плотно в G (теорема 2.2), то $N_G(H^0) = G$, т. е. H^0 — нормальный делитель в G. Поскольку группа G не имеет $\mathbb{Q}$-определенных нормальных делителей положительной размерности, то $H^0 = G$. Теорема доказана.

Замечание. Хотя приведенное доказательство теоремы плотности существенно использует арифметичность Γ и не переносится на другие типы подгрупп группы G, сам результат справедлив в гораздо более общей ситуации. А именно, плотной в G в топологии Зарисского является любая замкнутая в вещественной топологии подгруппа $\Gamma \subset G_{\mathbb{R}}$, для которой пространство $G_{\mathbb{R}}/\Gamma$ имеет конечный инвариантный объем (см. Рагунатан [5], гл. V). В частности, плотной в топологии Зарисского является любая решетка $\Gamma \subset G_{\mathbb{R}}$, т. е. дискретная подгруппа с конечным объемом факторпространства $G_{\mathbb{R}}/\Gamma$ (тот факт, что арифметическая подгруппа полупростой $\mathbb{Q}$-определенной группы является решеткой, мы установим в § 4.6).

В заключение этого параграфа мы получим своеобразное обращение следствия 1 из предложения 1. А именно, для полупростой $\mathbb{Q}$-группы G и ее арифметической подгруппы Γ вычислим

$$C(\Gamma) = \{g \in G \mid \Gamma \text{ соизмерима с } g^{-1}\Gamma g\}.$$

(Здесь мы считаем, что $G = G_{\mathbb{C}}$.)

Используя тот факт, что отношение соизмеримости есть отношение эквивалентности, легко получить, что $C(\Gamma)$ является подгруппой в G, которая называется *подгруппой соизмеримости* Γ. Из этого факта вытекает также, что $C(\Gamma)$ в действительности не зависит от Γ. Так как, очевидно, $\Gamma \subset C(\Gamma)$, то $C(\Gamma)$ выступает как универсальное вместилище всех арифметических подгрупп группы G. Описание $C(\Gamma)$ дается следующим утверждением.

Предложение 6. *Пусть G — полупростая $\mathbb{Q}$-определенная алгебраическая группа, N — ее наибольшая инвариантная $\mathbb{Q}$-подгруппа компактного типа и π: $G \to G/N$ — соответствующая проекция. Тогда $C(\Gamma) = \pi^{-1}((G/N)_{\mathbb{Q}})$.*

Доказательство Пусть $G^1, \ldots, G^r$ — простые над $\mathbb{Q}$ сомножители группы G. Тогда N порождается теми G^i, для которых группа $G^i_{\mathbb{R}}$ компактна, и центрами остальных сомножителей. Пусть также H — нормальный делитель, порожденный G^i с некомпактной группой $G^i_{\mathbb{R}}$. Ясно, что $G = H \cdot N$ и пересечение $H \cap N$ конечно, т. е. морфизм-произведение $H \times N \to G$ является изогенией. Так как подгруппы $H \cap \Gamma$ и $N \cap \Gamma$ арифметичны в H и N соответственно, то из теоремы 1 получаем, что группа $(H \cap \Gamma)(N \cap \Gamma)$ арифметична в G. В силу компактности $N_{\mathbb{R}}$ группа $N \cap \Gamma$ конечна, так что $H \cap \Gamma$ является подгруппой конечного индекса в Γ. Как мы отмечали выше, отсюда следует, что $C(\Gamma) = C(\Gamma \cap H)$. Воспользовавшись тем, что ограничение π на H является изогенией, нетрудно получить, что $C(\Gamma \cap H)$ совпадает с прообразом относительно π группы соизмеримости $\pi(\Gamma \cap H)$ в группе G/N. Тем самым мы свели нашу задачу к случаю $N = \{1\}$; в частности, $Z(G) = \{1\}$. Покажем, что здесь $C(\Gamma) = G_{\mathbb{Q}}$. В силу теоремы плотности замыкание по Зарисскому $\overline{\Gamma}$ совпадает с G, причем можно без ограничения общности предполагать, что $\Gamma \subset G_{\mathbb{Z}}$. Зафиксируем некоторое вложение $G \subset GL_n(\mathbb{C})$ и через $\mathbb{C}[A]$ будем обозначать $\mathbb{C}$-оболочку подмножества $A \subset G$, т. е. подпространство в $M_n(\mathbb{C})$, порожденное A. Тогда, так как $\overline{\Gamma} = G$, то $\mathbb{C}[\Gamma] = \mathbb{C}[G]$. Более того, если $g \in C(\Gamma)$, то группа $\Gamma \cap g^{-1}\Gamma g$ имеет конечный индекс в Γ, и поэтому также $\overline{\Gamma \cap g^{-1}\Gamma g} = G$, откуда $\mathbb{Q}[\Gamma] = \mathbb{Q}[\Gamma \cap g^{-1}\Gamma g]$. Поэтому для любого $g \in C(\Gamma)$

$$g\mathbb{Q}[\Gamma]g^{-1} = g\mathbb{Q}[\Gamma \cap g^{-1}\Gamma g]g^{-1} = \mathbb{Q}[\Gamma]. \tag{8}$$

Рассмотрим присоединенное представление ρ: $G \to GL(V)$ в пространстве $V = \mathbb{C}[G]$, $\rho(g)v = gvg^{-1}$. Так как $V_{\mathbb{Q}} = \mathbb{Q}[\Gamma]$, то из (8) получаем, что $\rho(C(\Gamma)) \subset \rho(G)_{\mathbb{Q}}$. Но по условию $Z(G) = \{1\}$, так что представление ρ является точным и $C(\Gamma) \subset G_{\mathbb{Q}}$. Обратное включение получаем из следствия 1 из предложения 1. Предложение 6 доказано.

Из предложения 6 вытекает, что любая арифметическая подгруппа полупростой присоединенной группы G некомпактного типа обязательно содержится в $G_{\mathbb{Q}}$. Наоборот, если $G = SL_n(\mathbb{C})$, то арифметической в G будет подгруппа Γ, порожденная $SL_n(\mathbb{Z})$ и матрицей $\begin{pmatrix} s & & 0 \\ & \ddots & \\ 0 & & s \end{pmatrix}$, где s — примитивный корень степени n из единицы; ясно, что $\Gamma \not\subset G_{\mathbb{Q}}$ при $n > 2$. Здесь подгруппа соизмеримости есть

$$\left\{ \frac{1}{(\det A)^{1/n}} A \,\middle|\, A \in GL_n(\mathbb{Q}) \right\}.$$

§ 4.5. Критерий компактности факторпространства $G_{\mathbb{R}}/G_{\mathbb{Z}}$

Изложенная в § 4.2—4.3 теория приведения уже позволила нам получить ряд структурных теорем об арифметических группах. К указанной там конструкции фундаментального множества мы еще не раз вернемся. Тем не менее эта конструкция не позволяет ответить на все возникающие в теории приведения вопросы, в частности, дать критерий компактности факторпространства $G_{\mathbb{R}}/G_{\mathbb{Z}}$, что важно, например, для изучения когомологий арифметических групп. Этому вопросу в основном и посвящен настоящий параграф. Мы начинаем рассмотрение с алгебраических торов. Оказывается, что здесь общий случай сводится к норменным торам $S = \mathbf{R}^{(1)}_{K/\mathbb{Q}}(\boldsymbol{G}_m)$, где K — конечное расширение $\mathbb{Q}$ (определение норменного тора см. в § 2.1, п. 7). Построение же фундаментального множества для таких торов эквивалентно доказательству известной теоремы Дирихле о единицах. Используемый нами для этого метод имеет достаточно общую природу и применим к другим группам, возникающим из алгебр с делением.

Предложение 7. *Пусть K — конечное расширение поля $\mathbb{Q}$ степени n, $S = \mathbf{R}^{(1)}_{K/\mathbb{Q}}(\boldsymbol{G}_m)$ — соответствующий норменный тор. Тогда факторпространство $S_{\mathbb{R}}/S_{\mathbb{Z}}$ компактно.*

Доказательство. Положим $V = K \otimes_{\mathbb{Q}} \mathbb{R}$ и будем обозначать через N естественное продолжение норменного отображения $N_{K/\mathbb{Q}}$ на V. Хорошо известно, что для $a \in V$ норма $N(a)$ совпадает с определителем преобразования левого сдвига $x \mapsto ax$, $x \in V$. Отсюда следует (см. § 3.5), что сдвиги на элементы из $S_{\mathbb{R}} = \{x \in V \mid N(x) = 1\}$ сохраняют меру Хаара μ на аддитивной группе V. Пусть $\mathcal{O}$ — кольцо целых поля K. Тогда $\mathcal{O}$ является решеткой в пространстве V, в частности, $V/\mathcal{O}$ компактно и $\mu(V/\mathcal{O}) < \infty$. Выберем компактное подмножество $B \subset V$ со свойством $\mu(B) > \mu(V/\mathcal{O})$ и положим $C = \{b_1 - b_2 \mid b_1, b_2 \in B\}$. Если $a \in S_{\mathbb{R}}$, то $\mu(aB) = \mu(a^{-1}B) = \mu(B) > \mu(V/\mathcal{O})$, так что

ограничение на aB и $a^{-1}B$ проекции $V \to V/\mathcal{O}$ не может быть инъективным. Следовательно, найдутся такие $c, d \in C$, что $\alpha = ac$, $\beta = a^{-1}d$ лежат в $\mathcal{O}$. Тогда $\alpha\beta = cd \in C^2 \cap \mathcal{O}$. Последнее пересечение, будучи одновременно компактным и дискретным, является конечным. Воспользуемся теперь следующим простым утверждением.

Лемма 13. *Пусть $\gamma \in \mathcal{O}$, $\gamma \neq 0$. Тогда среди всех разложений $\gamma = \alpha\beta$ $(\alpha, \beta \in \mathcal{O})$ имеется лишь конечное число неассоциированных.*

(Напомним, что два разложения $\gamma = \alpha_1\beta_1 = \alpha_2\beta_2$ называются *ассоциированными*, если существует обратимый элемент (единица) $\varepsilon \in \mathcal{O}^*$ такой, что $\alpha_2 = \varepsilon\alpha_1$, $\beta_1 = \varepsilon\beta_2$.)

Из леммы 13 вытекает, что если рассмотреть всевозможные разложения $\gamma = \alpha\beta$, где $\alpha, \beta \in \mathcal{O}$, всех элементов $\gamma \in C^2 \cap \mathcal{O}$, то среди возникающих здесь элементов β имеется лишь конечное число неассоциированных. Так как норма любой единицы $\varepsilon \in \mathcal{O}^*$ есть ± 1, то найдется конечное число таких элементов $\beta_1, \ldots, \beta_r \in \mathcal{O}$, что любой элемент β из рассматриваемого класса имеет вид $\beta = \beta_i\varepsilon$ для подходящего $\varepsilon \in \mathcal{O}^* \cap S = S_{\mathbb{Z}}$. С другой стороны, по построению $\beta = a^{-1}d$, где $d \in C$. Отсюда $a = d\beta_i^{-1}\varepsilon^{-1}$, и, следовательно,

$$S_{\mathbb{R}} = \left(\bigcup_{i=1}^{r} (C\beta_i^{-1} \cap S_{\mathbb{R}}) \right) S_{\mathbb{Z}}.$$

Из этого разложения в силу компактности C вытекает компактность факторпространства $S_{\mathbb{R}}/S_{\mathbb{Z}}$. Предложение доказано.

Из предложения 7 можно легко вывести теорему Дирихле о единицах, однако мы проведем соответствующие рассуждения чуть позднее, установив предварительно критерий компактности факторпространства $S_{\mathbb{R}}/S_{\mathbb{Z}}$ для случая произвольных торов.

Теорема 11. *Пусть S — $\mathbb{Q}$-определенный алгебраический тор. Тогда следующие условия эквивалентны:*

1) *S анизотропен над $\mathbb{Q}$,*

2) *факторпространство $S_{\mathbb{R}}/S_{\mathbb{Z}}$ компактно.*

Доказательство. 2) $\Rightarrow$ 1). Пусть S не является $\mathbb{Q}$-анизотропным. Тогда существует $\mathbb{Q}$-определенный эпиморфизм $\varphi: S \to \boldsymbol{G}_m = T$. Так как $\varphi(S_{\mathbb{R}})$ имеет конечный индекс в $T_{\mathbb{R}}$ (следствие 3 из теоремы 3.6), то пространство $T_{\mathbb{R}}/\varphi(S_{\mathbb{Z}})$ должно быть компактным, если компактно пространство $S_{\mathbb{R}}/S_{\mathbb{Z}}$. С другой стороны, $\varphi(S_{\mathbb{Z}})$ — арифметическая подгруппа в T (теорема 1), и так как $T_{\mathbb{Z}} \simeq \mathbb{Z}^* = \{\pm 1\}$, то $\varphi(S_{\mathbb{Z}})$ — конечная группа. Поэтому пространство $T_{\mathbb{R}}/\varphi(S_{\mathbb{Z}})$ не может быть компактным, ибо некомпактно $T_{\mathbb{R}} \simeq \mathbb{R}^*$.

1) $\Rightarrow$ 2). Известно (см. предложение 2.2), что существует $\mathbb{Q}$-определенный эпиморфизм $\varphi: T \to S$, где тор T квазиразло-

жим, т. е. имеет вид $T=\prod_{i=1}^{d}\mathbf{R}_{K_i/\mathbf{Q}}(\mathbf{G}_m)$, K_i — конечные расширения поля $\mathbf{Q}$. Так как S является $\mathbf{Q}$-анизотропным, то ограничение φ на тор $T_0=\prod_{i=1}^{d}\mathbf{R}^{(1)}_{K_i/\mathbf{Q}}(\mathbf{G}_m)$ сюръективно. Согласно предложению 7 пространство $(T_0)_{\mathbf{R}}/(T_0)_{\mathbf{Z}}$ компактно, поэтому компактно и факторпространство $\varphi((T_0)_{\mathbf{R}})/\varphi((T_0))_{\mathbf{Z}}$. Но ввиду конечности индекса $[S_{\mathbf{R}}:\varphi((T_0)_{\mathbf{R}})]$ и арифметичности $\varphi((T_0)_{\mathbf{Z}})$ в S, последнее эквивалентно компактности исходного пространства $S_{\mathbf{R}}/S_{\mathbf{Z}}$. Теорема доказана.

Следствие 1 (теорема Дирихле о единицах). *Пусть S — $\mathbf{Q}$-определенный алгебраический тор. Тогда группа $S_{\mathbf{Z}}$ изоморфна прямому произведению конечной группы и свободной абелевой группы ранга* $\operatorname{rang}_{\mathbf{R}} S-\operatorname{rang}_{\mathbf{Q}} S$.

Доказательство. Пусть S_1 и S_2 — соответственно максимальный разложимый и максимальный анизотропный над $\mathbf{Q}$ подторы в S. Так как $(S_1)_{\mathbf{Z}}$ — конечная группа, то применяя теорему 1 к изогении $S_1\times S_2\to S$, получаем конечность индекса $(S_2)_{\mathbf{Z}}$ в $S_{\mathbf{Z}}$. С другой стороны, $\operatorname{rang}_{\mathbf{R}} S-\operatorname{rang}_{\mathbf{Q}} S=(\operatorname{rang}_{\mathbf{R}} S_1+\operatorname{rang}_{\mathbf{R}} S_2)-(\operatorname{rang}_{\mathbf{Q}} S_1+\operatorname{rang}_{\mathbf{Q}} S_2)=\operatorname{rang}_{\mathbf{R}} S_2$, ибо $\operatorname{rang}_{\mathbf{R}} S_1=\operatorname{rang}_{\mathbf{Q}} S_1=\dim S_1$. Поэтому в силу общих фактов об абелевых группах достаточно установить, что группа $(S_2)_{\mathbf{Z}}$ является произведением конечной группы на группу $\mathbf{Z}^r$, где $r=\operatorname{rang}_{\mathbf{R}} S_2$. Тем самым мы получаем редукцию к случаю $\mathbf{Q}$-анизотропного тора S. Из обсуждения в § 2.2, п. 4 вытекает, что над $\mathbf{R}$ любой тор изоморфен произведению торов $\mathbf{G}_m$, $\mathbf{R}^{(1)}_{\mathbf{C}/\mathbf{R}}(\mathbf{G}_m)$ и $\mathbf{R}^{(1)}_{\mathbf{C}/\mathbf{R}}(\mathbf{G}_m)$. Отсюда следует существование изоморфизма $S_{\mathbf{R}}\simeq\mathbf{R}^r\times D$, где $r=\operatorname{rang}_{\mathbf{R}} S$, а группа D компактна. С другой стороны, согласно теореме 11 факторгруппа $S_{\mathbf{R}}/S_{\mathbf{Z}}$ компактна. Поэтому наше утверждение вытекает из следующего хорошо известного факта, который мы сформулируем в несколько более общей форме, чем это надо для доказательства следствия, имея в виду дальнейшие ссылки.

Лемма 14. *Пусть G — абелева топологическая группа вида $\mathbf{Z}^a\times\mathbf{R}^b\times D$, где группа D компактна. Тогда любая дискретная подгруппа $\Gamma\subset G$ такая, что факторгруппа G/Γ компактна, имеет вид $\mathbf{Z}^{a+b}\times F$ для некоторой конечной группы F.*

Доказательство легко редуцируется к случаю $G=\mathbf{R}^n$, который разобран, например, у Бурбаки [2], гл. VII, § 1, п. 1.

Возьмем в качестве S тор $\mathbf{R}_{K/\mathbb{Q}}(\boldsymbol{G}_m)$, где K — конечное расширение поля $\mathbb{Q}$. Так как над $\mathbb{R}$ мы имеем $S \simeq \boldsymbol{G}_m^s \times \mathbf{R}_{\mathbb{C}/\mathbb{R}}(\boldsymbol{G}_m)^t$, где s, t — соответственно число вещественных и попарно несопряженных комплексных нормирований поля K, то $\operatorname{rang}_{\mathbb{R}} S = s + t$. Но $\operatorname{rang}_{\mathbb{Q}} S = 1$, и поэтому мы получаем классическую форму теоремы Дирихле: группа единиц $U(K)$ изоморфна $F \times \mathbb{Z}^{s+t-1}$, где F — группа всех корней из единицы в K. В следующей главе мы получим обобщение этого результата на S-единицы.

Получим теперь доказательство утверждения, которое мы использовали в предыдущем параграфе.

Следствие 2. *Пусть G — полупростая $\mathbb{Q}$-определенная группа. Группа $G_{\mathbb{Z}}$ бесконечна в том и только том случае, когда группа $G_{\mathbb{R}}$ некомпактна.*

Доказательство. Если группа $G_{\mathbb{R}}$ компактна, то $G_{\mathbb{Z}}$ является дискретной подгруппой компактной группы, и, следовательно, конечна. Обратно, пусть группа $G_{\mathbb{R}}$ некомпактна. Если G изотропна над $\mathbb{Q}$, то имеется одномерная $\mathbb{Q}$-определенная унипотентная подгруппа $U \subset G$, и уже группа $U_{\mathbb{Z}}$ бесконечна. Разберем теперь случай $\mathbb{Q}$-анизотропной группы G. Группа $G_{\mathbb{R}}$ некомпактна, т. е. $\mathbb{R}$-изотропна, и поэтому обладает максимальным $\mathbb{R}$-определенным тором T, который изотропен над $\mathbb{R}$. Согласно следствию 3 из предложения 7.3 найдется максимальный $\mathbb{Q}$-определенный тор $S \subset G$, который также изотропен над $\mathbb{R}$ (доказательство этого утверждения получается из рациональности многообразия торов и не использует никаких результатов настоящей главы). Но тогда в силу следствия 1 группа $S_{\mathbb{Z}}$ бесконечна. Другое доказательство следствия 2 см. в следующем параграфе.

Участвующие в формулировке теоремы 11 условия (компактность факторпространства $S_{\mathbb{R}}/S_{\mathbb{Z}}$ и $\mathbb{Q}$-анизотропность группы S) на самом деле эквивалентны для произвольных алгебраических групп, как показывает следующая теорема:

Теорема 12. *Пусть G — алгебраическая группа, определенная над $\mathbb{Q}$. Тогда следующие условия эквивалентны:*

1) *$G_{\mathbb{R}}/G_{\mathbb{Z}}$ компактно;*

2) *редуктивная часть связной компоненты G анизотропна над $\mathbb{Q}$.*

(Отметим, что второе условие можно также сформулировать в виде: $\mathbf{X}(G^0)_{\mathbb{Q}} = \{1\}$ и каждый унипотентный элемент группы $G_{\mathbb{Q}}$ принадлежит унипотентному радикалу G.)

Доказательство. Достаточно рассмотреть случай связной группы G; пусть $G = HR_u(G)$ — ее разложение Леви. Тогда компактность $G_{\mathbb{R}}/G_{\mathbb{Z}}$ равносильна компактности $H_{\mathbb{R}}/H_{\mathbb{Z}}$. В одну сторону это вытекает из леммы 7, а в другую — из следующего утверждения.

Лемма 15. *Пусть H — редуктивная подгруппа связной группы G, причем G и H определены над $\mathbb{Q}$. Тогда пространство $H_{\mathbb{R}}/H_{\mathbb{Z}}$ замкнуто в $G_{\mathbb{R}}/G_{\mathbb{Z}}$.*

Доказательство. Согласно усиленной теореме Шевалле найдутся $\mathbb{Q}$-определенное представление $\rho\colon G \to GL(V)$ и вектор $v \in V_{\mathbb{Q}}$ такие, что стабилизатор v относительно ρ совпадает с H. Тогда множество $W = v\rho(G_{\mathbb{Z}})$ содержится в некоторой решетке пространства $V_{\mathbb{Q}}$ (см. замечание после предложения 2) и, следовательно, замкнуто в $V_{\mathbb{R}}$. Поэтому множество $H_{\mathbb{R}}G_{\mathbb{Z}} = G_{\mathbb{R}} \cap \rho^{-1}(W)$ также замкнуто в $G_{\mathbb{R}}$. Лемма доказана.

Таким образом, достаточно рассмотреть случай редуктивной группы G. В этом случае импликация 1) $\Rightarrow$ 2) легко вытекает из леммы 15. В самом деле, если G является $\mathbb{Q}$-изотропной, то в ней имеется нетривиальный $\mathbb{Q}$-разложимый тор $S \subset G$. Тогда пространство $S_{\mathbb{R}}/S_{\mathbb{Z}}$ некомпактно (теорема 11) и замкнуто в $G_{\mathbb{R}}/G_{\mathbb{Z}}$, так что последнее также не может быть компактным.

Для доказательства обратной импликации осуществим вначале редукцию к случаю полупростой присоединенной группы. Пусть $Z = Z(G)$ — центр G. Тогда связная компонента $S = Z^0$ является $\mathbb{Q}$-анизотропным тором, и поэтому пространство $S_{\mathbb{R}}/S_{\mathbb{Z}}$ компактно (теорема 11). Так как индекс $[Z_{\mathbb{R}}\colon S_{\mathbb{R}}]$ конечен, то пространство $Z_{\mathbb{R}}/Z_{\mathbb{Z}}$ также компактно. Положим $H = G/Z$ и обозначим через π каноническую проекцию G на H. Рассмотрим, далее, отображение $\varphi\colon G_{\mathbb{R}}/G_{\mathbb{Z}} \to \pi(G_{\mathbb{R}})/\pi(G_{\mathbb{Z}})$, индуцированное π. Компактная группа $B = Z_{\mathbb{R}}/Z_{\mathbb{Z}}$ действует сдвигами на $G_{\mathbb{R}}/G_{\mathbb{Z}}$, и легко видеть, что орбиты группы B в точности совпадают со слоями отображения φ. Отсюда без труда следует собственность φ. Учитывая конечность индекса $[H_{\mathbb{R}} : \pi(G_{\mathbb{R}})]$ и арифметичность $\varphi(G_{\mathbb{Z}})$, мы видим, что компактность $G_{\mathbb{R}}/G_{\mathbb{Z}}$ эквивалентна компактности $H_{\mathbb{R}}/H_{\mathbb{Z}}$. Последнее мы и будем доказывать. Предварительно установим критерий компактности подмножества в факторпространстве $GL_n(\mathbb{R})/GL_n(\mathbb{Z})$.

Предложение 8 (критерий Малера). *Подмножество $\Omega \subset GL_n(\mathbb{R})$ относительно компактно по модулю группы $GL_n(\mathbb{Z})$ (т. е. компактен его образ в факторпространстве $GL_n(\mathbb{R})/GL_n(\mathbb{Z})$) в том и только том случае, если*

а) $\det g$ *ограничен для* $g \in \Omega$,

б) *существует окрестность нуля* $U \subset \mathbb{R}^n$ *со свойством* $\Omega(\mathbb{Z}^n \setminus \{0\}) \cap U = \varnothing$.

Доказательство. Если образ Ω в $GL_n(\mathbb{R})/GL_n(\mathbb{Z})$ относительно компактен, то найдется такой компакт $D \subset GL_n(\mathbb{R})$, что $\Omega \subset DGL_n(\mathbb{Z})$. Отсюда, очевидно, следует ограниченность $\det g$, $g \in \Omega$. Далее, имеем

$$\Omega(\mathbb{Z}^n \setminus \{0\}) \subset DGL_n(\mathbb{Z})(\mathbb{Z}^n \setminus \{0\}) = D(\mathbb{Z}^n \setminus \{0\}),$$

причем в силу дискретности $\mathbb{Z}^n$ и компактности D последнее множество замкнуто в $\mathbb{R}^n$ и не содержит нуля, откуда следует существование требуемой окрестности U.

Обратно, пусть выполнены условия а) и б), и пусть $\Sigma = \Sigma_{t,v}(t \geqslant 2/\sqrt{3},\ v \geqslant 1/2)$ — *область Зигеля в группе* $GL_n(\mathbb{R})$. Мы знаем (теорема 4), что $\Sigma GL_n(\mathbb{Z}) = GL_n(\mathbb{R})$, поэтому найдется такое подмножество $\Theta \subset \Sigma$, что $\Theta GL_n(\mathbb{Z}) = \Omega GL_n(\mathbb{Z})$. При этом $\Omega(\mathbb{Z}^n \setminus \{0\}) = \Theta(\mathbb{Z}^n \setminus \{0\})$, так что для Θ также выполнены условия а) и б), и *достаточно установить относительную компактность* Θ. Заметим, что условие б) означает, что $\|g(x)\| \geqslant c > 0$ для всех $g \in \Theta$ и всех $\mathbb{Z}^n \setminus \{0\}$, где $\|\ \|$ — евклидова норма в пространстве $\mathbb{R}^n$. В частности, $\|g(e_1)\| = \|a_g(e_1)\| = a_1 \geqslant c$, где $g = k_g a_g u_g$ — разложение Ивасавы элемента $g \in \Theta$ (обозначения — см. в § 4.2), $e_1, \ldots, e_n$ — фиксированный ортонормированный базис пространства $\mathbb{R}^n$. Так как $a_g \in A_t$, то $a_i \geqslant s a_1$ для всех $i = 1, \ldots, n$ и некоторого $s > 0$. Отсюда следует, что все a_i ограничены снизу. С другой стороны, $|\det g| = |\det a_g| = a_1 \ldots a_n$ ограничено сверху, поэтому все a_i ограничены также сверху. Таким образом, мы показали, что a-компоненты a_g элементов $g \in \Theta$ пробегают относительно компактное множество. Так как $\Theta \subset \Sigma$, то отсюда следует относительная компактность Θ. Предложение доказано.

Теперь у нас есть все необходимое для доказательства компактности пространства $H_{\mathbb{R}}/H_{\mathbb{Z}}$. Рассмотрим алгебру Ли $\mathfrak{h} = L(H)$ и присоединенное представление $\rho\colon H \to GL(\mathfrak{h})$. Без ущерба для общности можно считать, что $H_{\mathbb{Z}} = \{h \in H \mid \rho(h) L = L\}$, где $L \subset \mathfrak{h}_{\mathbb{Q}}$ — некоторая решетка. В силу леммы 15 достаточно установить относительную компактность $H_{\mathbb{R}}$ по модулю группы $GL_n(\mathbb{Z})$, $n = \dim \mathfrak{h}$, где $GL_n(\mathbb{Z})$ рассматривается относительно некоторого базиса решетки L. Применим критерий Малера. Так как $\det \rho(H) = 1$, то в проверке нуждается лишь условие б) критерия. Рассмотрим характеристический многочлен

$$\det(t - \operatorname{ad} x) = t^n + \sum_{i=0}^{n-1} f_i(x) t^i,$$

отвечающий присоединенному действию элемента $x \in L$. Так как H анизотропна над $\mathbb{Q}$, то алгебра Ли $\mathfrak{h}_{\mathbb{Q}}$ не содержит нильпотентных элементов, следовательно, все $f_i(x)$ не могут одновременно обратиться в нуль, т. е. $f(x) = \sum f_i^2(x) > 0$. С другой стороны, функции f_i являются многочленами с рациональными коэффициентами от координат x в базисе L. Поэтому $f(x) = (1/d) g(x)$, где $d \in \mathbb{Z}$, $g(x)$ — многочлен с целыми коэффициентами. Так как $g(x) \neq 0$ для $x \in L \setminus \{0\}$, то $|f(L \setminus \{0\})| \geqslant 1/d$. Но для любого $h \in H$ имеем $f_i(x) = f_i(hx)$, следова-

тельно, для любого $h \in H_{\mathbb{R}}$

$$|f(h(L\setminus\{0\}))| = |f(L\setminus\{0\})| \geqslant \frac{1}{d}.$$

Тогда условие $|f(x)| < 1/d$ определяет искомую окрестность U. Доказательство теоремы 12 завершено.

Приведем два примера.

Пример 1. Пусть $G = \boldsymbol{SO}_n(f)$ — специальная ортогональная группа невырожденной квадратичной формы f от n переменных с рациональными коэффициентами. Тогда при $n = 2$ группа G является одномерным тором, а при $n \geqslant 3$ полупроста (см. § 2.3). При этом в силу предложения 2.14 группа G является $\mathbb{Q}$-анизотропной в том и только том случае, если анизотропна форма f. Тем самым из теоремы 12 получаем следующий критерий компактности: пространство $SO_n(f)_{\mathbb{R}}/SO_n(f)_{\mathbb{Z}}$ компактно в том и только том случае, если f не представляет нуля над $\mathbb{Q}$. Полезно сравнить наше доказательство этого факта и доказательство в терминах теории приведения квадратичных форм (см. Бёге [1], Касселс [1]; адельный вариант рассуждений можно найти у Годемана [1]).

Пример 2. Пусть $G = \boldsymbol{SL}_1(D)$, где D — конечномерное центральное тело над $\mathbb{Q}$. Согласно предложению 2.12 группа G является $\mathbb{Q}$-анизотропной, поэтому пространство $G_{\mathbb{R}}/G_{\mathbb{Z}}$ компактно. Доказательство этого факта принадлежит Хей, а его адельный вариант — Фудзисаки.

§ 4.6. Конечность объема факторпространства $G_{\mathbb{R}}/G_{\mathbb{Z}}$

Получение некоторых структурных результатов об арифметических группах (см., в частности, Маргулис [2, 3]) в существенной степени опирается на тот факт, что арифметическая подгруппа полупростой группы G является решеткой в $G_{\mathbb{R}}$, т. е. объем факторпространства $G_{\mathbb{R}}/G_{\mathbb{Z}}$ в мере Хаара конечен. Вряд ли нуждается в комментариях и значение этого результата для развития анализа на $G_{\mathbb{R}}/G_{\mathbb{Z}}$, в частности, для построения теории автоморфных функций (см., например, Борель [6]). Цель этого параграфа — дать критерий конечности объема $G_{\mathbb{R}}/G_{\mathbb{Z}}$ для произвольных алгебраических групп.

Теорема 13. *Пусть G — $\mathbb{Q}$-определенная алгебраическая группа. Пространство $G_{\mathbb{R}}/G_{\mathbb{Z}}$ имеет конечный инвариантный объем в том и только том случае, если связная компонента G^0 не имеет нетривиальных характеров, определенных над $\mathbb{Q}$.*

Этот результат является наиболее техничным во всей главе. Читатель, не желающий разбираться во всех деталях доказательства, может ограничиться рассмотрением случая $G = \boldsymbol{SL}_n$. Согласно следствию из теоремы 4 здесь $G_{\mathbb{R}} = \Sigma^{(1)}_{t,v} G_{\mathbb{Z}}$ $(t \geqslant 2/\sqrt{3}$, $v \geqslant 1/2)$, где $\Sigma^{(1)}_{t,v} = \Sigma_{t,v} \cap G_{\mathbb{R}}$, $\Sigma_{t,v}$ — область Зигеля в $GL_n(\mathbb{R})$.

Так как группа $G_{\mathbb{R}}$ унимодулярна (следствие из теоремы 3.18), то на пространстве $G_{\mathbb{R}}/G_{\mathbb{Z}}$ существует инвариантная мера, и поэтому достаточно установить конечность объема множества $\Sigma^{(1)}_{t,v}$. Для этого воспользуемся выражением для меры Хаара dg группы G, которое вытекает из результатов § 3.5:

$$dg = \rho(a)\, dk\, da\, du,$$

где k, a, u — компоненты разложения Ивасавы элемента g; dk, da и du соответственно меры Хаара на группах $\mathbf{K}_0 = \boldsymbol{SO}_n(\mathbb{R})$, $A_0 = A \cap G$, U (обозначения, связанные с разложением Ивасавы, см. в § 4.2); $\rho(a) = \prod_{i<j} a_i/a_j$, если $a = \operatorname{diag}(a_1, \ldots, a_n)$. Имеем

$$\int\limits_{\Sigma^{(1)}_{t,v}} dg = \int\limits_{\mathbf{K}_0} dk \int\limits_{(A_0)_t} \rho(a)\, da \int\limits_{U_v} du, \quad (A_0)_t = A_t \cap G,$$

причем первый и третий интегралы конечны в силу компактности соответствующих областей интегрирования. Докажем конечность второго интеграла. Прежде всего заметим, что соответствие

$$\operatorname{diag}(a_1, \ldots, a_n) \longmapsto (a_1/a_2,\ a_2/a_3,\ \ldots,\ a_{n-1}/a_n)$$

отождествляет A_0 с группой $(\mathbb{R}^{>0})^{n-1}$, при этом множество $(A_0)_t$ переходит в $\{(x_1, \ldots, x_{n-1}) \in (\mathbb{R}^{>0})^{n-1} \mid x_i \leqslant t \text{ для всех } i\}$. Далее, в терминах координат $x_1, \ldots, x_n$ функция ρ запишется в виде

$$\rho(a) = \prod_{i=1}^{n-1} x_i^{r_i},$$

где r_i — целые положительные числа. Так как (мультипликативная) мера Хаара на $\mathbb{R}^{>0}$ есть dx/x, то имеет место равенство

$$\int\limits_{(A_0)_t} \rho(a)\, da = \int\limits_0^t \ldots \int\limits_0^t \prod_{i=1}^{n-1} x_i^{r_i} \frac{dx_1}{x_1} \ldots \frac{dx_{n-1}}{x_{n-1}} = \prod_{i=1}^{n-1} \int\limits_0^t x_i^{r_i - 1}\, dx_i,$$

причем каждый интеграл $\int\limits_0^t x^{r-1}\, dx = t^r/r$ конечен для $r > 0$. Требуемое доказано.

Для произвольных полупростых групп G ситуация, в общих чертах, вполне аналогична. А именно, так как группа $G_{\mathbb{R}}$ унимодулярна (следствие из теоремы 3.18), то на $G_{\mathbb{R}}/G_{\mathbb{Z}}$ существует инвариантная мера, и для доказательства конечности инвариантного объема $G_{\mathbb{R}}/G_{\mathbb{Z}}$ достаточно найти измеримое подмножество в $G_{\mathbb{R}}$, которое накрывает $G_{\mathbb{R}}/G_{\mathbb{Z}}$ и имеет конечный

объем. Показывается, что построенное в § 4.3 фундаментальное множество в $G_{\mathbb{R}}$ относительно $G_{\mathbb{Z}}$ на самом деле содержится в объединении конечного числа сдвигов подходящей области Зигеля группы $G_{\mathbb{R}}$, а затем устанавливается конечность объема произвольной области Зигеля (отметим, что эта часть рассуждений мало чем отличается от случая группы $\boldsymbol{SL}_n$).

Итак, пусть $G \subset GL_n(\mathbb{C})$ полупростая $\mathbb{Q}$-определенная группа. В § 4.3 мы показали, что в качестве фундаментального множества в $G_{\mathbb{R}}$ относительно $G_{\mathbb{Z}}$ можно взять множество вида $\Omega = \left(\bigcup_b a\Sigma b\right) \cap G_{\mathbb{R}}$, где Σ — некоторая область Зигеля в $GL_n(\mathbb{R})$, b пробегает конечный набор матриц из $GL_n(\mathbb{Z})$, $a \in GL_n(\mathbb{R})$ — такая матрица, что группа $H = a^{-1}Ga$ самосопряжена. Для доказательства теоремы 13 выбор a следует подчинить более жестким ограничениям, а именно, потребовать, чтобы для a выполнялись все условия, перечисленные в предложении 3.14. Ниже мы будем использовать введенные в формулировке этого предложения обозначения. В частности, $S = H \cap D_n$ — максимальный $\mathbb{R}$-разложимый тор в H, $U = H \cap U_n$ — максимальная унипотентная подгруппа. Обозначим также через R систему корней H относительно S, и пусть $\Pi \subset R$ — подсистема простых корней, отвечающая U. Так как $a^{-1}(a\Sigma b \cap G_{\mathbb{R}})a = \Sigma ba \cap H_{\mathbb{R}}$, то конечность объема Ω вытекает из следующего утверждения:

Предложение 9. *Для любой области Зигеля $\Sigma \subset GL_n(\mathbb{R})$ и любого $x \in GL_n(\mathbb{R})$ объем пересечения $\Sigma x \cap H_{\mathbb{R}}$ в мере Хаара группы $H_{\mathbb{R}}$ конечен.*

Доказательство опирается на конструкцию относительных областей Зигеля для группы H. Пусть $H_{\mathbb{R}} = \mathbf{K}^* A^* U^*$ — разложение Ивасавы в группе $H_{\mathbb{R}}$ (см. теорему 3.9), в котором $\mathbf{K}^*$ — максимальная компактная подгруппа в $H_{\mathbb{R}}$, A^* — связная компонента $S_{\mathbb{R}}$, $U^* = U_{\mathbb{R}}$. *Областью Зигеля* $\Sigma^*_{t,\omega}$ группы $H_{\mathbb{R}}$ (где $t > 0$, $\omega \subset U^*$ — компактное подмножество) называется произведение $\mathbf{K}^* A^*_t \omega$, где $A^*_t = \{a \in A^* \mid \alpha(a) \leqslant t$ для всех $\alpha \in \Pi\}$. Ясно, что для группы $G = \boldsymbol{SL}_n$ относительные области Зигеля сводятся к пересечениям $G \cap \Sigma$, где Σ — обычная область Зигеля в $GL_n(\mathbb{R})$. Небольшое рассуждение показывает, что при выполнении наших условий это же имеет место и для H. В самом деле, пусть $h \in \Sigma_{t,v} \cap H$. Тогда разложения Ивасавы элемента h в группах $H_{\mathbb{R}}$ и $GL_n(\mathbb{R})$ совпадают. В силу выполнимости условия (iii) предложения 3.14 простые корни группы H имеют вид $\alpha = d_1\varepsilon_1 + \ldots + d_{n-1}\varepsilon_{n-1}$, где $d_i \geqslant 0$, ε_i — простые корни группы $GL_n(\mathbb{C})$. Поэтому найдется константа $s > 0$ такая, что $\alpha(a_h) \leqslant s$ для всех $h \in \Sigma_{t,v} \cap H_{\mathbb{R}}$ и всех $\alpha \in \Pi$; тогда $\Sigma_{t,v} \cap H_{\mathbb{R}} \subset \Sigma^*_{s,\omega}$, где $\omega = (U_{n\mathbb{R}})_v \cap H_{\mathbb{R}}$. Сходное рассуждение позволяет установить и обратное утверждение (которое нам, впрочем, не понадобится): любая область Зигеля группы H содержится

в подходящей области Зигеля группы $GL_n(\mathbb{R})$. Наиболее технически сложный момент доказательства предложения 9 заключается в доказательстве аналогичного утверждения для сдвигов областей Зигеля.

Предложение 10. *Пусть Σ — область Зигеля в $GL_n(\mathbb{R})$, $x \in GL_n(\mathbb{R})$. Тогда найдутся такая область Зигеля $\Sigma^* \subset H_{\mathbb{R}}$ и такой конечный набор элементов $x_i \in H_{\mathbb{R}}$, что*

$$\Sigma x \cap H_{\mathbb{R}} \subset \bigcup_i \Sigma^* x_i.$$

Для доказательства предложения 9 тогда остается доказать

Предложение 11. *Объем любой области Зигеля $\Sigma^* = \Sigma^*_{t,\omega}$ в мере Хаара группы $H_{\mathbb{R}}$ конечен.*

Доказательство опирается на формулу для меры Хаара группы $H_{\mathbb{R}}$, которая аналогична формуле для группы $SL_n(\mathbb{R})$ и также может быть получена из результатов § 3.5:

$$dh = \rho(a)\, dk^*\, da^*\, du^*,$$

где dk^*, da^*, du^* — меры Хаара соответственно на группах $\mathbf{K}^*$, A^*, U^*, ρ — сумма положительных корней из R. Как и в случае группы $SL_n(\mathbb{R})$, имеем

$$\int_{\Sigma^*} dh = \int_{\mathbf{K}^*} dk^* \int_{A^*_t} \rho(a)\, da^* \int_{\omega} du^*,$$

причем первый и третий интегралы берутся по компактным множествам и, следовательно, конечны. Для вычисления второго интеграла рассмотрим отображение φ: $A^* \to (\mathbb{R}^{>0})^d$, $d = |\Pi|$, определенное формулой $\varphi(a) = (\alpha(a))_{\alpha \in \Pi}$. Нетрудно видеть, что φ является изоморфизмом групп, причем

$$\varphi(A^*_t) = \{(x_1, \ldots, x_d) \in (\mathbb{R}^{>0})^d \mid x_i \leqslant t\}.$$

Кроме того, $\rho = \sum b_\alpha \alpha$, b_α — целые положительные числа. Поэтому имеем

$$\int_{A^*_t} \rho(a)\, da = \prod_{\alpha \in \Pi} \int_0^t x^{b_\alpha - 1}\, dx = \left(\prod_{\alpha \in \Pi} b_\alpha^{-1}\right) t^{\Sigma b_\alpha} < \infty.$$

Предложение 11 доказано.

Переходим к доказательству предложения 10. Вначале установим одно вспомогательное утверждение о сдвигах областей Зигеля в $GL_n(\mathbb{R})$.

Лемма 16. *Пусть Σ — область Зигеля в $GL_n(\mathbb{R})$, $x \in GL_n(\mathbb{R})$. Тогда для любого $s > 0$ пересечение $\Sigma x \cap \mathbf{K} A_s U_{n\mathbb{R}}$ содержится в некоторой области Зигеля группы $GL_n(\mathbb{R})$.*

Доказательство не содержит обращения к группе H и ее подгруппам, поэтому мы, чтобы не усложнять обозначений,

вернемся к обозначениям § 4.2. В частности, вместо $U_{n\mathbb{R}}$ будем писать просто U, $B=AU$. Ясно, что для любого $b\in B$ множества Σb и $(\mathbf{K}A_sU)b$ содержатся соответственно в подходящей области Зигеля и множестве вида $\mathbf{K}A_sU$. Так как любой элемент $x\in GL_n(\mathbb{R})$ допускает разложение Брюа $x=v_x^-wb_x$ ($v_x^-\in U$, $b_x\in B$, $w\in W$), то достаточно доказать утверждение леммы для $x=w\in W$. Пусть π — отвечающая w перестановка индексов $\{1, \ldots, n\}$. Положим $I=\{(i, j)\mid i<j,\ \pi i>\pi j\}$ и обозначим через S тор $\{x=\operatorname{diag}(x_1, \ldots, x_n)\mid x_i=x_j$ для $(i, j)\in I\}$. Пусть F — коммутант централизатора $C_{GL_n}(S)$, $T=D_n\cap F$, $U'=U\cap F$. Положим также $A'=(T_{\mathbb{R}})^0$, $A''=(S_{\mathbb{R}})^0$, $U''=\{u=(u_{ij})\in U\mid u_{ij}=0$ для $(i, j)\in I\}$. Нам понадобится следующий простой факт, доказательство которого читатель может рассматривать как упражнение: морфизм-произведение индуцирует изоморфизм $A'\times A''\xrightarrow{\sim}A$ и гомеоморфизм $U'\times U''\xrightarrow{\sim}U$. Обозначим через δ' и δ'' проекции A на A' и A'' соответственно.

Лемма 17. 1) *w централизует S;*

2) *для любых $s, t>0$ множество $\delta'(wA_tw^{-1}\cap A_s)$ компактно.*

Доказательство. 1) Пусть $\{1, \ldots, n\}=J_1\cup\ldots\cup J_r$ — разложение на непересекающиеся орбиты циклической группы $\langle\pi\rangle$. Тогда множество элементов из D_n, перестановочных с w, есть $\{x=\operatorname{diag}(x_1, \ldots, x_n)\mid x_i=x_j$, если i, j лежат в одной орбите$\}$. Пусть теперь $x=\operatorname{diag}(a_1, \ldots, a_n)\in S$ и J — произвольная орбита. Если $[J]=l$, то без ограничения общности можно предполагать, что $J=\{1, \ldots, l\}$. Пусть $a_1=\ldots=a_{f-1}$, но $a_f\neq a_{f-1}$, $1\leqslant f\leqslant l$. Так как подмножества $\{j\in J\mid j<f\}$ и $\{j\in J\mid j>f\}$ не могут быть инвариантными относительно π, то найдутся $j, k\in J$ такие, что $j<f<k$, $\pi k\leqslant f\leqslant\pi j$; при этом $\pi k<\pi j$. Ясно, что $(j, k)\in I$, поэтому $a_j=a_k$ (см. определение S). Если $\pi(f)>\pi(k)$, то $(f, k)\in I$, откуда $a_f=a_k=a_j$; если же $\pi(f)\leqslant\pi(k)<\pi(j)$, то $(j, f)\in I$ и опять $a_f=a_j$. Итак, во всех случаях $a_f=a_j$, что противоречит нашим построениям, ибо $j<f$.

2) Поскольку A' и A'' инвариантны относительно w, то

$$\delta'(wA_tw^{-1}\cap A_s)=w\delta'(A_t\cap w^{-1}A_sw)w^{-1},$$

поэтому достаточно установить ограниченность $\delta'(A_t\cap w^{-1}A_sw)$. Для этого рассмотрим отображение $\varphi\colon A\to(\mathbb{R}^{>0})^d$, $d=[I]$, определяемое формулой

$$\varphi(\operatorname{diag}(a_1, \ldots, a_n))=(a_i/a_j)_{(i, j)\in I}.$$

По построению $\operatorname{Ker}\varphi=A''$, так что ограничение $\varphi|_{A'}$ задает изоморфизм $A'\xrightarrow{\sim}\varphi(A')$. Поэтому достаточно установить относительную компактность множества $\Phi=\varphi(A_t\cap w^{-1}A_sw)$. Найдутся такие константы $t_0, s_0>0$, что $a_i/a\leqslant t_0$ (соответственно, s_0)

для всех $i<j$ и всех $a=\operatorname{diag}(a_1, \ldots, a_n)\in A_t$ (соотв. A_s). Тогда $\Phi\subset[s_0^{-1}, t_0^{-1}]^d$. В самом деле, по построению $\varphi(A_t)\subset\subset]-\infty, t_0]^d$. Если же $a\in w^{-1}A_s w$, то $waw^{-1}=\operatorname{diag}(a_{\pi^{-1}(1)}, \ldots, a_{\pi^{-1}(n)})\in A_t$. Пусть $(i, j)\in I$, $i'=\pi(i)$, $j'=\pi(j)$. Тогда $i'>j'$, и, значит, $a_i/a_j=a_{\pi^{-1}(i')}/a_{\pi^{-1}(j')}\geqslant s_0^{-1}$, что и требовалось. Лемма 17 доказана.

Завершим доказательство леммы 16. Сразу же отметим, что в доказательстве нуждается лишь ограниченность u-компонент элементов указанного в формулировке леммы пересечения. Пусть $g=kau\in\Sigma$; вычислим a-компоненту элемента gw. Положим $m=aua^{-1}w$, и пусть $m=k_m a_m u_m$ — соответствующее разложение Ивасавы. Тогда имеем

$$gw=kauw=kmw^{-1}aw=(kk_m)\,a_m u_m w^{-1}aw.$$

Так как элемент $w^{-1}aw$ нормализует U, то приравнивая a-компоненты, получим

$$a_{kauw}=a_{aua^{-1}w}w^{-1}aw. \tag{1}$$

Пусть теперь элемент gw пробегает пересечение $\Sigma w\cap \mathbf{K}A_s U$. Тогда из леммы 3 вытекает, что множество $a_{aua^{-1}w}$ относительно компактно. Так как $a_{gw}\in A_s$, то из (1) вытекает, что $w^{-1}aw\in A_{s'}$ для достаточно большого s'. Применяя пункт 2) леммы 17, получаем, что $\delta'(a)$ ограничено. Пусть $u=u'u''$, где $u'\in U'$, $u''\in U''$. Тогда имеем

$$gw=k\delta'(a)\,\delta''(a)\,u'u''w=(kw)\,(w^{-1}\delta'(a)\,u'w)\,\delta''(a)\,w^{-1}u''w.$$

Заметим теперь, что так как $F=[C_{GL_n}(S), C_{GL_n}(S)]$, а w перестановочно с S, то $w^{-1}Fw=H$, откуда $h=w^{-1}\delta'(a)\,u'w\in F_{\mathbf{R}}$. Тогда компоненты разложения Ивасавы $h=k_h a_h u_h$ также лежат в $F_{\mathbf{R}}$. Действительно, легко проверить, что если $c=\operatorname{diag}(\varepsilon_1, \ldots, \varepsilon_n)$, где $\varepsilon_i=\pm 1$, Z_c — централизатор c в GL_n и $h\in(Z_c)_{\mathbf{R}}$, то компоненты разложения Ивасавы элемента h также лежат в $(Z_c)_{\mathbf{R}}$. С другой стороны, F можно представить в виде $F=\bigcap_c Z_c$, где c пробегает подходящий набор элементов указанного вида. Учитывая это обстоятельство, продолжим вычисления:

$$gw=(kw)\,h\delta''(a)\,w^{-1}u''w=(kwk_h)\,(a_h\delta''(a))\,(u_h w^{-1}u''w).$$

Из сказанного выше вытекает, что элемент h пробегает относительно компактное множество, поэтому его компоненты и, в частности, u_h также пробегают относительный компакт. Так как $g\in\Sigma$, то компонента u'' также ограничена. Отсюда следует

ограниченность выражения $u_h w^{-1} u'' w$. Остается заметить, что из определения U'' вытекает, что $w^{-1} U'' w \subset U$, так что $u_h w^{-1} u'' w$ есть в точности u-компонента элемента gw. Лемма 16 доказана.

Нам понадобится еще обобщение на произвольные группы следующего замечания. Пусть $a \in A$; тогда для подходящего $w \in W$ имеем $w^{-1} a w \in A_1 (= A_t$ при $t = 1)$. Иными словами,

$$A = \bigcup_{w \in W} (w^{-1} A_1 w).$$

В самом деле, пусть $a = \operatorname{diag}(a_1, \ldots, a_n)$. Элементы a_i можно упорядочить: $a_{i_1} \leqslant \ldots \leqslant a_{i_n}$. Обозначим через π перестановку $\begin{pmatrix} 1 & \ldots & n \\ i_1 & \ldots & i_n \end{pmatrix}$, и пусть w — соответствующий элемент группы W. Тогда

$$w^{-1} a w = \operatorname{diag}(a_{i_1}, \ldots, a_{i_n}) \in A_1.$$

Чтобы обобщить этот факт применительно к группе H (мы возвращаемся к обозначениям, введенным в начале параграфа), напомним, что относительная группа Вейля W^* группы H определяется как факторгруппа $N_H(S)/C_H(S)$, где $N_H(S)$ (соответственно, $C_H(S)$) — нормализатор (соответственно, централизатор) S в H; при этом представители всех классов группы W^* могут быть выбраны из $N_H(S)_{\mathbf{R}}$, так что в действительности $W^* = N_H(S)_{\mathbf{R}}/C_H(S)_{\mathbf{R}}$. Отметим также, что имеется естественное действие W^* на S, задаваемое сопряжением.

Лемма 18. 1) *Представители всех классов группы W^* можно выбрать из максимальной компактной подгруппы* $\mathbf{K}^*$.

2) $A^* = \bigcup_{w \in W^*} w^{-1} A_1^* w$.

Доказательство. 1) Пусть $x \in N_H(S)_{\mathbf{R}}$ и $x = kau \in \mathbf{K}^* A^* U^*$ — его разложение Ивасавы. Тогда для любого $b \in S$ имеем

$$k^{-1} b k = (au) \bar{b} (au)^{-1},$$

где $\bar{b} = x^{-1} b x \in S$. Но $k^{-1} = {}^t k$, так что матрица $k^{-1} b k = {}^t k b k$ является симметричной. С другой стороны, матрица $(au)\bar{b}(au)^{-1}$ верхняя треугольная. Поэтому на самом деле матрица $(au)\bar{b}(au)^{-1}$ является диагональной и $au \in N_H(S)$. Так как централизатор любого тора в связной разрешимой группе совпадает с его нормализатором (см. Борель [8]), то в действительности $au \in C_H(S)$. Отсюда следует, что x и k представляют один и тот же класс в W^*.

2) Пусть $a \in A^*$. Положим $P = \{\alpha \in R \mid \alpha(a) \geqslant 1\}$. Легко видеть, что если $\alpha, \beta \in P$ и $\alpha + \beta \in R$, то $\alpha + \beta \in P$; кроме того, $P \cup (-P) = R$. Тем самым множество P параболично в терминологии Бурбаки [4] (см. гл. VI, § 1, п. 7) и поэтому содержит некоторую подсистему простых корней Π' системы R. Так как

группа Вейля W^* естественно изоморфна группе Вейля $W(R)$ системы корней R, а последняя однотранзитивно действует на подсистемах простых корней, то найдется такой $\tilde{w} \in W(R)$, что $\tilde{w}\Pi' = \Pi$, откуда $\tilde{w}P \supset \Pi$. Тогда если w — отвечающий $\tilde{w}$ элемент группы W^*, то $\alpha(w^{-1}aw) \leqslant 1$ для всех $\alpha \in \Pi$, т. е. $w^{-1}aw \in \in A_1$. Лемма 18 доказана.

Поясним ход дальнейших рассуждений. Пусть $y = zx \in \in \Sigma x \cap H_{\mathbb{R}}$, $y = k_1 a_1 u_1$ — соответствующее разложение Ивасавы. Согласно лемме 18 можно найти элемент $w \in N_{H_{\mathbb{R}}}(A^*) \cap \mathbf{K}^*$ со свойством $w^{-1}a_1 w \in A_1^*$. Тогда $w^{-1}a_1 w \in A_1$ — это вытекает из того, что по построению для любого $i = 1, \ldots, n-1$ ограничение ε_i на S положительно, т. е. $\varepsilon_i = \sum_{\alpha \in \Pi} c_\alpha^i \cdot \alpha$, где $c_\alpha^i \geqslant 0$. Далее, при доказательстве леммы 16 мы установили (равенство (1)), что

$$a_{yw} = a_{a_1 u_1 a_1^{-1} w} w^{-1} a_1 w.$$

Если показать, что элементы вида $a_1 u_1 a_1^{-1}$ образуют относительно компактное множество, то из этой формулы получим включение $a_{yw} \in A_s$ для достаточно большого s, т. е.

$$yw \in \mathbf{K} A_s (U_n)_{\mathbb{R}} \cap \Sigma x w.$$

Из леммы 16 вытекает существование такой области Зигеля Σ_1 группы $GL_n(\mathbb{R})$, что $\mathbf{K} A_1 (U_n)_{\mathbb{R}} \cap \Sigma x w \subset \Sigma_1$; тогда $\Sigma_1 \cap H_{\mathbb{R}} \subset \Sigma^*$ для подходящей области Зигеля Σ^* группы $H_{\mathbb{R}}$. Окончательно имеем $yw \in \Sigma^*$, т. е.

$$\Sigma x \cap H_{\mathbb{R}} \subset \bigcup_w \Sigma^* w^{-1},$$

где Σ^* — достаточно большая область Зигеля группы H, w пробегает некоторую систему представителей классов группы W^*, лежащую в $\mathbf{K}^*$.

Прежде чем доказывать ограниченность множества элементов вида $a_1 u_1 a_1^{-1}$, проведем редукцию доказательства предложения 10 к элементам x более специального вида. Во-первых, пусть $x = bwu$ — «перевернутое» разложение Брюа элемента x, где b — верхняя треугольная матрица, u — верхняя унипотентная матрица, $w \in W$. Так как Σb содержится в некоторой большей области Зигеля группы $GL_n(\mathbb{R})$, то можно считать, что $b = 1$, т. е. $x = wu$. Далее, согласно лемме 2.1 найдется такое замкнутое по Зарисскому $\mathbb{R}$-определенное множество $P \subset U_n$, инвариантное относительно присоединенного действия S, что морфизм-произведение индуцирует $\mathbb{R}$-определенные изоморфизмы $P \times U \xrightarrow{\sim} U_n$ и $U \times P \xrightarrow{\sim} U_n$. Представим u в виде $u = pv$, где

$p \in P_{\mathbb{R}}$, $v \in U_{\mathbb{R}}$. Если мы покажем, что $\Sigma wp \cap H_{\mathbb{R}} \subset \bigcup_i \Sigma^* x_i$, то $\Sigma x \cap H_{\mathbb{R}} \subset \bigcup_i \Sigma x_i v$. Таким образом, можно предполагать, что $x = wp$, $p \in P_{\mathbb{R}}$. Для элементов x такого вида мы докажем ограниченность множества $\{a_1 u_1 a_1^{-1} \mid y = k_1 a_1 u_1 \in \Sigma x \cap H_{\mathbb{R}}\}$, что и завершит доказательство предложения 10.

Итак, пусть $y = zx \in \Sigma x \cap H_{\mathbb{R}}$; $z = kau$, $y = k_1 a_1 u_1$ — соответствующие разложения Ивасавы. Выразим a_1, u_1 через a, u и воспользуемся тем обстоятельством, что z берется из области Зигеля Σ. Имеем

$$y = (kau)\, wp = (kw)\,(w^{-1}aua^{-1}w)\,(w^{-1}aw)\, p. \tag{2}$$

Если положить $c = w^{-1}aua^{-1}w$, взять разложение Ивасавы $c = k_c a_c u_c$ и подставить в (2), то мы получим

$$y = (kwk_c)\, a_c u_c w^{-1} awp = (kwk_c)\,(a_c w^{-1} aw)\,((w^{-1}aw)^{-1} u_c (w^{-1}aw))\, p,$$

откуда

$$a_1 = a_c w^{-1} aw,$$
$$u_1 = (w^{-1}aw)^{-1} u_c (w^{-1}aw)\, p.$$

Поэтому

$$a_1 u_1 p^{-1} a_1^{-1} = (a_1 u_1 a_1^{-1})\,(a_1 p^{-1} a_1^{-1}) = a_c u_c a_c^{-1}.$$

Так как элемент z выбирался из области Зигеля, то согласно лемме 3 элементы вида aua^{-1} образуют относительно компактное множество. Отсюда следует ограниченность множества $\{c\}$ и, следовательно, множества $\{a_c u_c a_c^{-1}\}$. Чтобы получить теперь ограниченность множества $\{a_1 u_1 a_1^{-1}\}$, остается заметить, что $a_1 u_1 a_1^{-1}$ является проекцией $a_c u_c a_c^{-1}$ на $U_{\mathbb{R}}$ относительно изоморфизма $U_{\mathbb{R}} \times P_{\mathbb{R}} \xrightarrow{\sim} (U_n)_{\mathbb{R}}$. Доказательство предложения 10 завершено.

Таким образом, нами доказана

Теорема 14. *Пусть G — полупростая $\mathbb{Q}$-определенная группа, $\Gamma \subset G_{\mathbb{R}}$ — ее арифметическая подгруппа. Тогда факторпространство $G_{\mathbb{R}}/\Gamma$ имеет конечный инвариантный объем. Другими словами, Γ является решеткой в $G_{\mathbb{R}}$.*

(Напомним, что *решеткой* в локально компактной топологической группе G называется такая дискретная подгруппа $\Gamma \subset G$, что факторпространство G/Γ имеет конечный инвариантный объем.)

Из теоремы 14 немедленно вытекает другое доказательство бесконечности арифметических подгрупп полупростых алгебраических $\mathbb{Q}$-групп G с некомпактной группой $G_{\mathbb{R}}$ (следствие 2 из теоремы 11). В самом деле, если группа $G_{\mathbb{R}}$ некомпактна, то ее объем в мере Хаара бесконечен. Отсюда следует, что для

любой конечной подгруппы $\Gamma \subset G_{\mathbf{R}}$ объем $G_{\mathbf{R}}/\Gamma$ также бесконечен. С другой стороны, для арифметической подгруппы Γ этот объем обязан быть конечным.

Доказательство теоремы 13 получается из теоремы 14 путем несложных рассуждений. А именно, группу G можно с самого начала считать связной. Если G является тором, то факторпространство $G_{\mathbf{R}}/G_{\mathbf{Z}}$ является группой, и поэтому конечность его объема равносильна компактности (предложение 3.23). Последнее же имеет место тогда и только тогда, когда тор G является $\mathbf{Q}$-анизотропным, т. е. $\mathbf{X}(G)_{\mathbf{Q}} = 1$ (теорема 11). Таким образом, в данном случае теорема 13 выполняется. Пусть теперь G — произвольная редуктивная группа. Представим G в виде почти прямого произведения $G = FS$, где F — полупростая $\mathbf{Q}$-группа, S — максимальный центральный тор в G, и заметим, что условие $\mathbf{X}(G)_{\mathbf{Q}} = 1$ равносильно $\mathbf{Q}$-анизотропности S. Положим $H = F \times S$ и рассмотрим изогению φ: $H \to G$. Тогда группа $H_{\mathbf{R}} = F_{\mathbf{R}} \times S_{\mathbf{R}}$, очевидно, унимодулярна, поэтому из конечности индекса $[G_{\mathbf{R}}: \varphi(H_{\mathbf{R}})]$ вытекает унимодулярность $G_{\mathbf{R}}$. Если принять еще во внимание конечность $\operatorname{Ker}\varphi$ и арифметичность $\varphi(H_{\mathbf{Z}})$, то легко показать, что пространства $G_{\mathbf{R}}/G_{\mathbf{Z}}$ и $H_{\mathbf{R}}/H_{\mathbf{Z}}$ одновременно имеют конечный или бесконечный объем. В силу теоремы 14 объем пространства $F_{\mathbf{R}}/F_{\mathbf{Z}}$ конечен, поэтому конечность объема $H_{\mathbf{R}}/H_{\mathbf{Z}}$ равносильна конечности объема $S_{\mathbf{R}}/S_{\mathbf{Z}}$, что, как мы видели, также сводится к $\mathbf{Q}$-анизотропности S.

Случай произвольной связной группы G сводится, как обычно, к редуктивному случаю путем рассмотрения разложения Леви $G = HU$, где U — унипотентный радикал G, а группа H редуктивна. Тогда $G_{\mathbf{R}} = H_{\mathbf{R}}U_{\mathbf{R}}$ — полупрямое произведение, и поэтому мера Хаара dg группы $G_{\mathbf{R}}$ представляется в виде прямого произведения $dg = dh\,du$ мер Хаара dh и du на группах $H_{\mathbf{R}}$ и $U_{\mathbf{R}}$ соответственно (см. Бурбаки [3], гл. VII, § 11, предложение 14). В силу леммы 7 в $G_{\mathbf{R}}$ относительно $G_{\mathbf{Z}}$ имеется фундаментальное множество Ω вида $\Omega = \Sigma\Phi$, где Σ — фундаментальное множество в $H_{\mathbf{R}}$ относительно $H_{\mathbf{Z}}$, Φ — некоторое компактное подмножество в $U_{\mathbf{R}}$; ясно, что Ω имеет конечный объем в том и только том случае, если это имеет место для Σ. С другой стороны, из результатов § 3.5 вытекает, что существование инвариантной меры на пространстве $G_{\mathbf{R}}/G_{\mathbf{Z}}$, относительно которой оно имеет конечный объем, равносильно унимодулярности $G_{\mathbf{R}}$ и существованию относительно $G_{\mathbf{Z}}$ фундаментального множества $F \subset G_{\mathbf{R}}$ конечного объема, и тогда любое фундаментальное множество также имеет конечный объем. Поэтому, если $\mathbf{X}(G)_{\mathbf{Q}} \neq 1$, то $\mathbf{X}(H)_{\mathbf{Q}} \neq 1$, и из рассмотрения редуктивного случая вытекает, что Σ имеет бесконечный объем. Тогда объем Ω также бесконечен, и, значит, объем $G_{\mathbf{R}}/G_{\mathbf{Z}}$ не может быть конечным. Обратно, если $\mathbf{X}(G)_{\mathbf{Q}} = 1$, то $\mathbf{X}(H)_{\mathbf{Q}} = 1$,

следовательно, объемы Σ и Ω конечны. Таким образом, остается показать, что в этом случае группа $G_{\mathbb{R}}$ унимодулярна. Но это доказывается точно так же, как и следствие из теоремы 3.18. В самом деле, пусть ω — левоинвариантная $\mathbb{Q}$-определенная рациональная дифференциальная форма на G степени $n = \dim G$. Тогда, как мы видели при доказательстве указанного следствия, имеет место соотношение $\rho_g^*(\omega) = \chi(g)\,\omega$, где ρ_g — правый сдвиг на элемент $g \in G$, χ — некоторый характер группы G. Поскольку ω определена над $\mathbb{Q}$, то нетрудно видеть, что характер χ также определен над $\mathbb{Q}$. Поэтому в нашей ситуации $\chi = 1$, т. е. форма ω является также правоинвариантной, и следовательно, группа $G_{\mathbb{R}}$ унимодулярна в силу теоремы 3.18. Теорема 13 полностью доказана.

В тех случаях, когда объем факторпространства $G_{\mathbb{R}}/G_{\mathbb{Z}}$ конечен, естественно возникает задача его явного вычисления в терминах некоторой канонической меры Хаара. Как мы увидим в следующей главе, этот вопрос тесно связан с вычислением так называемых чисел Тамагавы. Для норменного тора $S = \mathbf{R}^{(1)}_{K/\mathbb{Q}}(\boldsymbol{G}_m)$ значение $\mu(S_{\mathbb{R}}/S_{\mathbb{Z}})$ выражается через дискриминант и регулятор поля K (меру Хаара следует нормализовать таким образом, чтобы объем $K_\infty/\mathcal{O}$, где $K_\infty = K \otimes_{\mathbb{Q}} \mathbb{R}$, $\mathcal{O}$ — кольцо целых в K, равнялся единице, см. Ленг [2]).

Для полупростой односвязной $\mathbb{Q}$-разложимой группы G объем $G_{\mathbb{R}}/G_{\mathbb{Z}}$ является произведением значений ζ-функции в некоторых целых точках (см. статью Ленглендса в сборнике «Арифметические группы и автоморфные функции»). Эти примеры позволяют утверждать, что задача вычисления объема $G_{\mathbb{R}}/G_{\mathbb{Z}}$ представляет значительный арифметический интерес. С другой стороны, как показывает работа Ленглендса, ее решение связано с использованием сложной арифметической техники (скажем, теории рядов Эйзенштейна). Поэтому в настоящей книге мы ограничимся одним примером, где вычисления могут быть проведены в явной форме.

Пример. Пусть $G = \boldsymbol{SL}_2$. Разложение Ивасавы позволяет определить систему координат φ, a, u на группе $G_{\mathbb{R}} = SL_2(\mathbb{R})$ таким образом, чтобы координаты, отвечающие матрице $x \in G_{\mathbb{R}}$, получались из соотношения

$$x = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}.$$

В § 3.5 (см. пример 3) мы показали, что относительно этих координат мера Хаара на $G_{\mathbb{R}}$ может быть записана в виде $a\,d\varphi\,da\,du$. Поэтому объем $G_{\mathbb{R}}/G_{\mathbb{Z}}$ выражается интегралом $\int_F a\,d\varphi\,da\,du$, где $F \subset G_{\mathbb{R}}$ — измеримая фундаментальная область относительно $G_{\mathbb{Z}}$. Построим фундаментальную область, удовле-

творяющую условиям 1), 2) в (3), § 3.5. Для этого вернемся к рассмотрениям § 4.2 и снова рассмотрим проекцию $SL_2(\mathbb{R})$ на верхнюю полуплоскость $P = SO_2(\mathbb{R})\backslash SL_2(\mathbb{R})$ комплексной плоскости, задаваемую формулой ψ: $\begin{pmatrix} x & y \\ u & t \end{pmatrix} \longmapsto \frac{ti+y}{ui+x}$. Далее, рассмотрим замкнутую область $\bar{D} = \{z \in P \mid |\operatorname{Re} z| \leqslant 1/2,\ |z| \geqslant 1\}$, которая, как мы показали в § 4.2, является фундаментальной областью для естественного действия группы $PSL_2(\mathbb{Z})$ на P. Тогда легко видеть, что в качестве F можно взять множество $F = \mathbf{K}_0 D_0$, где

$$\mathbf{K}_0 = \left\{\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \middle| \varphi \in [0,\ \pi]\right\},$$

$$D_0 = \left\{\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \middle| (a,\ u) \in \Omega\right\},$$

$$\Omega = \left\{(a,\ u) \in \mathbb{R}^{>0} \times \mathbb{R} \mid \psi\begin{pmatrix} a & au \\ 0 & a^{-1} \end{pmatrix} \in \bar{D}\right\}.$$

Поэтому объем $G_{\mathbb{R}}/G_{\mathbb{Z}}$ относительно указанной меры равен $\int\limits_0^{\pi} d\varphi \int\limits_{\Omega} a\,da\,du$. Прямое вычисление показывает, что $\Omega = \left\{(a,\ u) \in \mathbb{R}^{>0} \times \mathbb{R} \,\middle|\, |u| \leqslant 1/2,\ 0 \leqslant a \leqslant \frac{1}{\sqrt[4]{1-u^2}}\right\}$, и тогда

$$\operatorname{vol}(G_{\mathbb{R}}/G_{\mathbb{Z}}) = \int\limits_0^{\pi} d\varphi \int\limits_{\Omega} a\,da\,du = \int\limits_0^{\pi} d\varphi \int\limits_{-1/2}^{1/2} du \int\limits_0^{\frac{1}{\sqrt[4]{1-u^2}}} a\,da = \frac{\pi^2}{6}.$$

(Заметим, что это число совпадает со значением $\zeta(2)$ дзета-функции Римана, см. Серр [8].)

§ 4.7. Заключительные замечания по теории приведения

Мы уже выполнили намеченную программу построения теории приведения для арифметических подгрупп алгебраических групп. Тем не менее ряд интересных концепций, не имеющих прямого отношения к темам, которые мы избрали для детального освещения в книге, остался вне нашего внимания. Настоящий параграф призван в какой-то степени ликвидировать этот пробел. Здесь мы собрали (без доказательств) ряд дополнительных сведений по теории приведения (другую конструкцию фундаментальных множеств, связь с теорией приведения квадратичных форм и т. д.), а также переформулировку полученных результатов для $\mathcal{O}$-арифметических подгрупп.

Конструкция фундаментальных множеств из § 4.3 связана, главным образом, со свойствами группы $G_{\mathbb{R}}$ и сравнительно мало-

зависит от групп $G_{\mathbb{Q}}$ и $G_{\mathbb{Z}}$. Однако основываясь на этой конструкции, можно указать другую, вообще говоря, лучшую конструкцию, которая существенным образом использует $\mathbb{Q}$-структуру группы G. Ее преимущества проявляются, например, при построении теории автоморфных функций, ибо соответствующие выходы на бесконечность устроены более или менее так же, как и фундаментальные области фуксовых групп в верхней полуплоскости при приближении к параболическим точкам. Эта конструкция дает также ключ к построению компактификации пространства $G_{\mathbb{R}}/G_{\mathbb{Z}}$, что является основным моментом при изучении когомологий арифметических групп.

Итак, пусть G — полупростая $\mathbb{Q}$-определенная алгебраическая группа. Если G анизотропна над $\mathbb{Q}$, то ситуацию можно считать идеальной: пространство $G_{\mathbb{R}}/G_{\mathbb{Z}}$ компактно (теорема 12), в силу чего для группы $G_{\mathbb{Z}}$ существует компактное фундаментальное множество. Пусть теперь G изотропна над $\mathbb{Q}$, $S \subset G$ — максимальный $\mathbb{Q}$-разложимый тор и P — содержащая S минимальная $\mathbb{Q}$-определенная параболическая подгруппа. Хорошо известно, что P является полупрямым произведением своего унипотентного радикала U на централизатор $Z_G(S)$ тора S. В свою очередь, $Z_G(S)$ записывается в виде почти прямого произведения

$$Z_G(S) = M \cdot S, \tag{1}$$

в $Z_G(S)$. Обозначим через $\mathbf{K}$ максимальную компактную подгруппу группы $G_{\mathbb{R}}$ и пусть A — связная компонента группы $S_{\mathbb{R}}$. Тогда $G_{\mathbb{R}} = \mathbf{K} \cdot P_{\mathbb{R}}$, так что из (1) получаем следующее разложение для группы $G_{\mathbb{R}}$:

$$G_{\mathbb{R}} = \mathbf{K} M_{\mathbb{R}} A U_{\mathbb{R}}$$

где M — наибольшая связная $\mathbb{Q}$-анизотропная подгруппа (заметим, что это разложение, как правило, не является однозначным). Так как пространство $M_{\mathbb{R}}/M_{\mathbb{Z}}$ компактно, то имеет смысл поискать фундаментальное множество относительно $G_{\mathbb{Z}}$ в виде так называемой обобщенной области Зигеля

$$\Sigma_{t,\,y,\,w} = \mathbf{K} y A_t w, \quad t > 0,$$

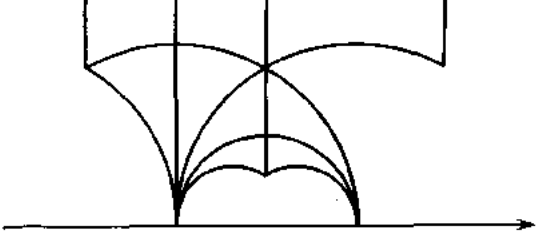
где y (соотв. w) компактное подмножество в $M_{\mathbb{R}}$ (соответственно $U_{\mathbb{R}}$), $A_t = \{a \in A \mid \alpha(a) \leqslant t$ для всех $\alpha \in \Pi\}$, Π — система простых корней группы G относительно тора S, ассоциированная с P.

Теорема 15. *Пусть G — полупростая $\mathbb{Q}$-определенная алгебраическая группа, $\Gamma \subset G_{\mathbb{Q}}$ — ее арифметическая подгруппа.*

1) *Существуют обобщенная область Зигеля $\Sigma = \Sigma_{t,\,y,\,w}$ и конечное подмножество $C \subset G_{\mathbb{Q}}$ такие, что $\Omega = \Sigma C$ является фундаментальным множеством для Γ в $G_{\mathbb{R}}$. Множество C содержит тогда по крайней мере один представитель каждого двойного класса смежности $\Gamma \backslash G_{\mathbb{Q}}/P_{\mathbb{Q}}$ (в частности, число таких двойных классов конечно).*

2) *Обратно, если C — конечное подмножество в $G_{\mathbb{Q}}$, содержащее представитель каждого класса смежности $P_{\mathbb{Q}}\backslash C_{\mathbb{Q}}/\Gamma$, то существует область Зигеля Σ такая, что $\Omega = \Sigma C$ является фундаментальным множеством в $G_{\mathbb{R}}$ относительно* Γ.

Доказательство — см. Борель [6], § 12 и 14. Отметим только, что доказательство п. 1) использует конструкцию фундаментального множества из § 4.3 и в общих чертах сходно с доказательством предложения 10. Нетрудно показать, что обобщенная область Зигеля имеет конечный объем в мере Хаара группы $G_{\mathbb{R}}$, так что утверждение 1) теоремы 15 позволяет получить другое доказательство теоремы 14. Благодаря теореме 15 в теорию входит новый инвариант — число двойных классов $P_{\mathbb{Q}}\backslash G_{\mathbb{Q}}/\Gamma$. Получается, что это число совпадает с минимальным количеством сдвигов обобщенных областей Зигеля группы G, которые в объединении дают фундаментальное множество для группы Γ. Для группы $G = \boldsymbol{SL}_2$ имеем $P = \left\{\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \middle| \, a \in \mathbb{C}^*, b \in \mathbb{C}\right\}$, так что $P_{\mathbb{R}}$ совпадает со стабилизатором бесконечно удаленной точки ∞ при естественном «левом» действии группы $SL_2(\mathbb{R})$ на верхней полуплоскости $\mathscr{P}$ (см. § 4.2). Тогда орбита $SL_2(\mathbb{Q})(\infty)$ есть множество параболических точек, которое совпадает с объединением $\{\infty\}$ и множества точек вещественной оси с рациональными координатами. Число двойных классов $P_{\mathbb{Q}}\backslash G_{\mathbb{Q}}/\Gamma$ в данном случае есть число классов эквивалентности параболических точек относительно Γ. Это число оказывается равным числу точек, которые нужно добавить к факторпространству $\mathscr{P}/\Gamma$ для получения его компактификации, или же числу выходов («вершин») соответствующей фундаментальной области на бесконечность (см. рис. для случая, когда Γ совпадает с конгруэнц-подгруппой $SL_2(\mathbb{Z}, 2)$; здесь имеется 3



вершины). В общем случае дополнения к компактным подмножествам в области Зигеля $\Sigma_{t,y,w}$ имеют вид $\Sigma_{s,y,w}$, где s достаточно мало, и их можно рассматривать как аналог «вершины» в случае группы SL_2. Тогда число двойных смежных классов $\Gamma\backslash G_{\mathbb{Q}}/P_{\mathbb{Q}}$ также получает интерпретацию как минимальное число вершин фундаментальной области для Γ. Отметим, что в следующей главе мы дадим адельную интерпретацию числа классов $\Gamma\backslash G_{\mathbb{Q}}/P_{\mathbb{Q}}$. Отсюда, в частности, будет вытекать другое доказательство его конечности и связь с числом классов группы P.

Обобщенные области Зигеля обладают свойством функториальности: если $f\colon G\to H$ определенный над $\mathbb{Q}$ морфизм полупростых $\mathbb{Q}$-определенных групп и Σ — обобщенная область Зигеля в группе G, то $f(\Sigma)$ содержится в подходящей обобщенной области Зигеля группы H. Отсюда следует, что теорема 15 доставляет конструкцию фундаментальных множеств Ω, которые удовлетворяют следующему усилению условия (F2) из определения фундаментальной области.

$(\mathrm{F2})_{\mathrm{bis}}$ для любых $x,\ y\in C(\Gamma)_{\mathbb{R}}$, где $C(\Gamma)$ — подгруппа соизмеримости Γ, пересечение $\Omega^{-1}\Omega\cap x\Gamma y$ конечно.

В самом деле, достаточно показать, что для произвольной обобщенной области Зигеля Σ пересечение $\Sigma^{-1}\Sigma\cap x\Gamma y$ конечно. Для этого воспользуемся описанием $C(\Gamma)$, полученным в предложении 6: $C(\Gamma)=\pi^{-1}((G/N)_{\mathbb{Q}})$, где N — наибольший $\mathbb{Q}$-определенный нормальный делитель в G компактного типа, $\pi\colon G\to G/N$ — каноническая проекция. Пусть $\tilde{\Sigma}$ — такая область Зигеля группы G/N, что $\pi(\Sigma)\subset\tilde{\Sigma}$. Тогда $\pi(\Sigma^{-1}\Sigma\cap x\Gamma y)\subset\tilde{\Sigma}^{-1}\tilde{\Sigma}\cap\pi(x)\pi(\Gamma)\pi(y)$. Но $\pi(x),\ \pi(y)\in(G/N)_{\mathbb{Q}}$ и $\pi(\Gamma)$ — арифметическая подгруппа в G/N, поэтому из того, что $\tilde{\Sigma}$ удовлетворяет обычному условию (F2) (см. Борель [6], § 14), вытекает конечность последнего пересечения. Остается заметить, что в силу компактности $N_{\mathbb{R}}$ пересечение $\Gamma\cap N$ конечно, так что из конечности множества $\pi(\Sigma^{-1}\Sigma\cap x\Gamma y)$ следует конечность искомого множества $\Sigma^{-1}\Sigma\cap x\Gamma y$.

Фундаментальные множества из теоремы 15 обладают еще одним замечательным свойством. Перед тем как привести его формулировку в общем виде, напомним один из существенных моментов построения теории приведения для группы $GL_n(\mathbb{R})$ (см. § 4.2). Зафиксировав ортонормированный базис $e_1,\ \ldots,\ e_n$ пространства $\mathbb{R}^n$, мы ввели непрерывную функцию $\Phi\colon GL_n(\mathbb{R})\to\mathbb{R}^{>0}$, положив $\Phi(g)=\|ge_1\|$. Тогда множество значений Φ на любом смежном классе $gGL_n(\mathbb{Z})$ ограничено снизу, и минимальное значение принимается в некоторой точке множества $\Sigma=\Sigma_{2/\sqrt{3},\ 1/2}$, откуда $GL_n(\mathbb{R})=\Sigma\,GL_n(\mathbb{Z})$. Оказывается, что аналогичные принципы минимума выполняются для каждой по-

лупростой $\mathbb{Q}$-определенной алгебраической группы G. При описании конструкции соответствующих функций φ сохраним введенные выше обозначения. Пусть π: $G \to GL(V)$ — определенное над $\mathbb{Q}$ абсолютно неприводимое представление группы G такое, что существует вектор $v \in V_{\mathbb{Q}}$, собственный относительно P. Тогда положим $\varphi_\pi(g) = \|\pi(g)v\|$, где норма берется относительно ортонормированного базиса пространства $V_{\mathbb{R}}$, состоящего из собственных относительно S векторов. Частным случаем функций вида φ_π являются функции Φ_i из § 4.2, которые отвечают фундаментальным представлениям группы $\boldsymbol{SL}_n$.

Теорема 16. *Пусть G — полупростая $\mathbb{Q}$-определенная алгебраическая группа, $\varphi = \varphi_\pi$ — функция, отвечающая абсолютно неприводимому $\mathbb{Q}$-определенному представлению π: $G \to GL(V)$, и C — множество представителей двойных смежных классов $\Gamma \backslash G_{\mathbb{Q}}/P_{\mathbb{Q}}$, где $\Gamma \subset G_{\mathbb{Q}}$ — арифметическая подгруппа. Тогда существует такая обобщенная область Зигеля $\Sigma \subset G_{\mathbb{R}}$, что для любого $x \in G_{\mathbb{R}}$ функция φ достигает минимума на множестве $x\Gamma C$ в некоторой точке множества $x\Gamma C \cap \Sigma$. Отсюда выводим, что $G_{\mathbb{R}} = \Sigma C^{-1}\Gamma$.*

Отметим, что любая полупростая $\mathbb{Q}$-определенная группа G обладает достаточным запасом представлений π с описанными выше свойствами. Более того, как известно, любое абсолютно неприводимое представление определяется своим старшим весом, причем любой доминантный вес реализуется в качестве старшего веса некоторого представления (см. Хамфри [1]). При этом оказывается, что подходящее кратное любого доминантного веса реализуется в качестве старшего веса $\mathbb{Q}$-определенного представления, удовлетворяющего описанным требованиям.

Функции φ_π обладают теми же свойствами, что и функции Φ_i из § 4.2. Опираясь на них, можно доказать в нашей ситуации аналог теоремы Хариш-Чандры, а следовательно, и свойство (F2) из определения фундаментальной области. Подробности см. в Борель [6], § 13—14.

Всюду в этой главе мы рассматривали $\mathbb{Q}$-определенные алгебраические группы, однако полученные результаты можно распространить на алгебраические группы, определенные над произвольным полем алгебраических чисел K. Пусть $\mathcal{O}$ — кольцо целых поля K. Тогда $\mathcal{O}$-арифметическими подгруппами в G называются подгруппы в G, соизмеримые с группой $G_{\mathcal{O}}$ точек группы G над кольцом $\mathcal{O}$. Группа $G_{\mathcal{O}}$ является дискретной подгруппой группы $G_\infty = \prod_{v \in V_\infty^K} G_{K_v}$, которая является аналогом группы вещественных точек для $\mathbb{Q}$-определенных групп. Возникает задача построения теории приведения для группы G_∞ относительно $G_{\mathcal{O}}$. Основные результаты, которые получаются

в этом направлении, мы сформулируем в виде следующей теоремы.

Теорема 17. *Пусть G — алгебраическая группа, определенная над полем алгебраических чисел K. Тогда выполняются следующие утверждения:* 1) *существует открытое фундаментальное относительно $G_{\mathcal{O}}$ множество $\Omega \subset G_\infty$, т. е.*

(F0) $\mathbf{K}\Omega = \Omega$ *для подходящей максимальной компактной подгруппы* $\mathbf{K} \subset G_\infty$;

(F1) $\Omega G_{\mathcal{O}} = G_\infty$;

(F2) *для любых $x, y \in G_K$ пересечение $\Omega^{-1}\Omega \cap xG_{\mathcal{O}}y$ конечно.*

2) *$G_{\mathcal{O}}$ является группой с конечным числом образующих и конечным числом определяющих соотношений;*

3) *пространство $G_\infty/G_{\mathcal{O}}$ компактно тогда и только тогда, когда редуктивная часть связной компоненты G анизотропна над K;*

4) *пространство $G_\infty/G_{\mathcal{O}}$ имеет конечный инвариантный объем в том и только том случае, когда $\mathbf{X}(G^0)_K = 1$.*

Для доказательства выберем некоторый базис $\mathcal{O}$ над $\mathbb{Z}$ и с его помощью построим группу $H = \mathbf{R}_{K/\mathbb{Q}}(G)$ (см. § 2.1, п. 2). Тогда $G_{\mathcal{O}} \simeq H_{\mathbb{Z}}$, $G_\infty \simeq H_{\mathbb{R}}$ и поэтому применение соответствующих результатов для $\mathbb{Q}$-определенных групп позволяет доказать утверждения 1), 2) теоремы. Для доказательства 3) следует заметить, что редуктивная часть связной компоненты группы H имеет вид $\mathbf{R}_{K/\mathbb{Q}}(D)$, где D — редуктивная часть связной компоненты группы G, причем группа $\mathbf{R}_{K/\mathbb{Q}}(D)$ анизотропна над $\mathbb{Q}$ в том и только том случае, если D анизотропна над K, а затем воспользоваться теоремой 12. Наконец, утверждение 4) получается из теоремы 13 с учетом того обстоятельства, что $\mathbf{X}(H^0)_{\mathbb{Q}} = \mathbf{X}(G^0)_K$.

Без особых усилий можно распространить на $\mathcal{O}$-арифметические подгруппы и другие результаты (теорему плотности, описание подгруппы соизмеримости и т. д.). Мы не будем приводить соответствующих формулировок, ограничившись обобщением на $\mathcal{O}$-арифметический случай участвующих в них понятий. Говорят, что алгебраическая группа G, определенная над полем алгебраических чисел K, имеет компактный тип, если группа $G_\infty = \prod_{v \in V_\infty^K} G_{K_v}$ компактна. Пусть теперь группа G полупроста. Тогда говорят, что G имеет некомпактный тип, если группа G_∞^i некомпактна для каждого K-простого сомножителя G^i группы G. Полупростая группа, которая не относится ни к компактному, ни к некомпактному типу, называется группой смешанного типа.

Завершая изложение теории приведения для арифметических подгрупп, следует отметить, что корни этой теории лежат в клас-

сической теории приведения квадратичных форм (см., например, Касселс [1]), восходящей к Эрмиту и Минковскому. В частности, конструкция фундаментальных множеств как объединения конечного числа сдвигов подходящей области Зигеля обобщает конструкцию, примененную Эрмитом [1] в случае неопределенных рациональных квадратичных форм. Отдавая дань уважения нашим замечательным предшественникам, мы приведем здесь ряд результатов о приведении положительно определенных квадратичных форм (случай неопределенных квадратичных форм рассмотрен у Бореля ([6], § 5)).

Отождествим множество положительно определенных квадратичных форм на $\mathbb{R}^n$ с пространством H вещественных симметрических положительно определенных $(n \times n)$-матриц. Тогда группа $G = GL_n(\mathbb{R})$ транзитивно действует на H справа по формуле

$$g\colon F \to F[g] = {}^t gFg.$$

Стабилизатором единичной формы является группа $\mathbf{K} = O_n(\mathbb{R})$, так что $H = \mathbf{K}\backslash G$, причем проекция $\pi\colon G \to H$ задается формулой $\pi(g) = {}^t gg$. Ясно, что π переводит $SL_n(\mathbb{R})$ в множество $H^{(1)}$ элементов из H с определителем 1 и что $H^{(1)} = SO_n(\mathbb{R})\backslash SL_n(\mathbb{R})$. Назовем областью Зигеля $\Sigma'_{t,v}$ в H множество вида

$$\Sigma'_{t,v} = \{{}^t uau \mid a \in A_t,\ u \in U_v\}$$

в обозначениях § 4.2. Так как ${}^t kk = E_n$ для любого $k \in \mathbf{K}$, то

$$\pi(\Sigma_{t,v}) = \Sigma'_{t^2,v}.$$

Поскольку $\pi(g_1g_2) = \pi(g_1)[g_2]$, то из теорем 4 и 13 вытекает

Теорема 18. (i) (Коркин — Золотарев). $H = \Sigma'_{t,v}[GL_n(\mathbb{Z})]$ *при* $t \geqslant 4/3$, $v \geqslant 1/2$.

(ii) (Эрмит). *Если F — положительно определенная форма на пространстве $\mathbb{R}^n$, то*

$$\min_{x \in \mathbb{Z}^n \setminus \{0\}} F(x) \leqslant (4/3)^{\frac{n-1}{2}} (\det F)^{1/n}.$$

(iii) (Минковский). $H^{(1)} = (\Sigma'_{t,v} \cap H^{(1)})[SL_n(\mathbb{Z})]$ *при* $v \geqslant 1/2$, $t \geqslant 4/3$, *и* $H^{(1)}/SL_n(\mathbb{Z})$ *имеет конечный инвариантный объем.*

§ 4.8. Конечные арифметические группы

Арифметическая теория алгебраических групп изучает в основном бесконечные арифметические группы, ибо только в этой ситуации возникает тесная связь между свойствами алгебраической группы G и ее арифметических подгрупп. Считалось, что

случай конечных арифметических групп больше представляет интерес для теории простых конечных групп. И действительно, скажем, группа автоморфизмов 24-мерной положительно определенной решетки Лича (точнее, ее факторгруппа по центру) оказалась новой простой спорадической группой, открытой Конвеем (Конвей [1]). Однако в последние годы появился интересный круг чисто арифметических вопросов о конечных арифметических группах, которые группируются в основном вокруг следующей гипотезы:

Гипотеза 1. *Пусть G — определенная над $\mathbb{Q}$ алгебраическая группа компактного типа. Тогда для любого вполне вещественного расширения $K/\mathbb{Q}$ имеем $G_{\mathcal{O}} = G_{\mathbb{Z}}$, где $\mathcal{O}$ — кольцо целых поля K.*

(Напомним, что расширение $K/\mathbb{Q}$ называется *вполне вещественным*, если образ любого вложения $K \hookrightarrow \mathbb{C}$ содержится в поле $\mathbb{R}$. Для такого расширения в рассматриваемой ситуации группа $G_\infty = \prod_{v \in V_\infty^K} G_{K_v}$ компактна, так что группа $G_{\mathcal{O}}$ конечна.)

Другими словами, группа единиц $\mathbb{Q}$-определенной алгебраической группы компактного типа не изменяется («стабильна») при расширении кольца $\mathbb{Z}$ до кольца целых $\mathcal{O}$ вполне вещественного числового поля K. Так как любое вполне вещественное расширение, очевидно, содержится во вполне вещественном расширении Галуа, то без ограничения общности можно при этом считать, что $K/\mathbb{Q}$ — расширение Галуа. Эта гипотеза возникла при изучении свойств положительно определенных квадратичных решеток, и ее доказательство позволило бы получить ряд интересных следствий в теории решеток (см. ниже). Следующее утверждение показывает, что ее обобщение на произвольные алгебраические группы не является существенным.

Предложение 12. *Пусть $G \subset GL_n(\mathbb{C})$ — $\mathbb{Q}$-определенная алгебраическая группа такая, что группа вещественных точек $G_{\mathbb{R}}$ компактна и плотна по Зарисскому в G. Тогда существует n-мерная положительно определенная квадратичная форма f с рациональными коэффициентами, для которой $G \subset \mathbf{O}_n(f)$.*

Доказательство. Пусть h — произвольная n-мерная положительно определенная квадратичная форма. В силу компактности $G_{\mathbb{R}}$ для каждого $v \in \mathbb{R}^n$ определен интеграл $\int_{G_{\mathbb{R}}} h(gv)\,dg$, который мы обозначим через $h_0(v)$ (здесь dg — мера Хаара на группе $G_{\mathbb{R}}$). Элементарная проверка показывает, что соответствие $\mathbb{R}^n \to \mathbb{R}$, $v \longmapsto h_0(v)$ задает положительно определенную $G_{\mathbb{R}}$-инвариантную квадратичную форму на $\mathbb{R}^n$. В силу плотности $G_{\mathbb{R}}$ в G в топологии Зарисского, продолжение формы h_0 на пространство $\mathbb{C}^n$ инвариантно относительно G. Обозначим через V пространство всех G-инвариантных квадратичных форм на $\mathbb{C}^n$.

Поскольку G определена над $\mathbb{Q}$, то пространство V также определено над $\mathbb{Q}$. При этом из плотности $\mathbb{Q}$ в $\mathbb{R}$ вытекает плотность $V_{\mathbb{Q}}$ в $V_{\mathbb{R}}$. С другой стороны, подмножество $W \subset V_{\mathbb{R}}$, образованное положительно определенными формами, содержит h_0 и поэтому является непустым открытым подмножеством в $V_{\mathbb{R}}$, причем открытость является следствием известного критерия Сильвестра. В силу плотности $V_{\mathbb{Q}}$ в $V_{\mathbb{R}}$ отсюда следует существование искомой положительно определенной формы $f \in V_{\mathbb{Q}}$. Предложение 12 доказано.

Покажем теперь, что гипотезу 1 можно переформулировать следующим образом:

Гипотеза 1*. *Пусть f — положительно определенная квадратичная форма степени n с рациональными коэффициентами. Тогда $\boldsymbol{O}_n(f)_{\mathcal{O}} = \boldsymbol{O}_n(f)_{\mathbb{Z}}$ для кольца целых $\mathcal{O}$ любого вполне вещественного расширения $K/\mathbb{Q}$.*

Ясно, что гипотеза 1* является частным случаем гипотезы 1. Чтобы получить обратную импликацию, зафиксируем кольцо целых $\mathcal{O}$ вполне вещественного расширения Галуа $K/\mathbb{Q}$ и обозначим через H подгруппу, порожденную G^0 и $G_{\mathcal{O}}$. Так как $\mathcal{O}$ инвариантно относительно всех автоморфизмов $\mathbb{C}/\mathbb{Q}$, то $G_{\mathcal{O}}$, а следовательно, и $H = G^0 G_{\mathcal{O}}$ определены над $\mathbb{Q}$. Очевидно, что $H_{\mathbb{R}} = G^0_{\mathbb{R}} H_{\mathcal{O}}$; поэтому, учитывая плотность $G^0_{\mathbb{R}}$ в G^0 в топологии Зарисского (теорема 2.2), получаем плотность $H_{\mathbb{R}}$ в H. Поэтому согласно предложению 12 существует такая положительно определенная квадратичная форма f с рациональными коэффициентами, что $H \subset \boldsymbol{O}_n(f)$, где n — степень G как линейной группы. Тогда $G_{\mathcal{O}} = H_{\mathcal{O}} \subset \boldsymbol{O}_n(f)_{\mathcal{O}} = \boldsymbol{O}_n(f)_{\mathbb{Z}}$, и $G_{\mathcal{O}} = G_{\mathbb{Z}}$, что и требовалось.

В связи с гипотезой 1* нельзя не отметить следующий результат:

Предложение 13. *Пусть $f(x_1, \ldots, x_n) = a_1 x_1^2 + \ldots + a_n x_n^2$ — диагональная целочисленная положительно определенная квадратичная форма. Тогда $\boldsymbol{O}_n(f)_{\mathcal{O}} = \boldsymbol{O}_n(f)_{\mathbb{Z}}$ для кольца целых $\mathcal{O}$ любого вполне вещественного расширения $K/\mathbb{Q}$.*

Доказательство. Покажем, что у произвольного элемента $b = (b_{ij}) \in \boldsymbol{O}_n(f)_{\mathcal{O}}$ в каждом столбце и каждой строке имеется лишь один ненулевой элемент, который при этом равен ± 1. Без ограничения общности можно считать, что $a_1 \leqslant a_2 \leqslant \ldots \leqslant a_n$. Условие $b \in \boldsymbol{O}_n(f)$ означает, что ${}^t bFb = F$, где $F = \operatorname{diag}(a_1, \ldots, a_n)$, откуда получаются следующие соотношения:

$$\sum_{i=1}^{n} a_i b_{ij}^2 = a_j \quad \text{для любого} \quad j = 1, \ldots, n; \tag{1}$$

$$\sum_{i=1}^{n} a_i b_{ij} b_{ik} = 0 \quad \text{для любых} \quad j, k = 1, \ldots, n, \ j \neq k. \tag{2}$$

Найдем в последней строке матрицы b элемент b_{nj}, отличный от нуля. Тогда в силу (1) имеем

$$a_n\tau(b_{nj})^2 \leqslant \sum_{i=1}^{n} a_i\tau(b_{ij})^2 = a_j \leqslant a_n$$

для любого вложения $\tau\colon K \hookrightarrow \mathbb{R}$, так что $|b_{nj}|_v \leqslant 1$ для любого вещественного нормирования v поля K. Но

$$\prod_{v \in V_\infty^K} |b_{nj}|_v = |N_{K/\mathbb{Q}}(b_{nj})|,$$

где $N_{K/\mathbb{Q}}$ — норменное отображение, причем из того что $b_{nj} \in \mathcal{O}$, вытекает, что $N_{K/\mathbb{Q}}(b_{nj}) \in \mathbb{Z}$ и $|N_{K/\mathbb{Q}}(b_{nj})| \geqslant 1$. Поэтому $|b_{nj}|_v = 1$ для любого $v \in V_\infty^K$. Поскольку $|b|_v = |\tau_v(b)|$, где $\tau_v\colon K \hookrightarrow \mathbb{R}$ — соответствующее вложение, $|\ |$ — абсолютная величина вещественного числа, то $b_{nj} = \pm 1$. Возвращаясь к соотношению (1) и учитывая неравенство $a_j \leqslant a_n$, получаем, что $a_j = a_n$ и $b_{ij} = 0$ при $i < n$. Далее, применяя (2), получим, что $b_{nk} = 0$ для всех $k \neq j$. Подобное рассуждение можно применить к любой j-й строке, если $a_j = a_n$. Тогда получим, что матрица b имеет блочную структуру

$$b = \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix},$$

где b_1 — квадратная матрица размера $l \times l$, степень l которой совпадает с максимальным значением индекса, для которого $a_i < a_n$; b_2 — мономиальная матрица размера $(n-l)\times(n-l)$, все ненулевые элементы которой равны ± 1. (Возможна ситуация, когда все a_i совпадают, но тогда приведенное выше рассуждение полностью доказывает требуемое утверждение.) Доказательство предложения 13 теперь завершается очевидным индуктивным рассуждением.

Дадим еще одну эквивалентную формулировку гипотезы 1.

Гипотеза 1.** *Пусть $K/\mathbb{Q}$ — вполне вещественное расширение Галуа, $\mathcal{O}$ — кольцо целых поля K и $\Gamma \subset GL_n(\mathcal{O})$ — конечная подгруппа, инвариантная (в целом, а не поэлементно) относительно группы* $\mathrm{Gal}(K/\mathbb{Q})$. *Тогда $\Gamma \subset GL_n(\mathbb{Z})$.*

Легко убедиться в эквивалентности гипотез 1 и 1**. В самом деле, как мы уже отмечали, можно считать расширение $K/\mathbb{Q}$ в гипотезе 1 расширением Галуа. Тогда, если G — определенная над $\mathbb{Q}$ алгебраическая группа компактного типа, то $G_{\mathcal{O}}$ является конечной $\mathrm{Gal}(K/\mathbb{Q})$-инвариантной подгруппой в $GL_n(\mathcal{O})$, поэтому из справедливости гипотезы 1** вытекает справедливость гипотезы 1. Обратно, если $\Gamma \subset GL_n(\mathcal{O})$ — конечная $\mathrm{Gal}(K/\mathbb{Q})$-инвариантная подгруппа, то ее можно рассматривать как $\mathbb{Q}$-определенную алгебраическую группу, для которой группа вещественных точек $G_{\mathbb{R}} = \Gamma$ компактна.

К настоящему времени гипотеза 1** доказана лишь для специальных расширений Галуа, а именно для нильпотентных расширений и расширений, у которых все силовские подгруппы группы Галуа циклические (см. Бартельс, Китаока [1]). Доказательство для нильпотентных расширений содержит наиболее принципиальные моменты, поэтому рассмотрением этого случая мы и ограничимся, отсылая читателя за дополнительной информацией к статье Бартельса — Китаоки. Обратим внимание читателя на два факта, которые постоянно приходится использовать при работе с гипотезой 1**. Первый из них — это теорема Эрмита о несуществовании нетривиальных всюду неразветвленных расширений поля $\mathbb{Q}$ (см. теорему 1.3), второй — следующая лемма, принадлежащая Минковскому [1].

Лемма 19 (Минковский). *Для любого $p \neq 2$ конгруэнц-подгруппа $GL_n(\mathbb{Z}, p)$ не имеет кручения.*

Доказательство. Используя вложение $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$, из леммы 3.8 получаем, что порядок любого элемента из $GL_n(\mathbb{Z}, p)$ либо бесконечен, либо является степенью p. Поэтому достаточно показать, что $GL_n(\mathbb{Z}, p)$ не содержит отличных от E_n элементов порядка p. Пусть $E_n \neq x \in GL_n(\mathbb{Z}, p)$ и $x^p = E_n$. Представим x в виде $x = E_n + p^\alpha y$, где $y \in M_n(\mathbb{Z})$ и $y \not\equiv 0 \pmod p$. Тогда

$$x^p = (E_n + p^\alpha y)^p =$$
$$= E_n + C_p^1 p^\alpha y + \ldots + C_p^{p-1} p^{\alpha(p-1)} y^{p-1} + p^{\alpha p} y^p = E_n,$$

т. е.

$$p^{\alpha+1} y = -C_p^2 p^{2\alpha} y^2 - \ldots - C_p^{p-1} p^{\alpha(p-1)} y^{p-1} - p^{\alpha p} y^p. \qquad (3)$$

Все биномиальные коэффициенты C_p^i, $0 < i < p$, делятся на p, так что для $i > 1$ выполняется сравнение

$$C_p^i p^{i\alpha} y^i \equiv 0 \pmod{p^{2\alpha+1}}.$$

Поскольку $p > 2$, то $\alpha p \geqslant 2\alpha + 1$ и выполняется сравнение $p^{\alpha p} y^p \equiv 0 \pmod{p^{2\alpha+1}}$. Таким образом, правая часть (3) сравнима с 0 по модулю $p^{2\alpha+1}$, в то же время для левой части это сравнение по построению не выполняется, ибо $\alpha + 1 < 2\alpha + 1$. Лемма 19 доказана.

Пусть теперь $K/\mathbb{Q}$ — вполне вещественное расширение Галуа. Если $K/\mathbb{Q}$ — неразветвлено во всех точках, то согласно теореме Эрмита $K = \mathbb{Q}$, и доказывать нечего. Таким образом, можно считать, что в расширении $K/\mathbb{Q}$ ветвится, по крайней мере, одно простое число. Покажем, что для доказательства гипотезы 1** достаточно рассмотреть случай, когда имеется лишь одно разветвленное простое число.

Предложение 14. *Пусть $K/\mathbb{Q}$ — вполне вещественное расширение Галуа с группой Галуа $\mathcal{G}$, $\Gamma \subset GL_n(\mathcal{O})$ — конечная $\mathcal{G}$-инвариантная подгруппа. Предположим, что* $\Gamma \cap GL_n(L) \subset GL_n(\mathbb{Z})$

для любого собственного подрасширения Галуа $L \subset K$. Тогда если $\Gamma \not\subset GL_n(\mathbb{Z})$, то в K ветвится ровно одно простое число.

Доказательство. Предположим, что в расширении $K/\mathbb{Q}$ ветвятся простые числа p и q $(q \neq 2)$, и покажем, что $\Gamma \subset GL_n(\mathbb{Z})$. Рассмотрим некоторые продолжения $w_p | p$ и $w_q | q$, и пусть $\mathfrak{p} = \mathcal{O} \cap \mathfrak{p}_{w_p}$ и $\mathfrak{q} = \mathcal{O} \cap \mathfrak{q}_{w_q}$ — соответствующие идеалы в $\mathcal{O}$. Мы будем использовать группы ветвления $\mathcal{G}^{(i)}$, определения которых приведены в конце § 1.1. Пусть $x \in \Gamma$ и $\sigma \in \mathcal{G}^{(1)}(w_q)$. Тогда $x \equiv \sigma(x) \pmod{\mathfrak{q}}$, и поэтому в силу $\mathcal{G}$-инвариантности Γ элемент $y = x^{-1}\sigma(x)$ лежит в конгруэнц-подгруппе $\Gamma(\mathfrak{q})$. Возьмем теперь произвольный элемент $\tau \in \mathcal{G}^{(1)}(w_p)$. Тогда коммутатор $[y, \tau(y)] = y\tau(y)\, y^{-1}\tau(y)^{-1}$, с одной стороны, лежит в $\Gamma(\mathfrak{q})$, ибо $\Gamma(\mathfrak{q})$ — нормальный делитель в Γ, с другой — в $\Gamma(\mathfrak{p})$ в силу условия $y \equiv \tau(y) \pmod{\mathfrak{p}}$. Но, вкладывая $\mathcal{O}$ в $\mathcal{O}_{w_p}$ и $\mathcal{O}_{w_q}$, из леммы 3.8 получаем, что порядок любого элемента из $\Gamma(\mathfrak{p})$ (соответственно $\Gamma(\mathfrak{q})$) является степенью p (соответственно степенью q); в частности, $\Gamma(\mathfrak{p}) \cap \Gamma(\mathfrak{q}) = \{E_n\}$. Поэтому $[y, \tau(y)] = E_n$, т. е. элементы y и $\tau(y)$ перестановочны. Далее, так как $y \in \Gamma(\mathfrak{q})$, то порядок элемента y, а значит, и порядок элемента $z = y^{-1}\tau(y)$ является степенью q. Но в то же время $z \in \Gamma(\mathfrak{p})$, и поэтому в действительности $z = E_n$ и $\tau(y) = y$. Мы показали, что $\tau(y) = y$ для любого $\sigma \in \mathcal{G}^{(1)}(w_p)$, где $w_p | p$. Пусть $\mathcal{H}$ — подгруппа $\mathcal{G}$, порожденная группами инерции $\mathcal{G}^{(1)}(w_p)$, для всех $w_p | p$, $L = K^{\mathcal{H}}$ — соответствующее неподвижное поле. Как мы отмечали в конце § 1.1, L является максимальным расширением Галуа поля $\mathbb{Q}$, содержащимся в K и неразветвленным относительно p. Так как p ветвится в K, то $L \neq K$ и по условию $\Gamma \cap GL_n(L) \subset GL_n(\mathbb{Z})$. Но выше мы установили, что $y \in GL_n(L)$, и поэтому $y \in GL_n(\mathbb{Z})$. Вспоминая теперь, что $y \in \Gamma(\mathfrak{q})$, мы видим, что y является элементом конечного порядка в $GL_n(\mathbb{Z}, q)$, и, значит, $y = E_n$ в силу леммы Минковского. По построению $y = x^{-1}\sigma(x)$, где x — произвольный элемент из Γ, $\sigma \in \mathcal{G}^{(1)}(w_q)$. Отсюда следует, что в действительности $\Gamma \subset GL_n(P)$, где $P = K^{\mathcal{F}}$ — неподвижное поле подгруппы $\mathcal{F} \subset \mathcal{G}$, порожденной группами инерции $\mathcal{G}^{(1)}(w_q)$ для всех продолжений $w_q | q$. Рассуждая как и выше, получим, что $P \neq K$, и следовательно, $\Gamma = \Gamma \cap GL_n(P) \subset GL_n(\mathbb{Z})$. Предложение доказано.

Предложение 14 показывает, что если к гипотезе 1** существуют контрпримеры, то минимальный в смысле расширения полей контрпример отвечает расширению, в котором ветвится ровно одно простое число. Используя это наблюдение, мы докажем гипотезу 1** для нильпотентных расширений.

Теорема 19 (Бартельс — Китаока). *Пусть $K/\mathbb{Q}$ — вполне вещественное расширение Галуа с нильпотентной группой Га-*

луа $\mathcal{G}$. Если $\Gamma \subset GL_n(\mathcal{O})$ — конечная $\mathcal{G}$-инвариантная подгруппа, то $\Gamma \subset GL_n(\mathbb{Z})$.

Доказательство. Так как любое подрасширение Галуа в нильпотентном расширении также является нильпотентным, то из сделанного выше замечания вытекает, что достаточно рассмотреть расширения $K/\mathbb{Q}$, в которых ветвится только одно простое число p. Покажем, что в этом случае группа Галуа $\mathcal{G}$ циклическая. Для этого проведем индукцию по степени $[K:\mathbb{Q}]$. Центр Z группы $\mathcal{G}$ нетривиален, и по предположению индукции факторгруппа $\mathcal{G}/Z$ циклическая. Но тогда группа $\mathcal{G}$ абелева и по теореме Кронекера — Вебера (см., например, Ивасава [1], § 8.1) $K \subset \mathbb{Q}(\zeta_{p^d})$ для подходящего d, где ζ_{p^d} — примитивный корень степени p^d из единицы. Так как расширение $K/\mathbb{Q}$ вполне вещественно, то в действительности $K \subset \mathbb{Q}(\zeta_{p^d}+\zeta_{p^d}^{-1})$, и группа $\mathcal{G}$ является факторгруппой группы $(\mathbb{Z}/p^d\mathbb{Z})^*/\{\pm 1\}$, которая циклична. Теперь, когда цикличность $\mathcal{G}$ уже доказана, мы можем в силу теоремы Кронекера утверждать, что в нашей ситуации всегда $K \subset \mathbb{Q}(\zeta_{p^d}+\zeta_{p^d}^{-1})$ для подходящего числа $d>0$, и для доказательства теоремы 19 достаточно разобрать случай $K = \mathbb{Q}(\zeta_{p^d}+\zeta_{p^d}^{-1})$.

Лемма 20. *Гипотеза 1** верна для поля $K=\mathbb{Q}(\zeta_{p^d}+\zeta_{p^d}^{-1})$.*

Доказательство использует одну общую конструкцию, которая может оказаться полезной и в других ситуациях. А именно, для произвольного расширения Галуа $K/\mathbb{Q}$ с группой Галуа $\mathcal{G}$ определим подрасширение Галуа $M/\mathbb{Q}$ следующим образом. Зафиксируем некоторое простое p и рассмотрим некоторое продолжение $w_p \mid p$; пусть $\mathfrak{p}=\mathcal{O}\cap\mathfrak{p}_{w_p}$ — соответствующий идеал в $\mathcal{O}$ и r — минимальное натуральное число, для которого $p \notin \mathfrak{p}^{r(p-1)}$. Обозначим через $\mathcal{H}$ подгруппу в $\mathcal{G}$, порожденную r-ми группами ветвления $\mathcal{G}^{(r)}(w_p)$ для всех продолжений $w_p \mid p$, и положим $M=K^{\mathcal{H}}$. Получающееся подрасширение $M/\mathbb{Q}$ зависит от выбора простого числа p, однако для любого p оно является расширением Галуа, причем для любой конечной $\mathcal{G}$-инвариантной подгруппы $\Gamma \subset GL_n(\mathcal{O})$ справедливо включение $\Gamma \subset GL_n(\mathcal{O}_M)$, где $\mathcal{O}_M$ — кольцо целых в M. В самом деле, для любого $x \in \Gamma$ и любого $\sigma \in \mathcal{G}^{(r)}(w_p)$ имеем $\sigma(x) \equiv x \pmod{\mathfrak{p}^r}$, т. е. $x^{-1}\sigma(x) \in \Gamma(\mathfrak{p}^r)$. Поэтому достаточно установить тривиальность конгруэнц-подгруппы $\Gamma(\mathfrak{p}^r)$. Для этого, в свою очередь, достаточно показать, что конгруэнц-подгруппа $GL_n(\mathcal{O},\mathfrak{p}^r)$ не имеет кручения, что равносильно отсутствию в ней элементов порядка p. Последнее доказывается, практически, так же, как и лемма Минковского. А именно, пусть $E_n \neq x \in GL_n(\mathcal{O},\mathfrak{p}^r)$ и $x^p=E_n$. Представим x в виде $x=E_n+y$, где $y \equiv 0 \pmod{\mathfrak{p}^m}$ $(m \geqslant r)$, но

$y \not\equiv 0 \pmod{\mathfrak{p}^{m+1}}$. Тогда имеем $x^p = E_n + py + C_p^2 y^2 + \ldots + C_p^{p-1} y^{p-1} + y^p = E_n$, т. е.

$$py = -C_p^2 y^2 - \ldots - C_p^{p-1} y^{p-1} - y^p. \tag{4}$$

Обозначим через e индекс ветвления $e(w_p|p)$. Тогда e совпадает с показателем степени, в которой идеал $\mathfrak{p}$ входит в разложение идеала $p\mathcal{O}$, поэтому из определения числа r вытекает, что $r = \left[\frac{e}{p-1}\right] + 1$ (где, как обычно, [ ] — целая часть числа), и, стало быть, $(p-1)r > e$. Используя эту оценку, получим противоречие, вычислив степень $\mathfrak{p}$, на которую делятся соответственно правая и левая части (4). По построению для левой части (4) имеем

$$py \equiv 0 \pmod{\mathfrak{p}^{m+e}}, \quad \text{но} \quad py \not\equiv 0 \pmod{\mathfrak{p}^{m+e+1}}.$$

Так как C_p^i делятся на $p\,(i \neq 0, p)$, то для $1 < i < p$ имеем $C_p^i y^i \equiv 0 \pmod{\mathfrak{p}^{im+e}}$ и $ime \geqslant m + e + 1$. Наконец, $y^p \equiv 0 \pmod{\mathfrak{p}^{mp}}$, причем

$$mp = m + m(p-1) \geqslant m + r(p-1) > m + e.$$

Таким образом, правая часть (2) сравнима с нулем по модулю идеала $\mathfrak{p}^{m+e+1}$ — противоречие.

Чтобы завершить доказательство леммы, теперь достаточно установить, что для поля $K_d = \mathbb{Q}\left(\zeta_{p^d} + \zeta_{p^d}^{-1}\right)$ подрасширение, построенное при помощи простого числа p, содержится в K_{d-1} (поскольку $K_0 = \mathbb{Q}$, то это и даст требуемое). Нам понадобится информация о ветвлении простого числа p в круговом расширении $L_d/\mathbb{Q}$, $L_d = \mathbb{Q}\left(\zeta_{p^d}\right)$ (см. [АТЧ], гл. III).

Известно, что $L_d/\mathbb{Q}$ является абелевым расширением Галуа степени $\varphi(p^d) = p^{d-1}(p-1)$. Кольцо целых $\mathcal{O}_d$ поля L_d совпадает с $\mathbb{Z}\left[\zeta_{p^d}\right]$, причем $p\mathcal{O}_d = \mathfrak{P}^{\varphi(p^d)}$, где $\mathfrak{P} = \left(1 - \zeta_{p^d}\right)\mathcal{O}_d$; другими словами p-адическое нормирование допускает единственное продолжение на L_d, причем это продолжение вполне разветвлено и соответствующий идеал нормирования в $\mathcal{O}_d$ совпадает с главным идеалом, порожденным $1 - \zeta_{p^d}$. В частности, применяя этот факт к $d = 1$, получим, что идеал нормирования $\mathfrak{P}_1 \subset \mathcal{O}_1$ порождается $1 - \zeta_p$. С другой стороны, поскольку L_d/L_1 является вполне разветвленным расширением степени p^{d-1}, мы должны иметь $\mathfrak{P}_1\mathcal{O}_d = \mathfrak{P}^{p^{d-1}}$, откуда $1 - \zeta_p \in \mathfrak{P}^{p^{d-1}}$, т. е. $\zeta_p \equiv 1 \left(\mathrm{mod}\ \mathfrak{P}^{p^{d-1}}\right)$. Нам будет удобно использовать последнее соотношение в несколько другой форме. А именно, для любого целого a, взаимно простого с p, обозначим через σ_a

автоморфизм из $\mathrm{Gal}(L_d/\mathbb{Q})$, задаваемый условием $\sigma_a(\zeta_{p^d}) = \zeta_{p^d}^a$. Тогда установленное выше соотношение означает, что

$$\sigma_a(\zeta_{p^d}) \equiv \zeta_{p^d} \pmod{\mathfrak{P}^{p^{d-1}}} \quad \text{для} \quad a \equiv 1 \pmod{p^{d-1}}.$$

Так как ζ_{p^d} порождает $\mathcal{O}_d$, то в итоге для таких a имеем

$$\sigma_a(x) \equiv x \pmod{\mathfrak{P}^{p^{d-1}}} \quad \text{для всех} \quad x \in \mathcal{O}_d. \tag{5}$$

С другой стороны, вычисляя константу r для поля K_d, получим

$$r = \left[\frac{\varphi(p^d)/2}{p-1}\right] + 1 = \left[\frac{p^{d-1}}{2}\right] + 1, \tag{6}$$

ибо индекс ветвления e p-адического нормирования в расширении $K_d/\mathbb{Q}$ равен $\varphi(p^d)/2$. Так как индекс ветвления L_d/K_d равен 2, то используя (5) и (6), для нечетного p получаем сравнение

$$\sigma_a(x) \equiv x \pmod{\mathfrak{p}^r} \quad \text{при} \quad a \equiv 1 \pmod{p^{d-1}} \quad \text{для всех целых} \quad x \in K_d.$$

Если обозначить через $\mathcal{G}$ группу Галуа $\mathrm{Gal}(K_d/\mathbb{Q})$, а через w (единственное) продолжение p-адического нормирования на K_d, то последнее сравнение означает, что r-я группа ветвления $\mathcal{G}^{(r)}(w)$ содержит подгруппу $\mathcal{H} \subset \mathcal{G}$, состоящую из ограничений автоморфизмов σ_a для $a \equiv 1 \pmod{p^{d-1}}$. Но $K_d^{\mathcal{H}} = K_{d-1}$, так что конструируемое указанным выше способом поле M содержится в K_{d-1}, что и требовалось.

Чтобы разобраться с оставшимся случаем $p = 2$, мы усилим сравнение (4), показав, что $\sigma_a(x) \equiv x \pmod{\mathfrak{P}^{2^{d-1}+2}}$ для $a \equiv 1 \pmod{2^{d-1}}$ и любого целого $x \in K_d$. Достаточно показать, что

$$\sigma_a(\zeta_{2^d} + \zeta_{2^d}^{-1}) \equiv \zeta_{2^d} + \zeta_{2^d}^{-1} \pmod{\mathfrak{P}^{2^{d-1}+2}}.$$

Последнее легко следует из (5) и следующих вычислений:

$$\zeta_{2^d} + \zeta_{2^d}^{-1} = \zeta_{2^d}^{-1}(\zeta_{2^d}^2 + 1) = \zeta_{2^d}^{-1}((\zeta_{2^d} - 1)^2 + 2\zeta_{2^d}),$$

с учетом того, что $(\zeta_{2^d} - 1)^2 + 2\zeta_{2^d} \in \mathfrak{P}^2$. Лемма 20 полностью доказана.

Изучая частные случаи гипотез 1 — 1**, можно накладывать дополнительные ограничения двух типов — на вполне вещественное расширение $K/\mathbb{Q}$ и на группу Γ в гипотезе 1** или соответственно форму f в гипотезе 1*. Ограничения первого типа мы накладывали в теореме 19. Приведем теперь пример результата с ограничениями второго типа, который показывает, что в пространстве вещественных симметрических матриц имеется открытое подмножество, для целочисленных матриц из которого

(точнее, для соответствующих квадратичных форм) выполняется гипотеза 1*.

Предложение 15. *Пусть f — положительно определенная квадратичная форма степени n с целыми коэффициентами и матрицей $a=(a_{ij})$. Предположим, что для всех $i=1, \ldots, n$ выполняется неравенство $a_{ii} \leqslant 4\lambda$, где λ — наименьшее собственное значение матрицы a. Тогда для любого вполне вещественного расширения $K/\mathbb{Q}$ имеем $\boldsymbol{O}_n(f)_{\mathcal{O}}=\boldsymbol{O}_n(f)_{\mathbb{Z}}$, где $\mathcal{O}$ — кольцо целых поля K.*

Доказательство. Пусть $x=(x_{ij}) \in \boldsymbol{O}_n(f)_{\mathcal{O}}$. Покажем, что относительно любого вещественного вложения K выполняются неравенства

$$\sum_{i=1}^{n} x_{ij}^2 \leqslant \frac{a_{jj}}{\lambda}. \tag{7}$$

Действительно, обозначим через v_j вектор $(0, 0, \ldots, 0, 1, 0, \ldots \ldots, 0)$, где 1 стоит на j-м месте. Тогда $xv_j=(x_{1j}, \ldots, x_{nj})=w_j$, причем $a_{jj}=f(v_j)=f(w_j)$. Если обозначить через g квадратичную форму на $\mathbb{R}^n$, относительно которой базис $v_1, \ldots, v_n$ является ортонормированным, то левая часть (7) есть $g(w_j)$, и поэтому достаточно показать, что для любого вектора $w \in \mathbb{R}^n$ справедливо неравенство $f(w) \geqslant \lambda g(w)$. Приводя форму f к диагональному виду при помощи преобразования из $\boldsymbol{O}_n(g)_{\mathbb{R}}$, мы видим, что достаточно разобрать случай диагональной формы f, в котором требуемое утверждение тривиально. Комбинируя (7) с условием $a_{ii} \leqslant 4\lambda$, мы видим, что в нашей ситуации

$$\sum_{i=1}^{n} x_{ij}^2 \leqslant 4 \quad \text{для всех} \quad j=1, \ldots, n.$$

В частности, $|x_{ij}|_v \leqslant 2$ для всех $i, j=1, \ldots, n$ и для любого нормирования $v \in V_\infty^K$. Отсюда следует, что все x_{ij} совпадают с вещественными частями некоторых корней из единицы. В самом деле, пусть a — целое вполне вещественное алгебраическое число и $|a|_v \leqslant 2$ для любого вещественного нормирования v. Тогда $b=\sqrt{a^2/4-1}$ — вполне мнимое. Число $a/2+b$ удовлетворяет уравнению $t^2-at+1=0$ и поэтому является целым алгебраическим числом, все сопряженные которого имеют абсолютное значение 1. Отсюда легко следует, что $a/2+b$ есть корень из единицы, так что $a=2\operatorname{Re}(a/2+b)$ есть его вещественная часть. Из доказанного вытекает, что коэффициенты x_{ij} порождают абелево расширение поля $\mathbb{Q}$, поэтому доказательство предложения завершается применением теоремы 19.

Приведем без доказательства еще два результата, которые также получаются при помощи метрических соображений (Китаока [1], [2]).

Предложение 16. *Для каждой размерности n можно найти такое конечное множество S целых алгебраических чисел, что если $K \cap S = \varnothing$, то для расширения $K/\mathbb{Q}$ и любой квадратичной формы выполняется гипотеза 1*.*

(Отметим, что используя теорию приведения квадратичных форм (см. § 4.7), можно явно найти S для небольших значений n (см. Китаока [1]).

Предложение 17. *Если либо степень расширения $K/\mathbb{Q}$, либо размерность формы f не превосходит 42, то выполняется гипотеза 1*.*

Мы привели практически все известные результаты, относящиеся к обсуждаемым гипотезам. С целью привлечь интерес читателя и, возможно, стимулировать дальнейшие исследования в этом направлении, отметим возможные приложения (см. Бартельс [1, 2]).

Предложение 18. *Предположим, что для расширения $K/\mathbb{Q}$ и любой положительно определенной квадратичной формы выполняется гипотеза 1*. Тогда, если целочисленные положительно определенные квадратичные формы f и g эквивалентны над кольцом целых $\mathcal{O}$ поля K, то они эквивалентны над $\mathbb{Z}$.*

Доказательство. Пусть $a \in GL_n(\mathcal{O})$ осуществляет эквивалентность $f \simeq g$. Рассмотрим форму $h = f \perp g$ и построим элемент $b \in \boldsymbol{O}_{2n}(h)$, задав его матрицей

$$\begin{pmatrix} 0 & a^{-1} \\ a & 0 \end{pmatrix}.$$

Тогда $b \in \boldsymbol{O}_{2n}(h)_{\mathcal{O}} = \boldsymbol{O}_{2n}(h)_{\mathbb{Z}}$, так что $a \in GL_n(\mathbb{Z})$, что и требовалось.

В двух следующих утверждениях участвуют когомологии Галуа и группы аделей, систематическому изложению которых посвящены гл. V и VI. Мы приводим эти результаты здесь, чтобы собрать воедино весь материал, относящийся к рассматриваемым гипотезам. Читатель же может сначала ознакомиться с гл. V и VI, а затем вернуться к данным утверждениям.

Теорема 20. *Пусть $K/\mathbb{Q}$ — вполне вещественное расширение Галуа, G — алгебраическая $\mathbb{Q}$-группа компактного типа. Предположим, что $G_{\mathcal{O}} = G_{\mathbb{Z}}$. Тогда естественное отображение когомологий Галуа*

$$H^1(K/\mathbb{Q}, G_{\mathcal{O}}) \to \prod_p H^1(K_v/\mathbb{Q}_p, G_{\mathcal{O}_v})$$

имеет тривиальное ядро.

Теорема 21. *В условиях предыдущего предложения потребуем дополнительно, чтобы G была связной группой, удовлетворяющей принципу Хассе для когомологий Галуа. Тогда*

$$G_{A_{\mathbb{Q}}} \cap G_K G_{A_K(\infty)} = G_{\mathbb{Q}} G_{A_{\mathbb{Q}}(\infty)},$$

т. е. отображение

$$G_{\mathbb{Q}}\backslash G_{A_{\mathbb{Q}}}/G_{A_{\mathbb{Q}}(\infty)} \to G_K\backslash G_{A_K}/G_{A_K(\infty)}$$

имеет тривиальное ядро.

(Здесь $G_{A_{\mathbb{Q}}}(\infty)$, $G_{\mathbb{Q}}$ (соответственно, $G_{A_K(\infty)}$, G_K) — подгруппы целых и главных аделей в адельных группах $G_{A_{\mathbb{Q}}}$ и G_{A_K} над полями $\mathbb{Q}$ и K соответственно, см. § 5.1.)

Доказательство теорем 20 и 21 и некоторые их приложения см. в § 8.4. Отметим только, что в применении к квадратичным формам теорема 21 означает, что если две положительно определенные формы над $\mathbb{Z}$ принадлежат одному роду и попадают в один класс при расширении кольца скаляров до $\mathcal{O}$, то они лежат в одном классе над $\mathbb{Z}$.

В заключение приведем пример, который показывает, что относительный вариант гипотез 1, 1* и 1** (т. е. когда поле $\mathbb{Q}$ меняется на некоторое вполне вещественное расширение) не имеет места.

Пример. Пусть E/F — нетривиальное расширение Галуа, неразветвленное во всех (неархимедовых) точках, где E и F — вполне вещественные числовые поля. (Такое расширение можно построить, взяв в качестве F любое вполне вещественное числовое поле с нечетным числом классов, бо́льшим 1 (например, для $F=\mathbb{Q}(\sqrt{142})$ имеем $h_F=3$), а в качестве E — его гильбертово поле классов). Наша цель — построить пример такой конечной подгруппы $\Gamma\subset GL_n(E)$ для подходящего n, которая была бы инвариантна относительно группы Галуа $\mathcal{G}=\mathrm{Gal}(E/F)$, но не содержалась в $GL_n(F)$. Ключ к построению такой группы содержится в доказательстве предложения 18. А именно, предположим, что нам удалось построить n-мерное векторное пространство V над полем F, снабженное положительно определенной квадратичной формой f, и две свободные решетки L, $M\subset V$ над кольцом целых $\mathcal{O}_F$ такие, что выполняются следующие свойства:

1) $\mathcal{O}_E L=\mathcal{O}_E M$,

2) решетки L и M неизометричны, т. е. не существует $g\in \in \boldsymbol{O}_n(f)$ со свойством $g(L)=M$.

Тогда рассуждения из доказательства предложения 18 показывают, что группа $\Gamma=\boldsymbol{O}_{2n}(f\perp f)_{\mathcal{O}_E}^{\mathcal{O}_E L\perp \mathcal{O}_E M}\subset GL_{2n}(E)$ является искомой. Для построения свободных решеток L, M со свойствами 1), 2) поступим следующим образом. Обозначим через V_0 групповое кольцо $F[\mathcal{G}]$ и введем на V_0 скалярное произведение, полагая, что элементы группы $\mathcal{G}$ образуют ортонормированный базис. Далее, определим действие $\mathcal{G}$ на пространстве $EV_0 = = E[\mathcal{G}]$ формулой $g\left(\sum_h a_h h\right)=\sum_h g(a_h)(gh)$. Положим, нако-

нец, $L_0 = \perp_{g \in \mathcal{G}} \mathcal{O}_F g$, $M_0 = (\mathcal{O}_E L_0)^{\mathcal{G}}$ (неподвижные точки). Решетки L_0 и M_0 обладают следующими свойствами:

(i) $\mathcal{O}_E L_0 = \mathcal{O}_E M_0$;

(ii) решетка M_0 является $\mathcal{O}_F$-неразложимой, т. е. непредставима в виде ортогональной прямой суммы собственных $\mathcal{O}_F$-подрешеток;

(iii) для любого целого $m \geqslant 1$ решетки $L_0^m = L_0 \perp \ldots \perp L_0$ и $M_0^m = M_0 \perp \ldots \perp M_0$ неизометричны.

Для доказательства (i) нам придется напомнить некоторые факты из теории ветвления (см., например, Ленг [2], гл. III). Неразветвленность E/F во всех точках эквивалентна тому, что дискриминантный идеал $D_{E/F}$ совпадает с $\mathcal{O}_F$. При этом $D_{E/F}$ определяется как идеал в $\mathcal{O}_F$, порожденный дискриминантами всех базисов $a_1, \ldots, a_n$ поля E над F (т. е. квадратами определителей $\det(g_i(a_j))^2$, где $\mathcal{G} = \{g_1, \ldots, g_n\}$), содержащимися в $\mathcal{O}_E$. Из условия $D_{E/F} = \mathcal{O}_F$ вытекает, что для любого $w \in V_f^E$ найдутся такие $a_1, \ldots, a_n \in \mathcal{O}_E$, что $\det(g_i(a_j))$ является единицей в кольце $\mathcal{O}_{E_w}$. Рассмотрим элементы $x_i = \sum_{g \in \mathcal{G}} g(a_i)\, g \in M_0$ $(i = 1, \ldots, n)$. Тогда из наших построений вытекает, что все элементы $g \in \mathcal{G}$ выражаются в виде линейных комбинаций элементов x_i с коэффициентами из $\mathcal{O}_{E_w}$, откуда $\mathcal{O}_{E_w} L_0 = \mathcal{O}_{E_w} M_0$. Поскольку последнее равенство справедливо для любого $w \in V_f^E$, то обязательно $\mathcal{O}_E L_0 = \mathcal{O}_E M_0$ (см. § 1.5). Докажем теперь (ii). Пусть $M_0 = M_1 \perp M_2$; тогда $\mathcal{O}_E L_0 = \mathcal{O}_E M_0 = \mathcal{O}_E M_1 \perp \mathcal{O}_E M_2$, в частности, каждый элемент $g \in \mathcal{G}$ имеет представление вида $g = g_1 + g_2$, где $g_i \in \mathcal{O}_E M_i$. В этом случае получаем соотношение

$$1 = f(g) = f(g_1) + f(g_2),$$

откуда $|f(g_i)|_w \leqslant 1$ для любого вещественного нормирования w поля E $(i = 1, 2)$. Но $f(g_i) \in \mathcal{O}_E$, поэтому в случае $f(g_i) \neq 0$ мы должны иметь

$$\prod_{w \in V_\infty^E} |f(g_i)|_w = |N_{E/Q}(f(g_i))| \geqslant 1.$$

Отсюда следует, что $f(g_i)$ всегда есть либо 0, либо 1, т. е. g попадает в одно из слагаемых $\mathcal{O}_E M_i$. Но $M_i \subset M_0 = (\mathcal{O}_E L_0)^{\mathcal{G}}$, так что каждое слагаемое должно быть $\mathcal{G}$-инвариантным, и в итоге одно из слагаемых совпадает с M_0, а другое сводится к нулю, т. е. (ii) доказано. Наконец, пусть t: $L_0^m \to M_0^m$ — некоторая изометрия. Зафиксируем некоторый элемент $g \in \mathcal{G}$ и

положим $L_1 = \mathcal{O}_F g$, $L_2 = \left(\perp_{h \neq g} \mathcal{O}_F h\right) \perp L_0^{m-1}$. Тогда $L_0^m = L_1 \perp L_2$, и поэтому мы должны иметь $M_0^m = t(L_1) \perp t(L_2)$. Рассмотрим теперь элемент $t(g) \in M_0^m$, и пусть $t(g) = x_1 + \ldots + x_m$, где $x_i \in M_0$. Вычисляя значение f, получим

$$1 = f(t(g)) = f(x_1) + \ldots + f(x_m),$$

поэтому, рассуждая как и выше, мы придем к заключению, что $t(g)$ попадает в одно из слагаемых M_0 решетки M_0^m. Но тогда $M_0 = t(L_1) \perp (M_0 \cap t(L_2))$, что противоречит неразложимости M_0.

Чтобы завершить наше построение, остается подобрать число m таким образом, чтобы решетки L_0^m и M_0^m оказались свободными. Для этого достаточно положить m равным экспоненте группы классов идеалов поля F. В самом деле, любая решетка $L \subset K^n$ допускает представление вида $L = \mathcal{O}x_1 \oplus \ldots \oplus \mathcal{O}x_{n-1} \oplus \mathfrak{a}x_n$, где $\mathfrak{a} \subset \mathcal{O}$ — некоторый идеал (см. § 1.5, п. 3). Тогда L^m допускает представление вида $\mathcal{O}y_1 \oplus \ldots \oplus \mathcal{O}y_{mn-1} \oplus \mathfrak{a}^m y_m$. Но идеал $\mathfrak{a}^m$ становится главным, и поэтому решетка L^m свободна.

Следует обратить внимание на то обстоятельство, что в основе построения примера лежит существование расширений, неразветвленных во всех точках. Поэтому над $\mathbb{Q}$ такая конструкция принципиально невозможна в силу теоремы Эрмита.

Библиографические замечания. Основные результаты в теории приведения были получены Борелем и Хариш-Чандрой [2]. Изложенное нами в § 4.5 доказательство критерия компактности факторпространства $G_{\mathbb{R}}/G_{\mathbb{Z}}$ принадлежит Мостову и Тамагаве [1]. Вывод конечной представимости арифметических групп из существования для них открытого фундаментального множества (теорема 2) был проделан Бером [1]. Теорема плотности доказана Борелем в [5]. Наше изложение теории приведения не претендует на полноту. Более обстоятельное изложение можно найти в книге Бореля [7] и его лекциях [6]. Элементарным введением в теорию приведения может служить книга Хамфри [2]. Как мы уже отмечали, истоки общей теории приведения лежат в теории приведения квадратичных форм, современное изложение которой содержится в книге Касселса [1]. Менее традиционен материал § 4.8. Основные результаты здесь принадлежат Бартельсу [1—2], Китаоке [1—2] и Бартельсу — Китаоке [1].

ГЛАВА V

АДЕЛИ

В настоящей главе вводятся группы аделей. Это понятие играет центральную роль в арифметической теории алгебраических групп. Подобно тому как на языке иделей и их когомологий могут быть выражены основные результаты теории полей классов, так на языке групп аделей алгебраических групп и связанных с ними конструкций и понятий выражаются результаты некоммутативной арифметики. Поэтому работать с аделями мы будем на протяжении всей книги, и основой для этого послужат результаты данной главы. Вот ее краткое содержание. В § 5.1 мы определяем группу аделей G_A линейной алгебраической группы G над числовым полем K и наделяем ее соответствующей (адельной) топологией. При этом группа K-рациональных точек G_K оказывается дискретной подгруппой в G_A, и можно ставить вопрос о построении теории приведения для G_A относительно G_K. Эту задачу мы решаем в § 5.2—5.3. Часть результатов здесь (например, критерий компактности пространства G_A/G_K) полностью аналогична соответствующим результатам гл. IV и, в действительности, в существенной степени на них опирается. Другие результаты носят специфически адельный характер. К их числу прежде всего относится важная теорема 1 о конечности числа классов $G_{A(\infty)}xG_K$ в разложении группы аделей G_A по подгруппам целых главных аделей соответственно. Это число, называемое *числом классов* алгебраической группы G, является очень важной арифметической характеристикой группы G, а его вычисление тесно связано с классическими теоретико-числовыми проблемами (см. гл. VIII). Другой возникающий здесь инвариант — так называемое *число Тамагавы* $\tau(G)$ группы G, равное для полупростой группы объему факторпространства G_A/G_K. Используя результаты теории приведения, мы в § 5.4 переносим структурные результаты об арифметических подгруппах (см. § 4.4) на произвольные S-арифметические группы.

§ 5.1. Основные определения

Введем понятие *пространства аделей* X_A произвольного многообразия X над полем алгебраических чисел K. Для этого сначала будем считать многообразие X аффинным и зафиксируем

реализацию X в виде K-замкнутого подмножества аффинного пространства $\mathbb{A}^n$. Тогда по определению X_A есть совокупность точек X над кольцом аделей $A = A_K$ поля K (см. § 1.2). Другими словами, элементами X_A являются наборы $(a_1, \ldots, a_n)$, состоящие из аделей, которые удовлетворяют всем уравнениям, определяющим X. Естественно наделить X_A топологией, которая индуцируется топологией прямого произведения на пространстве $A^n = A \times \ldots \times A$. При этом оказывается, что тот же объект можно получить, исходя из конструкции ограниченного прямого произведения (см. § 3.5). В самом деле, рассмотрев проекцию π_v: $A \to K_v$ на v-компоненту и ее n-мерное продолжение π_v^n: $A^n \to K_v^n$, мы будем иметь, что проекция $\pi_v^n(x)$ любой точки $x \in X_A$ лежит в X_{K_v} для любого $v \in V^K$, причем для всех v, кроме конечного числа, эта проекция попадает на самом деле во множество $\mathcal{O}_v$-точек $X_{\mathcal{O}_v}$.

Легко видеть, что выполнима также обратная процедура восстановления точки $x \in X_A$ по заданным проекциям $\pi_v^n(x)$ при условии, что последние лежат в $X_{\mathcal{O}_v}$ для почти всех v. Тем самым X_A оказывается *ограниченным топологическим произведением* пространств X_{K_v} относительно выделенных открытых подпространств $X_{\mathcal{O}_v}$, причем не только в теоретико-множественном, но и в топологическом смысле. Отсюда вытекает представимость X_A в виде объединения

$$X_A = \bigcup_S X_{A(S)} \tag{1}$$

по всем конечным подмножествам $S \subset V^K$, содержащим V_∞^K, пространств S-целых аделей $X_{A(S)} = \prod_{v \in S} X_{K_v} \times \prod_{v \notin S} X_{\mathcal{O}_v}$ (если $S = V_\infty^K$, то говорят просто о *целых аделях*, которые обозначают $X_{A(\infty)}$). При этом топология на $X_{A(S)}$ является обычной топологией прямого произведения, а топология на X_A восстанавливается отсюда как топология индуктивного предела.

Диагональное вложение $K \to A$ (см. § 1.2) индуцирует диагональное вложение множества K-точек X_K в X_A; образ этого вложения, который мы, как правило, будем отождествлять с X_K, называется *пространством главных аделей*. Следует отметить, что из дискретности K в A вытекает дискретность K^n в A^n, следовательно, дискретность (и замкнутость) X_K в X_A.

Следующим шагом в обосновании конструкции аделей является доказательство ее независимости от выбора геометрической реализации X. С этой целью введем понятие *аделизации регулярного K-определенного отображения* f: $X \to Y$ двух аффинных K-определенных замкнутых подмножеств $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$. Как мы знаем, для любого $v \in V^K$ такое отображение индуци-

рует непрерывное отображение $f_{K_v}\colon X_{K_v} \to Y_{K_v}$. Рассмотрим произведение $\prod_v f_{K_v}$ по всем v и обозначим через f_A его ограничение на X_A.

Лемма 1. *$f_A(X_A) \subset Y_A$, и отображение $f_A\colon X_A \to Y_A$ непрерывно.*

Доказательство. Отображение f в координатах имеет вид

$$(x_1, \ldots, x_n) \longmapsto (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)),$$

где f_i — полиномы с коэффициентами из K. Обозначим через S_0 такое конечное подмножество в V^K, содержащее V^K_∞, что коэффициенты всех f_i являются v-целыми для $v \notin S_0$. Тогда ясно, что $f_{K_v}(X_{\mathcal{O}_v}) \subset Y_{\mathcal{O}_v}$ для $v \notin S_0$, и поэтому $f_A(X_{A(S)}) \subset Y_{A(S)}$ для любого подмножества $S \subset V^K$, содержащего S_0. Далее, учитывая тот факт, что топология на $X_{A(S)}$ является топологией прямого произведения, получаем непрерывность ограничения $f_A|_{X_{A(S)}}$. Теперь остается воспользоваться представимостью X_A и Y_A в виде объединения (1). Лемма доказана.

Из леммы 1 легко получается

Предложение 1. *Пусть $f\colon X \to Y$ — определенный над K бирегулярный изоморфизм двух K-определенных замкнутых подмножеств $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$. Тогда отображение $f_A\colon X_A \to Y_A$ является гомеоморфизмом.*

Действительно, если $g\colon Y \to X$ — обратное к f регулярное K-определенное отображение, то по лемме 1 $g_A\colon Y_A \to X_A$ является непрерывным отображением, очевидно, обратным к f_A.

Для работы с линейными алгебраическими группами в большинстве случаев вполне достаточно приведенных выше определений. Однако мы потратим еще несколько абзацев на то, чтобы определить пространство аделей X_A для произвольного K-многообразия X и обосновать корректность этого определения. С одной стороны, это позволит соблюсти разумную полноту изложения, с другой — описать подход, при помощи которого получаются результаты, представляющие интерес также и в аффинном случае.

Итак, пусть X — произвольное K-определенное многообразие. Чтобы определить X_A, нужно для каждого $v \in V^K_f$ выделить в X_{K_v} открытое компактное подмножество $X_{\mathcal{O}_v}$ целых v-адических точек и построить ограниченное топологическое произведение X_{K_v} относительно $X_{\mathcal{O}_v}$. Для определения $X_{\mathcal{O}_v}$ воспользуемся конечным покрытием $X = \bigcup X_i$ многообразия X открытыми аффинными K-определенными множествами X_i (такое покрытие существует по определению многообразия). Далее, для каждого i зафиксируем K-определенный бирегулярный изоморфизм $f_i\colon X_i \to X_i^0$ на K-замкнутое подмножество $X_i^0 \subset \mathbb{A}^{n_i}$.

Тогда по определению положим

$$X_{\mathcal{O}_v} = \bigcup_i f_i^{-1}\left(X^0_{i_{\mathcal{O}_v}}\right)$$

для любого $v \in V_f^K$ и введем X_A как соответствующее ограниченное произведение. (Эквивалентным образом можно положить $X_A = \bigcup_i f_{i_A}^{-1}\left(X^0_{i_A}\right)$, где $f_{i_A}^{-1}\left(X^0_{i_A}\right)$ рассматривается как подмножество в $\prod_v X_{K_v}$.) Доказательство инвариантности этой конструкции опирается на обобщение леммы 1 на случай произвольных многообразий.

Лемма 2. *Пусть $f\colon X \to Y$ — определенный над K морфизм произвольных K-многообразий. Тогда $f_A(X_A) \subset Y_A$ и отображение $f_A\colon X_A \to Y_A$ непрерывно.*

(Отметим, что как и в аффинном случае, *аделизация* f_A морфизма f определяется как ограничение на X_A произведения $\prod_v f_{K_v}$.)

Доказательство. Как показывает доказательство леммы 1, в обосновании нуждается лишь тот факт, что $f(X_{\mathcal{O}_v}) \subset Y_{\mathcal{O}_v}$ для почти всех v. Так как по определению $X_{\mathcal{O}_v} = \bigcup_i f_i^{-1}\left(X^0_{i_{\mathcal{O}_v}}\right)$ — конечное объединение, то достаточно показать, что для любого i и почти всех v выполняется включение

$$\left(f \circ f_i^{-1}\right)\left(X^0_{i_{\mathcal{O}_v}}\right) \subset Y_{\mathcal{O}_v}.$$

Таким образом, можно с самого начала считать, что $i = 1$, т. е. многообразие X аффинно. Пусть $Y = \bigcup Y_j$ — конечное аффинное покрытие, при помощи которого определяется $Y_{\mathcal{O}_v}$. Зафиксируем вложения $X \subset \mathbb{A}^n$, $Y_j \subset \mathbb{A}^{n_j}$ в соответствующие аффинные пространства, координаты в которых мы будем обозначать через $x_1, \ldots, x_n$; $y_1^j, \ldots, y_{n_j}^j$. Тогда для любого j отображение f записывается в виде рационального выражения функций y_k^j через x_i:

$$y_k^j = \varphi_k/\psi, \quad k = 1, \ldots, n_j, \tag{2}$$

где φ_k, ψ берутся из кольца регулярных K-определенных функций $K[X]$. Разумеется, представление вида (2) не единственно. Поэтому для того чтобы учесть все представления, для каждого j рассмотрим идеал возможных знаменателей

$$a_j = \{\psi \in K[X] \mid \psi y_k^j \in K[X] \text{ для всех } k = 1, \ldots, n_j\}.$$

Образ $f(x)$ любой точки $x \in X$ лежит в одном из Y_j. Это значит, что для каждого $x \in X$ найдется индекс j, для которого

все функции y_k^j, $k=1, \ldots, n_j$ определены в x, т. е. существует представление $y_k^j=\varphi_{kx}/\psi_x$ вида (2) со свойством $\psi_x(x)\neq 0$. Следовательно, идеал в $K[X]$, порожденный всеми $\mathfrak{a}_j$, не имеет нулей на X, и поэтому совпадает с $K[X]$ (теорема Гильберта о нулях, см., например, Хамфри [1]). Таким образом, существуют такие $\psi_j\in\mathfrak{a}_j$, что $\sum\psi_j=1$. Выберем соответствующие представления $y_k^j=\varphi_k^j/\psi_j$ вида (2), и пусть Φ_k^j, Ψ_j — представляющие φ_k^j, ψ_j полиномы из $K[x_1, \ldots, x_n]$. Тогда для почти всех $v\in V^f$ коэффициенты этих полиномов являются целыми относительно v. Утверждается, что для таких v выполняется требуемое включение $f(X_{\mathcal{O}_v})\subset Y_{\mathcal{O}_v}=\bigcup Y_{j\mathcal{O}_v}$. В самом деле, пусть $x\in X_{\mathcal{O}_v}$. Так как $\psi_j(x)\in\mathcal{O}_v$ для любого j и $\sum\psi_j(x)=1$, то все $\psi_j(x)$ не могут лежать в максимальном идеале $\mathfrak{p}_v$ кольца $\mathcal{O}_v$. Поэтому найдется j, для которого значение $\psi_j(x)$ обратимо в $\mathcal{O}_v$. Но тогда соответствующие значения y_k^j, очевидно, лежат в $\mathcal{O}_v$, т. е. $f(x)\in Y_{j\mathcal{O}_v}$, что и требовалось. Лемма 2 доказана.

Предложение 2. *Пусть $f\colon X\to Y$ — определенный над K изоморфизм K-многообразий. Тогда отображение $f_A\colon X_A\to Y_A$ является гомеоморфизмом. В частности, пространство X_A не зависит от выбора аффинного покрытия.*

Первое утверждение немедленно следует из леммы 2 (ср. доказательство предложения 1). Второе утверждение вытекает из первого, если рассмотреть два аффинных покрытия X и взять в качестве f тождественное отображение между двумя экземплярами X, снабженными этими покрытиями. Отсюда, в частности, вытекает, что для аффинных многообразий оба определения пространства аделей эквивалентны.

Имеется, однако, существенное топологическое отличие общего случая от аффинного. А именно, пространство главных аделей X_K, определение которого ничем не отличается от аффинного случая, не является, вообще говоря, дискретным в X_A. Так, например, для проективного многообразия X пространство X_A компактно, и поэтому X_K не может быть дискретным в X_A, если оно бесконечно. Отметим одно любопытное следствие предложения 2.

Лемма 3. *Пусть $X=\bigcup X_i$ — произвольное покрытие K-многообразия X открытыми K-многообразиями X_i. Тогда $X_A=\bigcup X_{iA}$.*

Действительно, выбирая из рассматриваемого открытого покрытия конечное подпокрытие, можно с самого начала считать исходное покрытие конечным. Тогда из определения пространства X_A вытекает, что наше утверждение справедливо, если многообразия X_i аффинны. Чтобы получить доказательство в общем случае, для каждого i рассмотрим некоторое конечное открытое аффинное покрытие соответствующего X_i: $X_i=\bigcup\limits_k X_{ik}$.

Тогда $X=\bigcup_{i,k} X_{ik}$ — открытое аффинное покрытие X. Так как согласно предложению 2 определение X_A не зависит от выбора открытого аффинного покрытия, то $X_A=\bigcup_{i,k} X_{ikA}$. С другой стороны, для любого i по аналогичным причинам $X_{iA}=\bigcup_k X_{ikA}$, откуда и следует требуемое.

Заметим, что требование открытости всех X_i существенно. Действительно, рассмотрим разбиение $\mathbb{A}^1=X\cup Y$, где $X=\mathbb{A}^1\setminus(0)$, $Y=\{(0)\}$. Тогда X бирегулярно изоморфно гиперболе $\{(x, y)\in\mathbb{A}^2 \mid xy=1\}$, откуда следует, что X_A совпадает с множеством всех иделей J, а $Y_A=\{(0)\}$. Поэтому $\mathbb{A}^1_A=A\neq X_A\cup Y_A$. (Мы рекомендуем читателю в качестве небесполезного упражнения выяснить, какое место в доказательстве леммы 3 не проходит, если не предполагать покрытие $\{X_i\}$ открытым.)

Нам понадобится также

Лемма 4. *Пусть $Y\subset X$ — замкнутое K-определенное подмногообразие. Тогда $Y_A=X_A\cap\prod_v Y_{K_v}$. При этом топология на Y_A индуцируется с X_A.*

Доказательство. Пусть $X=\bigcup_i X_i$ — открытое аффинное покрытие многообразия X. Тогда $Y=\bigcup_i (Y\cap X_i)$ — открытое аффинное покрытие многообразия Y. Согласно данным выше определениям $Y_A=\bigcup_i (Y\cap X_i)_A$. Но для замкнутого подмножества аффинного многообразия утверждение леммы, очевидно, выполняется. (Чтобы убедиться в этом, достаточно рассмотреть произвольное вложение X в качестве замкнутого подмножества в аффинное пространство; тогда мы одновременно получим замкнутое вложение Y, и требуемое немедленно вытекает из определений.) Поэтому для любого i

$$(Y\cap X_i)_A=X_{iA}\cap\prod_v (Y\cap X_i)_{K_v}=X_{iA}\cap\prod_v Y_{K_v},$$

откуда

$$Y_A=\bigcup_i (Y\cap X_i)_A=\bigcup_i\left(X_{iA}\cap\prod_v Y_{K_v}\right)=$$
$$=\left(\bigcup_i X_{iA}\right)\cap\prod_v Y_{K_v}=X_A\cap\prod_v Y_{K_v}.$$

Доказательство того, что топология на Y_A индуцируется с X_A, предоставляется читателю в качестве упражнения (ср. доказательство непрерывности f_A в лемме 1).

Упражнение. Показать, что если $X=Y\times Z$, то $X_A=Y_A\times Z_A$ как топологическое пространство.

Работая с аделизациями многообразий и их морфизмов, полезно знать, какие наиболее употребительные свойства сохраняются или не сохраняются при переходе к адельным точкам. Ясно, например, что сюръективности морфизма $f\colon X \to Y$ недостаточно для сюръективности соответствующей аделизации $f_A\colon X_A \to Y_A$ (пример?). Тем не менее если многообразие Y неприводимо и для любого расширения F/K сюръективен морфизм $f_F\colon X_F \to Y_F$ соответствующих F-точек, то f_A также сюръективно. Действительно, применяя условие сюръективности к полю $F = K(Y)$ K-определенных рациональных функций на Y, мы получим, что для любой точки $y \in Y$ имеется определенное в y локальное сечение морфизма f, т. е. такой рациональный K-определенный морфизм $g_y\colon Y \to X$, что $f \circ g_y = id_Y$, и можно воспользоваться следующим утверждением:

Предложение 3. *Пусть $f\colon X \to Y$ — определенный над K морфизм K-многообразий. Если для каждой точки $y \in Y$ существует определенное в y локальное сечение (над K) морфизма f, то отображение $f_A\colon X_A \to Y_A$ сюръективно.*

Доказательство. Из условия вытекает существование такого открытого покрытия $Y = \bigcup Y_j$ и таких K-подмногообразий $X_j \subset X$, что f осуществляет K-определенный изоморфизм X_j и Y_j. (Действительно, в качестве Y_j достаточно взять области определения всевозможных локальных сечений, а в качестве X_j — их образы.) Тогда в силу предложения 2 и леммы 3 имеем

$$f_A(X_A) \supset \bigcup_j f_A(X_{jA}) = \bigcup_j Y_{jA} = Y_A.$$

В дальнейшем мы еще не раз встретимся с различными свойствами аделизаций морфизмов, однако в рамках настоящего параграфа мы на этом заканчиваем обсуждение адельных точек произвольных многообразий и переходим к наиболее важному для нас случаю линейных алгебраических групп.

Итак, пусть G — определенная над K линейная алгебраическая группа. Тогда G реализуется в качестве замкнутой K-определенной подгруппы некоторой полной линейной группы $\boldsymbol{GL}_n$, и согласно лемме 4 для описания G_A, фактически, достаточно описать $\boldsymbol{GL}_{nA}$. Для этого рассмотрим стандартную реализацию $\boldsymbol{GL}_n$ в качестве гиперповерхности в $\mathbb{A}^{n^2+1}$:

$$\boldsymbol{GL} \simeq \{(x_{11}, \ldots, x_{nn}, y) \in \mathbb{A}^{n^2+1} \mid y \det(x_{ij}) - 1 = 0\}.$$

Тогда GL_{nA} совпадает со множеством всех матриц из $M_n(A)$, определитель которых обратим в кольце аделей A, т. е. с $GL_n(A)$. Чтобы представить себе GL_{nA} с точки зрения ограниченного топологического произведения, следует отметить, что здесь также $GL_{n\mathcal{O}_v}$ совпадает с $GL_n(\mathcal{O}_v)$, так что $GL_{nA} = GL_n(A)$ является ограниченным топологическим произведением групп $GL_n(K_v)$

относительно выделенных подгрупп $GL_n(\mathcal{O}_v)$ для $v \in V_f^K$. Другими словами, GL_{nA} совпадает со множеством всех таких наборов $g=(g_v) \in \prod_v GL_n(K_v)$, что g_v лежит в $GL_n(\mathcal{O}_v)$ для почти всех $v \in V_f^K$. Топология на GL_{nA} выглядит следующим образом: базу открытых множеств образуют множества вида

$$U = \prod_{v \in S} U_v \times \prod_{v \notin S} GL_n(\mathcal{O}_v), \tag{3}$$

где S — конечное подмножество V^K, содержащее V_∞^K, элементам которого отвечают открытые подмножества $U_v \subset GL_n(K_v)$ (отметим, что иногда с целью унификации обозначений полагают $\mathcal{O}_v = K_v$ для $v \in V_\infty^K$, однако мы этого делать не будем). Подгруппа $GL_{nA(S)} = GL_n(A(S)) = \prod_{v \in S} GL_n(K_v) \times \prod_{v \notin S} GL_n(\mathcal{O}_v)$ называется *группой S-целых аделей*; для $S = V_\infty^K$ группа $GL_{nA(S)}$ обозначается через $GL_{nA(\infty)}$ и называется *группой целых аделей*. Группа GL_{nK} диагональным образом вкладывается в GL_{nA}, и ее образ, который мы обычно с ней отождествляем, называется *группой главных аделей*; она является дискретной подгруппой в GL_{nA}. Приведенное нами подробное обсуждение основных адельных понятий применительно к группе $\boldsymbol{GL}_n$ адресовано читателю, который впервые сталкивается с аделями алгебраических групп. Ему мы рекомендуем также обратиться к гл. V книги Хамфри [2], которая содержит введение в общую теорию адельных групп именно на примере групп $\boldsymbol{GL}_n$ и $\boldsymbol{SL}_n$.

Распространение данных выше определений на произвольную замкнутую подгруппу $G \subset \boldsymbol{GL}_n$ теперь не представляет труда. А именно, *группа аделей* G_A определяется как ограниченное топологическое произведение всех групп G_{K_v} относительно выделенных подгрупп $G_{\mathcal{O}_v} = G \cap GL_n(\mathcal{O}_v)$ для $v \in V_f^K$, т. е. G_A состоит из наборов $g=(g_v) \in \prod_v G_{K_v}$ таких, что $g_v \in G_{\mathcal{O}_v}$ для почти всех $v \in V_f^K$. Топология на G_A является индуцированной с GL_{nA}, и поэтому ее базу образуют множества, аналогичные (3). Относительно этой топологии группа G_A является локально компактной топологической группой, а подгруппа главных аделей G_K (т. е. группа K-рациональных точек G_K, диагонально вложенная в G_A) — дискретной подгруппой в G_A. Для любого конечного подмножества $S \subset V^K$, содержащего V_∞^K, определяется *подгруппа S-целых аделей* $G_{A(S)} = G_S \times \prod_{v \notin S} G_{\mathcal{O}_v}$, где $G_S = \prod_{v \in S} G_{K_v}$ (очевидно, $G_{A(S)}$ — открытое множество в G_A). При $S = V_\infty^K$ мы пишем $G_{A(\infty)}$, G_∞ вместо $G_{A(V_\infty^K)}$, $G_{V_\infty^K}$. Обратим внимание на тот факт,

что группы $G_{\mathcal{O}_v}$, а следовательно, и группа *целых аделей* $G_{A(\infty)}$ зависят от выбора матричной реализации G, поэтому, желая подчеркнуть, что целые точки берутся относительно решетки $L \subset K^n$, будем писать $G^L_{A(\infty)}$, подразумевая под этим $G_\infty \times \times \prod_{v \in V_f^K} G^{L_v}_{\mathcal{O}_v}$, где L_v — соответствующая локализация решетки L (см. § 1.5, п. 3).

В ряде случаев бывает удобно (и необходимо) рассматривать «усеченные» адели. Более точно, пусть S — произвольное подмножество в V^K. Тогда группа S-аделей G_{A_S} (аделей без S-компонент) алгебраической K-группы G определяется как образ G_A при естественной проекции $\prod_v G_{K_v}$ на $\prod_{v \notin S} G_{K_v}$. Таким образом, G_{A_S} состоит из наборов $g = (g_v) \in \prod_{v \notin S} G_{K_v}$, таких, что $g_v \in G_{\mathcal{O}_v}$ для почти всех $v \in V_f^K \setminus (V_f^K \cap S)$, и тем самым является ограниченным произведением групп G_{K_v} для $v \notin S$ относительно выделенных подгрупп $G_{\mathcal{O}_v} (v \in V_f^K \setminus S)$ как с теоретико-множественной, так и с топологической точки зрения. Как и в случае полных групп аделей, для S-аделей можно рассмотреть диагональное вложение $G_K \hookrightarrow G_{A_S}$, образ которого называется группой главных S-аделей, и, кроме того, для любого подмножества $T \subset V^K$, содержащего $S \cup V_\infty^K$, определить группу T-целых S-аделей $G_{A_S(T)} = \prod_{v \in T \setminus S} G_{K_v} \times \prod_{v \notin T} G_{\mathcal{O}_v}$. Группа $G_{A_{V_\infty^K}}$ обозначается через G_{A_f} и называется *группой конечных аделей*; при этом вместо $G_{A_f(V_\infty^K)}$ мы пишем $G_{A_f(\infty)}$. С этими понятиями связано следующее важное

Определение. *Говорят, что группа G обладает сильной аппроксимацией относительно множества S, если диагональное вложение $G_K \hookrightarrow G_{A_S}$ имеет плотный образ (в терминах полной группы аделей это означает, что произведение $G_K G_S$, где $G_S = \prod_{v \in S} G_{K_v}$, плотно в G_A). При $S = V_\infty^K$ говорят об абсолютной сильной аппроксимации.*

Аналогично вводится понятие пространства S-аделей и определение сильной аппроксимации для произвольного алгебраического многообразия (при этом, естественно, имеют место аналоги всех предшествовавших результатов этого параграфа). Однако в отличие от случая алгебраических групп, где критерий сильной аппроксимации известен (см. § 7.4), для произвольных многообразий сильная аппроксимация только начинает изучаться (см. Минчев [1], Рапинчук [8]). Тем не менее использование самого понятия сильной аппроксимации для произвольных

многообразий позволяет получить некоторые упрощения, как видно, например, из доказательства следующего утверждения.

Лемма 5. *Пусть U — определенная над K унипотентная группа. Тогда U обладает сильной аппроксимацией относительно любого непустого множества S.*

Доказательство построено на следующем простом замечании. Если два K-многообразия X и Y бирегулярно изоморфны над K, то $X_K \simeq Y_K$, $X_{A_S} \simeq Y_{A_S}$ для любого S; поэтому X и Y одновременно обладают или не обладают сильной аппроксимацией. (Вопрос для самоконтроля: сохраняется ли свойство сильной аппроксимации при бирациональных K-изоморфизмах?) В нашей ситуации U бирегулярно изоморфна аффинному пространству (а именно, соответствующей алгебре Ли $L(U)$, см. § 2.1, п. 8), поэтому достаточно установить сильную аппроксимацию для аффинного пространства, где она немедленно вытекает из сильной аппроксимационной теоремы для поля K (см. § 1.2). Лемма доказана.

Другое важное понятие связано с подгруппами $G_{A(\infty)}$ и G_K целых и главных аделей. Пусть $G_A = \bigcup_{i=1}^{h} G_{A(\infty)}\, x_i\, G_K$ — разложение группы аделей G_A на двойные смежные классы по этим подгруппам. Тогда число h называется *числом классов алгебраической группы* G и обозначается через $\mathrm{cl}(G)$. Следующая теорема является одним из наиболее важных результатов главы.

Теорема 1. *Число* $\mathrm{cl}(G)$ *всегда конечно.*

Вычислением и оценкой чисел $\mathrm{cl}(G)$ мы будем заниматься в гл. VIII. Там мы, в частности, увидим, что из теоремы 1 вытекает большинство известных результатов о конечности, а именно: конечность числа классов идеалов поля, конечность числа классов в роде квадратичной формы и т. д. Теорема 1 является следствием теории приведения для групп аделей, которую мы изложим в § 5.2—5.3. А в завершение этого параграфа приведем несколько простых утверждений, которые позволят нам редуцировать доказательство теоремы 1 к случаю связных редуктивных групп над $\mathbb{Q}$.

Предложение 4. *Пусть $G = HN$ — полупрямое произведение подгруппы H и нормального делителя N (все определено над K). Предположим, что N обладает свойством абсолютной сильной аппроксимации. Тогда* $\mathrm{cl}(G) \leqslant \mathrm{cl}(H)$. *В частности, для группы, обладающей абсолютной сильной аппроксимацией, число классов всегда равно единице.*

Доказательство использует следующую лемму.

Лемма 6. *В описанной ситуации N_A является нормальным делителем в G_A и $G_A = H_A N_A$ — полупрямое произведение.*

Доказательство использует то же наблюдение, что и лемма 5. Так как $G \simeq H \times N$ как многообразие, то $G_A \simeq H_A \times N_A$, т. е. $G_A = H_A N_A$. Утверждение о нормальности N_A в G_A очевидно.

Для любого $x \in G_A$ подгруппа $x^{-1}N_{A(\infty)}x$ открыта в N_A. С другой стороны, поскольку N обладает абсолютной сильной аппроксимацией, произведение $N_\infty N_K$ плотно в N_A. Поэтому для любого $y \in N_A$ открытое множество $(x^{-1}N_{A(\infty)}x)y$ обязано пересекаться с $N_\infty N_K$, откуда

$$N_A = (x^{-1}N_{A(\infty)}x)\, N_\infty N_K = (x^{-1}N_{A(\infty)}x)\, N_K, \tag{4}$$

ибо N_∞ является нормальным делителем в G_A, содержащимся в $N_{A(\infty)}$. Полагая $x = 1$, получаем $N_A = N_{A(\infty)}N_K$, так что из (4) вытекает соотношение

$$xN_{A(\infty)}N_K = N_{A(\infty)}xN_K$$

для любого $x \in G_A$. Поэтому, используя лемму 6, получаем

$$G_A = H_A N_A = H_A N_{A(\infty)} N_K = N_{A(\infty)} H_A N_K.$$

Если теперь $H_A = \bigcup_i H_{A(\infty)} x_i H_K$, то $G_A = \bigcup_i N_{A(\infty)} H_{A(\infty)} x_i H_K N_K = \bigcup_i G_{A(\infty)} x_i G_K$, откуда и следует требуемое. Предложение 4 доказано.

Предложение 5. *Пусть G — K-определенная алгебраическая группа, G^0 — ее связная компонента. Тогда факторгруппа G_A/G_A^0 компактна.*

Доказательство. Так как G^0 имеет конечный индекс в G, то для любого v найдется такое конечное подмножество $C_v \subset G_{K_v}$, что $G_{K_v} = C_v G^0_{K_v}$. Более того, как мы покажем ниже, для почти всех $v \in V_f^K$ такое подмножество можно найти уже в группе $G_{\mathcal{O}_v}$. В этом случае $C = \prod_v C_v$ лежит в группе $G_{A(S)}$ для подходящего конечного S и, следовательно, компактно в адельной топологии, ибо последняя совпадает на $G_{A(S)}$ с топологией прямого произведения. С другой стороны, очевидно, $G_A = CG_A^0$, и требуемое доказано.

Итак, осталось показать, что $G_{K_v} = G_{\mathcal{O}_v} G^0_{K_v}$ для почти всех $v \in V_f^K$. Для этого воспользуемся следующим фактом, в справедливости которого мы убедимся в § 6.2: если H — связная алгебраическая группа над полем алгебраических чисел K, L/K — некоторое конечное расширение Галуа, то для почти всех $v \in V_f^K$ и $w|v$ имеем $H^1(L_w/K_v, H_{\mathcal{O}_{L_w}}) = 1$, где $\mathcal{O}_{L_w}$ — кольцо целых w-адических чисел в L_w. В нашей ситуации существует такое конечное расширение Галуа L/K и такое конечное подмножество $C \subset G_L$, что $G = CG^0$. Исключая из рассмотрения

конечное число $v \in V_f^K$, можно считать, что морфизм $G \xrightarrow{\pi} G/G^0$ определен над $\mathcal{O}_v$ и для любого $w \mid v$ имеем $C \subset G_{\mathcal{O}_{L_w}}$ и $H^1\left(L_w/K_v, G^0_{\mathcal{O}_{L_w}}\right) = 1$. В частности, имеет место точная последовательность.

$$1 \to G^0_{\mathcal{O}_{L_w}} \to G_{\mathcal{O}_{L_w}} \to \left(G/G^0\right)_{\mathcal{O}_{L_w}} \to 1. \tag{5}$$

Переходя в (5) к когомологиям (см. точную последовательность (7) в § 1.3), получим, что $\pi\left(G_{\mathcal{O}_v}\right) = (G/G^0)_{\mathcal{O}_v}$. Но по построению $(G/G^0)_{\mathcal{O}_{L_w}} = (G/G^0)_{L_w}$, откуда $(G/G^0)_{\mathcal{O}_v} = (G/G^0)_{K_v}$. Поэтому $\pi\left(G_{K_v}\right) \subset \subset \left(G/G^0\right)_{K_v} = \left(G/G^0\right)_{\mathcal{O}_v} = \pi\left(G_{\mathcal{O}_v}\right)$, и, следовательно, $G_{K_v} = G_{\mathcal{O}_v} G^0_{K_v}$. Предложение 5 доказано.

Наконец, исследуем, как действует на адели конструкция ограничения основного поля (см. § 2.1, п. 2). А именно, пусть G — линейная алгебраическая группа, определенная над числовым полем K, $[K:\mathbb{Q}] = d$. Зафиксируем некоторый базис $\omega_1, \ldots, \omega_d$ кольца целых $\mathcal{O}$ над $\mathbb{Z}$ и с его помощью построим группу $H = \mathbf{R}_{K/\mathbb{Q}}(G)$. В п. 2 § 2.1 мы отмечали, что для любого простого p имеют место согласованные изоморфизмы

$$H_{\mathbb{Q}_p} \simeq \prod_{v \mid p} G_{K_v}, \tag{6}$$

$$H_{\mathbb{Z}_p} \simeq \prod_{v \mid p} G_{\mathcal{O}_v} \tag{7}$$

и, кроме того,

$$H_{\mathbb{R}} \simeq G_\infty. \tag{8}$$

Отсюда вытекает

Предложение 6. *В приведенных выше обозначениях существует естественный изоморфизм $H_{A_\mathbb{Q}} \simeq G_{A_K}$, продолжающий изоморфизм $H_\mathbb{Q} \simeq G_K$. При этом $H_{A_\mathbb{Q}(\infty)} \simeq G_{A_K(\infty)}$.*

Отметим, что при другом выборе базиса $\omega'_1, \ldots, \omega'_d$ поля K над $\mathbb{Q}$ группа H меняется на группу H', которая K-изоморфна H, и поэтому всегда $H'_{A_\mathbb{Q}} \simeq G_{A_K}$. Это связано с тем обстоятельством, что изоморфизмы (6) и (8) остаются справедливыми и для H', а изоморфизм (7) выполняется для почти всех p. Ясно также, что если $\omega'_1, \ldots, \omega'_d$ не является базисом $\mathcal{O}/\mathbb{Z}$, то, вообще говоря, $H_{A_\mathbb{Q}(\infty)} \not\simeq G_{A_K(\infty)}$.

§ 5.2. Теория приведения для G_A относительно G_K

Как мы видели в предыдущем параграфе, группа G_K является дискретной подгруппой в G_A, и поэтому естественно ставить вопрос о построении теории приведения для G_A относительно G_K. В настоящем параграфе мы укажем конструкцию со-

ответствующих фундаментальных множеств, из которой выведем доказательство теоремы 1, а также критерии того, когда пространство G_A/G_K компактно или имеет конечную меру. Прежде всего дадим определение фундаментального множества для адельных групп.

Определение. *Подмножество $\Omega \subset G_A$ называется фундаментальным множеством для G_K, если*

$(\mathrm{F1})_A$ $\Omega G_K = G_A$;

$(\mathrm{F2})_A$ *пересечение* $\Omega^{-1}\Omega \cap G_K$ *конечно.*

Читатель, безусловно, отметит полную аналогию между указанными адельными условиями и условиями (F1) и (F2) из определения фундаментального множества для арифметических групп (см. § 4.3). В действительности связь здесь более глубокая, нежели простое внешнее сходство. А именно, построенные в гл. IV фундаментальные множества для арифметических групп входят в качестве вещественных компонент в адельные фундаментальные множества. Это видно уже из рассмотрения простейшего случая $G = \boldsymbol{GL}_n$ над $\mathbb{Q}$.

Предложение 7. *Пусть $G = \boldsymbol{GL}_n$ над полем $\mathbb{Q}$ и Σ — фундаментальное множество для $G_{\mathbb{Z}}$ в $G_{\mathbb{R}}$. Тогда $\Omega = \Sigma \times \prod_p G_{\mathbb{Z}_p}$ — фундаментальное множество для $G_{\mathbb{Q}}$ в G_A.*

Доказательство. Прежде всего покажем, что $\mathrm{cl}(G) = 1$, т. е. $G_A = G_{A(\infty)}G_{\mathbb{Q}}$. Группа G представляется в виде полупрямого произведения $G = SH$, где $S = \{\mathrm{diag}(a, 1, \ldots, 1)\}$ — одномерный тор, $H = \boldsymbol{SL}_n$. Очевидно, группу S_A можно отождествить с группой $J_{\mathbb{Q}}$ иделей поля $\mathbb{Q}$; при этом $S_{A(\infty)}$ переходит в группу $J_{\mathbb{Q}}(\infty)$ целых иделей. Так как число классов идеалов поля $\mathbb{Q}$ равно единице, то $J_{\mathbb{Q}} = J_{\mathbb{Q}}(\infty)\mathbb{Q}^*$ (см. § 1.2, п. 2) и, следовательно, $S_A = S_{A(\infty)}S_{\mathbb{Q}}$, т. е. $\mathrm{cl}(S) = 1$. С другой стороны, для группы H имеет место абсолютная сильная аппроксимация. Это следует из критерия сильной аппроксимации, который мы установим в § 7.4, но можно дать и элементарное прямое доказательство. Для этого обозначим через U_{ij} $(i, j = 1, \ldots, n;\ i \neq j)$ подгруппу в H, состоящую из соответствующих элементарных матриц. Так как U_{ij} обладает абсолютной сильной аппроксимацией (лемма 5), то замыкание $\overline{H}_{\mathbb{Q}}$ группы $H_{\mathbb{Q}}$ в H_{A_f} содержит все группы $(U_{ij})_{A_f}$. Учитывая, что для любого поля L матрицы из $(U_{ij})_L$ порождают H_L, получаем, что $\overline{H}_{\mathbb{Q}}$ содержит все группы $H_S = \prod_{p \in S} H_{\mathbb{Q}_p}$, где S — некоторое конечное множество простых чисел. Но из определения адельной топологии вытекает, что объединение $\bigcup_S H_S$ плотно в H_{A_f}, и поэтому $\overline{H}_{\mathbb{Q}} = H_{A_f}$. Применяя теперь предложение 5, мы и получим требуемое равенство

$\mathrm{cl}(G)=1$. (Если рассматривать группу $G=\boldsymbol{GL}_n$ над произвольным полем K, то здесь $\mathrm{cl}(G)$ совпадает с числом h_K классов идеалов поля K; см. § 8.1.) Теперь уже легко завершить доказательство предложения. Так как $\Sigma G_{\mathbb{Z}}=G_{\mathbb{R}}$, то $\Omega G_{\mathbb{Z}}=G_{\mathbb{R}}\times\prod_p G_{\mathbb{Z}_p}=G_{A(\infty)}$. Поэтому $\Omega G_{\mathbb{Q}}=\Omega G_{\mathbb{Z}}G_{\mathbb{Q}}=G_{A(\infty)}G_{\mathbb{Q}}=G_A$. Если же $g\in\Omega^{-1}\Omega\cap G_{\mathbb{Q}}$, то $g\in G_{\mathbb{Z}_p}$ для всех p, и, следовательно, $g\in G_{\mathbb{Z}}$. С другой стороны, проекция на вещественную компоненту дает $g\in\Sigma^{-1}\Sigma$ и, следовательно, возможностей для g имеется лишь конечное число (см. условие (F2) в определении фундаментального множества для арифметических подгрупп).

Как видно из доказательства предложения 7, фундаментальные множества указанного там вида существуют всякий раз, когда $\mathrm{cl}(G)=1$. Их характерная особенность — компактность проекции на неархимедову часть. Ниже мы увидим, что построить фундаментальные множества с таким свойством можно и в общем случае, и именно это приведет нас к доказательству теоремы конечности 1.

Методология построения фундаментальных множеств в группах аделей произвольных групп подобна той, которую мы применяли в гл. IV к аналогичной задаче для арифметических подгрупп, т. е. основывается на лемме 2 гл. IV. Разница заключается лишь в том, что здесь приходится работать с действиями групп не на векторных пространствах, а на их аделизациях. Для этого отметим, что действие алгебраической K-группы G на алгебраическом K-многообразии X, т. е. соответствующий морфизм $G\times X\to X$, индуцирует непрерывное отображение $(G\times X)_A=G_A\times X_A\to X_A$, т. е. непрерывное действие G_A на аделизации X_A. Кроме того, для $a\in GL_n(\mathbb{R})$ обозначим через a^∞ адель из $GL_n(A_{\mathbb{Q}})$ с компонентами

$$(a^\infty)_v=\begin{cases}E_n, & v\neq\infty,\\ a, & v=\infty.\end{cases}$$

Предложение 8. *Пусть $G\subset\boldsymbol{GL}_n$ — редуктивная $\mathbb{Q}$-определенная группа, Ω — фундаментальное множество из предложения 7, отвечающее области Зигеля $\Sigma=\Sigma_{t,v}$, $t\geqslant 2/\sqrt{3}$, $v\geqslant 1/2$ (см. § 4.2). Тогда найдутся такие $a\in GL_n(\mathbb{R})$, $b_1,\ldots,b_r\in GL_n(\mathbb{Q})$, что множество*

$$\Delta=\left(\bigcup_{i=1}^{r}a^\infty\Omega b_i\right)\cap G_A \tag{1}$$

является фундаментальным для $G_{\mathbb{Q}}$ в G_A.

Доказательство. Согласно теореме 2.15 найдется такое $\mathbb{Q}$-определенное представление ρ: $\boldsymbol{GL}_n\to\boldsymbol{GL}_m$ и вектор $v\in\mathbb{Q}^m$, что орбита этого вектора относительно $\boldsymbol{GL}_n$ замкнута, а стационарная подгруппа совпадает с G. Далее, выберем $a\in GL_n(\mathbb{R})$ та-

ким образом, чтобы группа $a^{-1}Ga$ была самосопряженной (теорема 7 гл. III). Тогда пересечение $v(a^\infty\Omega)\cap vGL_n(\mathbb{Q})$ конечно. (Здесь и далее рассматривается действие группы $GL_n(A)$ на пространстве аделей A^m, индуцированное ρ.) В самом деле, достаточно показать, что пересечение $M=v(a^\infty\Omega)\cap\mathbb{Q}^m$ конечно. Из определения Ω и непрерывности ρ_A вытекает, что проекции всех элементов из $v(a^\infty\Omega)$ на A_f^m лежат в некотором компактном множестве. Отсюда следует, что $M\subset\frac{1}{l}\mathbb{Z}^m$ для подходящего целого l. Но тогда $lM\subset(lv)\Sigma\cap\mathbb{Z}^m$, а последнее пересечение конечно в силу предложения 5 гл. IV.

Если теперь $v(a^\infty\Omega)\cap vGL_n(\mathbb{Q})=\{vb_1,\ \ldots,\ vb_r\}$, $b_i\in GL_n(\mathbb{Q})$, то применяя лемму 2 главы IV, с учетом предложения 7 получим, что множество Δ вида (1) является фундаментальным для $G_\mathbb{Q}$ в G_A. Предложение 8 доказано.

Теорема 2. *Пусть G — редуктивная алгебраическая группа, определенная над полем алгебраических чисел K. Тогда в G_A для G_K существует фундаментальное множество с компактной проекцией на неархимедову часть.*

Доказательство. Пусть $H=\mathbf{R}_{K/\mathbb{Q}}(G)$ — группа, получаемая из G ограничением основного поля. Тогда согласно предложению 8 в $H_{A_\mathbb{Q}}$ существует фундаментальное множество относительно $H_\mathbb{Q}$ вида (1), которое имеет компактную проекцию на неархимедову часть (ибо этим свойством обладает фундаментальное множество Ω, построенное в предложении 7). Используя изоморфизм $H_{A_\mathbb{Q}}\simeq G_A$ (см. предложение 6), его можно перенести в G_A, что и дает искомое фундаментальное множество для G_K в G_A.

Доказательство теоремы 1. Пусть вначале группа G связна. Рассмотрим разложение Леви $G=HU$, где $U=R_u(G)$ — унипотентный радикал G, а K-группа H редуктивна (теорема 2.3). Тогда из предложения 5 с учетом леммы 5 вытекает, что $\mathrm{cl}(G)\leqslant\mathrm{cl}(H)$, и достаточно установить конечность $\mathrm{cl}(H)$. Для этого используем фундаментальное множество $\Delta\subset H_A$, построенное в теореме 2. Так как Δ имеет компактную проекцию на неархимедову часть, то для подходящего конечного набора $x_1,\ \ldots,\ x_r$ элементов из H_A справедливо включение $\Delta\subset\bigcup_{i=1}^r H_{A(\infty)}x_i$. Но тогда $H_A=\Delta H_K=\bigcup_{i=1}^r H_{A(\infty)}x_iH_K$, и поэтому $\mathrm{cl}(H)$ конечно.

Пусть теперь группа G произвольна. Так как конечность $\mathrm{cl}(G^0)$ уже доказана, то найдется такой конечный набор $x_1,\ \ldots,\ x_r$ элементов из G_A^0, что $G_A^0=\bigcup_{i=1}^r G_{A(\infty)}^0x_iG_K^0$. С другой стороны, из предложения 5 вытекает существование компактного

множества $D \subset G_A$ со свойством $G_A = DG_A^0$. Тогда D содержится в объединении конечного числа сдвигов $G_{A(\infty)}$, т. е. $D \subset \subset \bigcup_{j=1}^{s} G_{A(\infty)} y_j$, где $y_j \in G_A$. Имеем

$$G_A = DG_A^0 = \bigcup_{i=1}^{r} \bigcup_{j=1}^{s} G_{A(\infty)} y_j G_{A(\infty)}^0 x_i G_K^0,$$

поэтому достаточно показать, что для любых $x, y \in G_A$ множество $G_{A(\infty)} y G_{A(\infty)} x G_K$ содержится в объединении конечного числа двойных смежных классов вида $G_{A(\infty)} z G_K$, $z \in G_A$. Воспользуемся следующим фактом.

Лемма 7. *Для любого $y \in G_A$ группы $G_{A(\infty)}$ и $yG_{A(\infty)}y^{-1}$ соизмеримы.*

Доказательство. Обозначим через y_∞ и y_f проекции y на G_∞ и $G_{A_f} = G_{A_{V_\infty K}}$ соответственно, и пусть $U = G_{A_f(\infty)}$. Тогда $G_{A(\infty)} = = G_\infty \times U$ и $yG_{A(\infty)}y^{-1} = (y_\infty G_\infty y_\infty^{-1}) \times (y_f U y_f^{-1})$. Но группы U и $y_f U y_f^{-1}$ являются открытыми компактными подгруппами в G_{A_f} и поэтому соизмеримы. Поэтому группы $G_{A(\infty)}$ и $yG_{A(\infty)}y^{-1}$ также соизмеримы.

Таким образом, для любого $y \in G_A$ найдется такой конечный набор элементов $\{z_l\}_{l=1}^{t} \subset G_A$, что $yG_{A(\infty)}y^{-1} \subset \bigcup_{l=1}^{t} G_{A(\infty)} z_l$. Тогда

$$G_{A(\infty)} y G_{A(\infty)} x G_K = G_{A(\infty)} (yG_{A(\infty)}y^{-1}) yx G_K \subset \bigcup_{l=1}^{t} G_{A(\infty)} z_l yx G_K.$$

Доказательство теоремы 1 завершено.

Замечание. Очевидная модификация рассуждений позволяет доказать следующее обобщение леммы 7: если $f\colon G \to G'$ — определенный над K изоморфизм, то группы $G'_{A(\infty)}$ и $f(G_{A(\infty)})$ соизмеримы. Учитывая, что $G_\mathcal{O} = G_{A(\infty)} \cap G_K$, отсюда легко получить другое, «топологическое» по своей природе, доказательство предложения 4.1 об инвариантности арифметических подгрупп.

Используя теорему 1, можно post factum показать, что конструкция фундаментальных множеств, содержащаяся в предложении 7, является на самом деле универсальной.

Предложение 9. *Пусть G — произвольная K-группа. Если B — фундаментальное множество в G_∞ относительно $G_\mathcal{O}$ (см. § 4.7), то существует такое компактное подмножество $C \subset G_{A_f}$, что $B \times C$ является фундаментальным множеством в G_A относительно G_K.*

Доказательство. Пусть $G_A = \bigcup_{i=1}^{r} G_{A(\infty)} x_i G_K$, причем можно без ограничения общности считать, что $(x_i)_\infty = e$ для всех i, т. е.

$x_i \in G_{A_f}$. Положим $U = G_{A_f(\infty)}$, $C = \bigcup_{i=1}^{r} Ux_iU$. Тогда, учитывая соотношение $G_\infty = BG_{\mathcal{O}}$, легко показать, что для множества $\Omega = B \times C$ выполняется условие $(F1)_A$, т. е. $G_A = \Omega G_K$. Проверим теперь условие $(F2)_A$. Пусть $x \in \Omega^{-1}\Omega \cap G_K$. Проектируя на G_{A_f}, будем иметь $x \in D = C^{-1}C$. Зафиксируем матричную реализацию $G \subset \boldsymbol{GL}_n$ группы G. Тогда множество D является компактным подмножеством в $M_n(A_f)$, откуда без труда вытекает существование такого целого d, что $d(D \cap M_n(K)) \subset M_n(\mathcal{O})$; в частности, $dx \in M_n(\mathcal{O})$. При этом одновременно $x^{-1} \in D$, и поэтому также $dx^{-1} \in M_n(\mathcal{O})$. Тем самым $x \in G_d = \{g \in G_K \mid dx, dx^{-1} \in M_n(\mathcal{O})\}$. Рассмотрев теперь проекцию на G_∞, будем иметь $x \in B^{-1}B \cap G_d$. Но последнее пересечение конечно в силу очевидного обобщения леммы 4.8 на кольца целых алгебраических чисел. Предложение 9 доказано.

Помимо теоремы 1, построение фундаментального множества в G_A относительно G_K позволяет получить еще ряд важных результатов. Те из них, которые связаны с компактностью или конечностью объема факторпространства G_A/G_K, мы рассмотрим в следующем параграфе, а в настоящем установим адельный вариант теоремы 9 гл. IV.

Теорема 3. *Пусть H — редуктивная K-определенная подгруппа редуктивной K-группы G. Положим $X = G/H$ и обозначим через σ каноническую проекцию $G \to X$. Тогда пересечение $\sigma_A(G_A) \cap X_K$ состоит из конечного числа орбит группы G_K.*

Доказательство. Рассматривая группы $G' = \mathbf{R}_{K/\mathbb{Q}}(G)$, $H' = \mathbf{R}_{K/\mathbb{Q}}(H)$ и замечая, что многообразие $X' = \mathbf{R}_{K/\mathbb{Q}}(X)$ совпадает с факторпространством G'/H', мы с помощью предложения 6 легко получаем редукцию к случаю $K = \mathbb{Q}$. Дальнейшие рассуждения основаны на уже традиционном для нас использовании такого $\mathbb{Q}$-определенного представления ρ: $\boldsymbol{GL}_n \to \boldsymbol{GL}_m$ (где $G \subset \boldsymbol{GL}_n$), что существует точка $v \in \mathbb{Q}^m$ с замкнутой орбитой относительно $\rho(\boldsymbol{GL}_n)$, стабилизатор которой в $\boldsymbol{GL}_n$ совпадает с H. Тогда орбита $Y = v\rho(G)$ также замкнута и является геометрической реализацией X, т. е. существует K-определенный G-эквивариантный изоморфизм $X \simeq Y$. Отсюда следует, что наша задача сводится к доказательству того, что пересечение $v\rho_A(G_A) \cap \mathbb{Q}^m$ состоит из конечного числа орбит группы $G_{\mathbb{Q}}$. Но $G_A = \Delta G_{\mathbb{Q}}$, где Δ — фундаментальное множество, построенное в предложении 8, и достаточно установить конечность пересечения $v\rho_A(\Delta) \cap \mathbb{Q}^m$. Для этого вспомним, что $\Delta = \left(\bigcup_{i=1}^{r} a^\infty \Omega b_i\right) \cap G_A$ в обозначениях предложения 8. Здесь матрица $a \in GL_n(\mathbb{R})$ выбиралась исходя из единственного условия: группа $a^{-1}Ga$ должна быть самосопряженной. Поэтому можно специализировать выбор, потребовав дополнительно, чтобы группа

$a^{-1}Ha$ также была самосопряженной (теорема 8 гл. III). Поскольку $b_i \in GL_n(\mathbb{Q})$, то

$$v\rho_A(\Delta) \cap \mathbb{Q}^m = \bigcup_{i=1}^{r} v\rho_A((a^\infty \Omega b_i) \cap G_A) \cap \mathbb{Q}^m \subset v\rho_A(a^\infty \Omega) \cap \mathbb{Q}^m.$$

Но конечность последнего пересечения мы уже фактически установили при доказательстве предложения 8 (с заменой G на H). Теорема доказана.

В гл. VI мы дадим когомологическую интерпретацию теоремы 3, суть которой состоит в том, что для любой алгебраической K-группы G ядро канонического отображения когомологий Галуа $H^1(K, G) \to \prod_v H^1(K_v, G)$ конечно (см. § 6.4).

В заключение параграфа мы выведем из теоремы 1 утверждение о конечности числа двойных классов специального вида, которые встречаются при построении фундаментальных областей для арифметических подгрупп (см. § 4.7). Итак, пусть G — связная K-определенная группа, P — ее K-определенная параболическая подгруппа. Тогда факторпространство $X = G/P$ является проективным многообразием. Отсюда следует компактность соответствующего адельного пространства X_A. В самом деле, в силу леммы 4 достаточно установить компактность пространства аделей $\mathbb{P}^n_A$ для n-мерного проективного пространства $\mathbb{P}^n$. Чтобы определить $\mathbb{P}^n_A$, рассмотрим открытое аффинное покрытие $\mathbb{P}^n = \bigcup_{i=0}^{n} U_i$, где U_i состоит из таких $x = (x_0 : \ldots : x_n) \in \mathbb{P}^n$, что $x_i \neq 0$, причем изоморфизм $U_i \simeq \mathbb{A}^n$ задается соответствием $(x_0 : \ldots : x_n) \mapsto (x_0/x_i, \ldots, x_{i-1}/x_i, x_{i+1}/x_i, \ldots, x_n/x_i)$. Если теперь $v \in V_f^K$, $x = (x_0 : \ldots : x_n) \in \mathbb{P}^n_{K_v}$ и $|x_i|_v = \max_j |x_j|_v$, то, очевидно, $x \in U_{i\mathcal{O}_v}$, откуда $\mathbb{P}^n_{K_v} = \mathbb{P}^n_{\mathcal{O}_v}$. Поэтому пространство $\mathbb{P}^n_A$ совпадает с прямым произведением $\prod_v \mathbb{P}^n_{K_v}$, и, следовательно, компактно, ибо компактны все $\mathbb{P}^n_{K_v}$ (см. § 3.1). Далее, известно (см. Борель, Титс [1]), что каноническая проекция σ: $G \to X = G/P$ обладает K-определенным рациональным сечением. Используя плотность G_K в G (теорема 2.2), отсюда легко получить, что в нашей ситуации выполнены условия предложения 3, и поэтому отображение σ_A: $G_A \to X_A$ сюръективно. Тем самым X_A можно отождествить с G_A/P_A, равно как и X_K с G_K/P_K. Теперь у нас есть все необходимое для доказательства следующего результата.

Теорема 4. *Пусть G — связная K-определенная группа, P — ее K-определенная параболическая подгруппа. Тогда число $\nu(G, P)$ двойных смежных классов в разложении группы G_K по*

подгруппам $G_{\mathcal{O}}$ и P_K (или, эквивалентно, число орбит группы $G_{\mathcal{O}}$ на X_K) конечно.

Доказательство. Установим вначале конечность числа различных двойных смежных классов в разложении

$$G_A = \bigcup_i G_{A(\infty)} x_i P_K. \tag{2}$$

Выше мы видели, что пространство аделей X_A факторпространства $X = G/P$ является компактным; с другой стороны, X_A может быть отождествлено с G_A/P_A. Отсюда вытекает, что для подходящего компакта $C \subset G_A$ имеем $G_A = CP_A$. Далее, существуют такие конечные наборы $y_1, \ldots, y_r \in G_A$ и $z_1, \ldots, z_s \in P_A$, что

$$C \subset \bigcup_{j=1}^{r} G_{A(\infty)} y_j,$$

$$P_A = \bigcup_{l=1}^{s} P_{A(\infty)} z_l P_K,$$

и тогда $G_A = \bigcup_{j=1}^{r} \bigcup_{l=1}^{s} G_{A(\infty)} y_j P_{A(\infty)} z_l P_K$. Поэтому достаточно показать, что любое множество вида $G_{A(\infty)} y P_{A(\infty)} z P_K$ содержится в объединении конечного числа классов вида $G_{A(\infty)} x P_K$. Имеем

$$G_{A(\infty)} y P_{A(\infty)} z P_K \subset G_{A(\infty)} y G_{A(\infty)} z P_K = G_{A(\infty)} (y G_{A(\infty)} y^{-1}) yz P_K.$$

Но группа $yG_{A(\infty)}y^{-1}$ соизмерима с $G_{A(\infty)}$ (лемма 7), поэтому $yG_{A(\infty)}y^{-1} \subset \bigcup_{i=1}^{d} G_{A(\infty)} a_i$ для некоторого конечного набора $\{a_i\}_{i=1}^{d} \subset G_A$. Тогда

$$G_{A(\infty)} y P_{A(\infty)} z P_K \subset \bigcup_{i=1}^{d} G_{A(\infty)} a_i yz P_K,$$

что и требовалось. Из конечности числа различных классов в (2) вытекает существование такого конечного набора $\{t_j\}_{j=1}^{d} \subset G_K$, что

$$G_K \subset \bigcup_{j=1}^{d} G_{A(\infty)} t_j P_K,$$

откуда $G_K = \bigcup_{j=1}^{d} (G_{A(\infty)} \cap G_K) t_j P_K = \bigcup_{j=1}^{d} G_{\mathcal{O}} t_j P_K$, что и требовалось. Теорема доказана.

В § 4.7 мы отмечали, что для связной $\mathbb{Q}$-группы G число $\nu(G, P)$ двойных смежных классов $G_{\mathbb{Z}} \backslash G_{\mathbb{Q}} / P_{\mathbb{Q}}$, где P — минимальная $\mathbb{Q}$-определенная параболическая подгруппа, интерпретируется как минимальное число вершин фундаментальной области в $G_{\mathbb{R}}$ относительно $G_{\mathbb{Z}}$. Оказывается, что, с другой стороны, это число связано с числом классов группы P.

Предложение 10. *Предположим, что* $\mathrm{cl}(G) = 1$ *и* $G_{K_v} = G_{\mathcal{O}_v} P_{K_v}$ *для всех* $v \in V_f^K$. *Тогда* $\nu(G, P) = \mathrm{cl}(P)$.

Доказательство. Сначала покажем, что в случае $\mathrm{cl}(G)=1$ число $\nu(G, P)$ совпадает с числом d двойных смежных классов в разложении $G_A=\bigcup_{i=1}^{d} G_{A(\infty)}x_iP_K$ (см. доказательство теоремы 4). Действительно, несложная проверка показывает, что соответствие $G_{\mathcal{O}}xP_K \overset{\theta}{\mapsto} G_{A(\infty)}xP_K$ задает инъекцию множества двойных смежных классов $G_{\mathcal{O}}\backslash G_K/P_K$ во множество $G_{A(\infty)}\backslash G_A/P_K$, причем образ θ состоит из тех классов $G_{A(\infty)}xP_K$, которые пересекаются с G_K. Но если $\mathrm{cl}(G)=1$, т. е. $G_A=G_{A(\infty)}G_K$, то всякий класс такого вида пересекается с G_K и, значит, θ сюръективно. Вычислим теперь d другим способом. Для этого заметим, что из условия $G_{K_v}=G_{\mathcal{O}_v}P_{K_v}$ для всех $v\in V_f^K$ вытекает соотношение $G_A=G_{A(\infty)}P_A$, и поэтому любой класс $G_{A(\infty)}xP_K$ допускает представителя из P_A. При этом если $G_{A(\infty)}xP_K=G_{A(\infty)}yP_K$, где $x, y\in P_A$, то $P_{A(\infty)}xP_K=P_{A(\infty)}yP_K$, и, следовательно, $d=\mathrm{cl}(P)$. Предложение 10 доказано.

Пример. Пусть $G=\boldsymbol{SL}_2$ над полем K. Возьмем в качестве параболической подгруппы P подгруппу Бореля $B\subset G$, состоящую из верхних треугольных матриц, и покажем, что для G и $P=B$ выполнены условия предложения 10. Равенство $\mathrm{cl}(G)=1$ является следствием предложения 5 и сильной аппроксимации для группы G, которую мы установили при доказательстве предложения 7. Равенство $G_{K_v}=G_{\mathcal{O}_v}B_{K_v}$ проверяется прямым вычислением. В самом деле, если $x=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in SL_2(K_v)$, то существуют такие $\gamma, \delta\in\mathcal{O}_v$, одновременно не лежащие в $\mathfrak{p}_v$, что $\gamma a+\delta c=0$. Далее, найдутся $\alpha, \beta\in\mathcal{O}_v$, для которых матрица $y=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ лежит в $SL_2(\mathcal{O}_v)$. Тогда прямое вычисление показывает, что $yx\in B_{K_v}$. Применяя теперь предложение 10, получаем, что в рассматриваемой ситуации мы должны иметь равенство $\nu(G, B)=\mathrm{cl}(B)$. Представляя B в виде полупрямого произведения одномерного тора $T=\{\mathrm{diag}(a, a^{-1})\}$ и группы U верхних унипотентных матриц и используя очевидное равенство $B_{A(\infty)}=T_{A(\infty)}U_{A(\infty)}$, легко показать, что $\mathrm{cl}(B)=\mathrm{cl}(T)$ (ср. доказательство предложения 4). Но $T\simeq \boldsymbol{G}_m$ и поэтому $\mathrm{cl}(T)=[J_K : J_K(\infty)K^*]$ совпадает с числом классов идеалов h_K поля K. С другой стороны, по определению $\nu(G, B)$ совпадает с числом орбит группы $G_{\mathcal{O}}$ на пространстве X_K, где $X=G/B$. Так как в нашей ситуации $X\simeq \mathbb{P}^1$, то в итоге мы приходим к следующему результату: число орбит естественного действия группы $SL_2(\mathcal{O})$ на проективной прямой $\mathbb{P}^1_K$ над полем K совпадает с числом классов идеалов h_K поля K. (Последний факт можно доказать и непосредственно, см. Серр [7]).

§ 5.3. Критерии компактности и конечности объема факторпространства G_A/G_K

Теорема 5. 1) *Пространство G_A/G_K компактно тогда и только тогда, когда редуктивная часть связной компоненты G^0 анизотропна над K.*

2) *Пространство G_A/G_K имеет конечный инвариантный объем в том и только том случае, если $\boldsymbol{X}(G^0)_K = 1$.*

Доказательство. Поскольку подгруппа G_K дискретна в G_A, то инвариантная мера на пространстве G_A/G_K существует в том и только том случае, если группа G_A унимодулярна (см. § 3.5). Покажем, что последнее эквивалентно унимодулярности G_∞. Факторпространство $F = G_A/G_A^0$, являясь компактной топологической группой (см. предложение 4), обладает конечной G_A-инвариантной мерой, следовательно, ограничение функции модуля Δ_{G_A} на G_A^0 совпадает с $\Delta_{G_A^0}$ (теорема 3.17). В частности, из унимодулярности G_A вытекает унимодулярность G_A^0. Обратно, если предположить, что группа G_A^0 унимодулярна, то $\operatorname{Ker}\Delta_{G_A}$ содержит G_A^0, и поэтому Δ_{G_A} индуцирует непрерывный гомоморфизм F в $\mathbb{R}^{>0}$. Но $\mathbb{R}^{>0}$ не имеет нетривиальных компактных подгрупп, откуда $\Delta_{G_A} = 1$. Мы показали, что унимодулярность группы G_A равносильна унимодулярности группы G_A^0. То же самое можно сказать об унимодулярности групп G_∞ и G_∞^0, ибо факторпространство G_∞/G_∞^0 конечно. Поэтому мы имеем возможность с самого начала считать группу G связной. Тогда меру Хаара на G_A можно построить при помощи левоинвариантной K-определенной рациональной дифференциальной формы ω на G степени $n = \dim G$. Более точно, для каждого $v \in V^K$ форма ω индуцирует левоинвариантную меру ω_v на G_{K_v}, как описано в § 3.5. Выберем числа λ_v для $v \in V_f^K$, (называемые *множителями сходимости*) таким образом, чтобы произведение $\prod_v \lambda_v \omega_v(G_{\mathcal{O}_v})$ абсолютно сходилось (можно, например, положить $\lambda_v = 1/\omega_v(G_{\mathcal{O}_v})$). Тогда, рассматривая G_A как ограниченное топологическое произведение групп G_{K_v} относительно выделенных подгрупп $G_{\mathcal{O}_v}$, мы с помощью конструкций из § 3.5 получаем меру Хаара τ на группе G_A. Мера τ называется *мерой Тамагавы*, отвечающей системе множителей сходимости $\lambda = (\lambda_v)$. (Отметим, что τ на самом деле не зависит от выбора формы ω. Действительно, любая другая левоинвариантная K-определенная рациональная дифференциальная форма ω' имеет вид $\omega' = c\omega$, где $c \in K^*$, и тогда для любого $v \in V^K$ соответствующая мера ω'_v связана с мерой ω_v соотношением $\omega'_v = \|c\|_v^n \omega_v$,

где $\| \ \|_v$ — введенное в § 1.2, п. 1 нормализованное нормирование. Поэтому если строить меру τ' при помощи ω' с той же системой множителей сходимости, то $\tau' = \left(\prod_v \|c\|_v^n\right)\tau = \tau$ в силу формулы произведения (см. § 1.2, п. 1).) Из конструкции меры τ вытекает, что группа G_A унимодулярна в том и только том случае, если унимодулярны все группы G_{K_v}. Но согласно теореме 18 гл. III унимодулярность группы G_{K_v} для какого-либо v эквивалентна правоинвариантности формы ω, и тогда группы G_{K_v} унимодулярны для всех v. Отсюда следует, что группы G_A и G_∞ одновременно являются или не являются унимодулярными.

Дальнейшие рассуждения равным образом применимы к доказательству пунктов 1) и 2) теоремы. Согласно предложению 9 в G_A относительно G_K всегда существует фундаментальное множество вида $\Omega = B \times C$, где $B \subset G_\infty$ — замкнутое фундаментальное множество относительно $G_\mathcal{O}$, $C \subset G_{A(\infty)}$ — некоторый компакт. Из свойств фундаментального множества вытекает, что компактность пространства G_A/G_K равносильна компактности Ω, т. е. компактности B. Аналогично, существование фундаментального множества конечного объема равносильно конечности объема B. Так как группы G_∞ и G_A унимодулярны одновременно, то мы получаем следующие эквивалентности:

$$\{G_A/G_K \text{ компактно}\} \Leftrightarrow \{G_\infty/G_\mathcal{O} \text{ компактно}\}$$

$$\left\{G_A/G_K \begin{array}{l}\text{имеет конечный}\\ \text{инвариантный}\\ \text{объем}\end{array}\right\} \Leftrightarrow \left\{G_\infty/G_\mathcal{O} \begin{array}{l}\text{имеет конечный}\\ \text{инвариантный}\\ \text{объем}\end{array}\right\}$$

Поэтому утверждения 1) и 2) теоремы 5 следуют из соответствующих пунктов теоремы 17 гл. IV.

Хорошо известно, что множители сходимости, участвующие в определении меры Тамагавы, можно выбирать некоторым каноническим образом; в частности, для полупростой группы G они вообще не нужны (т. е. можно положить $\lambda_v = 1$ для всех v). Тогда инвариантный объем (если он существует) пространства G_A/G_K относительно получаемой таким образом меры Тамагавы называется *числом Тамагавы* группы G и обозначается через $\tau(G)$. Рассмотрим один пример.

Пример. Пусть $G = \boldsymbol{SL}_2$ над полем $\mathbb{Q}$. Покажем, что $\tau(G) = 1$. Рассмотрим дифференциальную форму ω на G, которая относительно координат x, y, z матрицы $X = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in G$ записывается в виде $\omega = \frac{1}{x}\, dx \wedge dy \wedge dz$. В § 3.5 мы видели, что эта форма является левоинвариантной рациональной формой на G. Там же мы подсчитали, что для соответствующей меры Хаара

ω_p на группе $SL_2(\mathbb{Q}_p)$ объем $\omega_p(SL_2(\mathbb{Z}_p))$ равен $1-p^{-2}$. Тогда произведение $\prod_p \omega_p(SL_2(\mathbb{Z}_p))^{-1}$ имеет вид эйлеровского разложения для дзета-функции Римана $\zeta(s)$ в точке $s=2$, и поэтому произведение $\prod_p \omega_p(SL_2(\mathbb{Z}_p))$ абсолютно сходится к значению $\zeta(2)^{-1}$ (в частности, множители сходимости здесь действительно не нужны). Пусть теперь Σ — фундаментальная область в $SL_2(\mathbb{R})$ относительно $SL_2(\mathbb{Z})$, построенная в примере из § 4.6. В § 3.5 мы показали, что в терминах координат φ, a, u на $SL_2(\mathbb{R})$, доставляемых разложением Ивасавы, дифференциальная форма ω записывается в виде $ad\varphi da du$, и поэтому для соответствующей меры Хаара ω_∞ на группе $SL_2(\mathbb{R})$ вычисления § 4.6 приводят к значению $\omega_\infty(\Sigma)=\frac{\pi^2}{6}$. Остается заметить, что, рассуждая как и при доказательстве предложения 7, легко показать, что $\Omega=\Sigma\times\prod_p SL_2(\mathbb{Z}_p)$ является фундаментальной областью в G_A относительно G_K, т. е. для нее выполняются условия 1), 2′) из § 3.5, так что $\tau(G)=\omega_\infty(\Sigma)\times\prod_p \omega_p(SL_2(\mathbb{Z}_p))=$ $=\frac{\pi^2}{6}\zeta(2)^{-1}=1$, ибо значение $\zeta(2)$ равно $\frac{\pi^2}{6}$ (см. Серр [8]).

В данном примере оказалось возможным в явном виде указать фундаментальную область в G_A относительно G_K и вычислить ее объем, что привело нас к значению числа Тамагавы $\tau(G)$. В общем случае такие построения нереальны, однако сама задача вычисления $\tau(G)$ представляется очень важной. Это в особенности стало ясно после того, как Кнезер и Тамагава независимо заметили, что для $G=\boldsymbol{SO}_n(f)$, где f — невырожденная квадратичная форма от n переменных с рациональными коэффициентами, равенство $\tau(G)=2$ совпадает по существу с одним из основных результатов Зигеля по аналитической теории квадратичных форм (формула для веса рода) (см. лекцию Кнезера в [АТЧ]). Согласно теореме 5 для полупростой группы G число $\tau(G)$ конечно, и основные усилия были направлены на вычисления чисел Тамагавы для полупростых групп над числовым полем K. Как показал Оно [8], [10], на самом деле достаточно вычислить одно число Тамагавы для каждого класса изогенных групп. Точнее, имеет место следующий изящный результат: пусть G — полупростая K-группа, π: $\tilde{G}\to G$ — универсальное K-определенное накрытие, $F=\operatorname{Ker}\pi$ — фундаментальная группа G и $\mathbf{X}(F)$ — ее группа характеров; тогда $\tau(G)=\tau(\tilde{G})\,\frac{h^0(\mathbf{X}(F))}{i^1(\mathbf{X}(F))}$, где $h^0(\mathbf{X}(F))=[H^0(K,\mathbf{X}(F))]=[\mathbf{X}(F)_K]$, $i^1(\mathbf{X}(F))$ — порядок ядра канонического отображения $H^1(K,\mathbf{X}(F))\to\prod_v H^1(K_v,\mathbf{X}(F))$.

Таким образом, достаточно вычислить $\tau(G)$ для всех односвязных групп. А. Вейль выдвинул предположение, ставшее затем известным как гипотеза Вейля, о том, что для односвязной группы G число Тамагавы $\tau(G)$ равно 1. В работах Вейля [4], [5] был развит метод вычисления чисел Тамагавы, использующий индукцию, вычеты некоторых аналогов дзета-функций, формулу суммирования Пуассона и позволивший доказать эту гипотезу для многих классических и некоторых исключительных групп. Затем Марс [3], [4] вычислил число Тамагавы для унитарных групп типа A_n и тем самым завершил доказательство гипотезы Вейля для классических полупростых групп над числовыми полями. Для групп Шевалле унифицированное доказательство гипотезы Вейля было дано Ленглендсом (см. его статью в сборнике «Арифметические группы и автоморфные функции»). Лэй [1], [2] вычислил $\tau(G)$ для квазиразложимой группы G. Полное доказательство гипотезы Вейля было получено совсем недавно Коттвицем [3] по модулю справедливости принципа Хассе для когомологий Галуа полупростых односвязных алгебраических групп. С другой стороны, Черноусов [6] завершил доказательство принципа Хассе, рассмотрев случай групп типа E_8 (см. гл. VI). Тем самым к настоящему времени гипотеза Вейля уже доказана в общем случае.

Для более общих редуктивных групп, чем полупростые, данное выше определение чисел Тамагавы нуждается в модификации, ибо в ряде важных для приложений случаев (например, для одномерного разложимого тора $\boldsymbol{G}_m$) объем факторпространства G_A/G_K бесконечен. Это обстоятельство заставляет нас предпринять поиск других однородных пространств, тесно связанных с группой аделей, но имеющих конечный инвариантный объем. Так как препятствием к конечности объема G_A/G_K является существование нетривиальных K-определенных характеров, т. е. наличие K-разложимого тора в виде почти прямого сомножителя, то естественно начать рассмотрение с одномерного K-разложимого тора $S=\boldsymbol{G}_m$. Здесь группа S_A изоморфна группе J_K иделей поля K. Факторпространство J_K/K^*, разумеется, некомпактно, но классический результат алгебраической теории чисел (см., например, Ленг [2]) утверждает, что компактным будет факторпространство J_K^1/K^*, где J_K^1 — группа специальных иделей (т. е. ядро гомоморфизма $c_K\colon J_K\to\mathbb{R}^{>0}$, $c_K((x_v))=\prod_v\|x_v\|_v$ (см. п. 1 § 1.2)). Определить аналог группы J_K^1 в общей ситуации можно следующим образом. С каждым характером $\chi\in\mathbf{X}(G)_K$ свяжем непрерывный гомоморфизм $c_K(\chi)\colon G_A\to\mathbb{R}^{>0}$ по формуле $c_K(\chi)((g_v))=\prod_v\|\chi(g_v)\|_v$. Тогда по определению

положим

$$G_A^{(1)} = \bigcap_{\chi \in \mathbf{X}(G)_K} \operatorname{Ker} c_K(\chi).$$

Ясно, что бесконечное пересечение здесь можно заменить конечным, ибо если $\chi_1, \ldots, \chi_r$ образуют базис $\mathbf{X}(G)_K$, то $G_A^{(1)} = \bigcap_{i=1}^{r} \operatorname{Ker} c_K(\chi_i)$. Читатель в качестве упражнения может показать, что последнее соотношение остается в силе, если $\chi_1, \ldots, \chi_r$ порождают подгруппу конечного индекса в $\mathbf{X}(G)_K$. Из формулы произведения вытекает включение $G_A^{(1)} \supset G_K$.

Теорема 6. *Пусть G — связная K-определенная группа. Тогда группа $G_A^{(1)}$ унимодулярна и факторпространство $G_A^{(1)}/G_K$ имеет конечный инвариантный объем. Оно компактно в том и только том случае, когда полупростая часть G анизотропна над K.*

(Отметим, что последнее условие можно также переформулировать в виде: каждый унипотентный элемент из G_K лежит в унипотентном радикале G. Кроме того, если группа G связна и $\mathbf{X}(G)_K = 1$, то $G_A^{(1)} = G_A$, и поэтому для связных групп теорема 6 является обобщением теоремы 5.)

Доказательство удобно начать с редукции к случаю $K = \mathbb{Q}$. Пусть $H = \mathbf{R}_{K/\mathbb{Q}}(G)$ — группа, полученная из G ограничением основного поля. Покажем, что изоморфизм $G_{A_K} \overset{\rho}{\simeq} H_{A_\mathbb{Q}}$ из предложения 6 индуцирует изоморфизм $G_{A_K}^{(1)} \simeq H_{A_\mathbb{Q}}^{(1)}$. Для этого заметим, что любой K-определенный характер χ: $G \to \mathbf{G}_m$ индуцирует морфизм $\tilde{\chi} = \mathbf{R}_{K/\mathbb{Q}}(\chi)$: $H \to \mathbf{R}_{K/\mathbb{Q}}(\mathbf{G}_m)$. Беря композицию $\tilde{\chi}$ с норменным отображением N: $\mathbf{R}_{K/\mathbb{Q}}(\mathbf{G}_m) \to \mathbf{G}_m$, мы получаем характер $\varkappa = N \circ \chi \in \mathbf{X}(H)_\mathbb{Q}$. При этом, используя разложение (4) из § 2.1, легко показать, что сопоставление $\chi \mapsto \varkappa$ определяет изоморфизм η: $\mathbf{X}(G)_K \to \mathbf{X}(H)_\mathbb{Q}$ соответствующих групп характеров. Из конструкции η вытекает коммутативность диаграммы

$$\begin{tikzcd} G_K \arrow[r, "\rho"] \arrow[d, "\chi"'] & H_\mathbb{Q} \arrow[d, "\eta(\chi)"] \\ K^* \arrow[r, "N_{K/\mathbb{Q}}"] & \mathbb{Q}^* \end{tikzcd}$$

для любого характера $\chi \in \mathbf{X}(G)_K$. Мы оставляем читателю в качестве упражнения проверить, что эта диаграмма распространяется и на соответствующие группы аделей. Из формул в п. 3 § 1.2 вытекает, что $c_K(\chi) = c_\mathbb{Q}(\eta(\chi))$, откуда следует, что ρ

действительно индуцирует изоморфизм $G^{(1)}_{A_K} \simeq H^{(1)}_{A_Q}$. Поэтому факторпространства $G^{(1)}_{A_K}/G_K$ и $H^{(1)}_{A_Q}/H_Q$ изоморфны, и с самого начала можно считать, что $K=\mathbb{Q}$. Упрощение рассуждений в этом случае связано с тем обстоятельством, что здесь можно дать удобное описание группы $G^{(1)}_{A(\infty)} = G^{(1)}_A \cap G_{A(\infty)}$. По определению $G_{A(\infty)} = G_{\mathbb{R}} \times G_{A_f(\infty)}$, причем $G_{A_f(\infty)} \subset G^{(1)}_{A(\infty)}(\infty)$ в силу компактности группы $G_{A_f(\infty)}$ и отсутствия компактных подгрупп в $\mathbb{R}^{>0}$. Таким образом, $G^{(1)}_{A(\infty)} = L_{\mathbb{R}} \times G_{A_f(\infty)}$, где $L \subset G$ — подгруппа, состоящая из таких g, что $\chi(g) = \pm 1$ для любого $\chi \in \mathbf{X}(G)_{\mathbb{Q}}$.

Лемма 8. *L — замкнутая по Зарисскому $\mathbb{Q}$-определенная подгруппа в G и $\mathbf{X}(L^0)_{\mathbb{Q}} = 1$. Кроме того, полупростые части групп G и L^0 совпадают.*

Доказательство. Пусть $\chi_1, \ldots, \chi_r$ — базис $\mathbf{X}(G)_{\mathbb{Q}}$ и $\varphi: G \to \mathbf{G}_m^r$ — гомоморфизм, определяемый формулой $\varphi(g) = (\chi_1(g), \ldots, \chi_r(g))$. Тогда $L = \varphi^{-1}(D)$, где $D \subset \mathbf{G}_m^r$ — (замкнутая) подгруппа, состоящая из $(\pm 1, \ldots, \pm 1)$, и первое утверждение леммы доказано. Если $G = HU$ — разложение Леви группы G, S — максимальный центральный тор в H и $S = S_1 S_2$ — его представление в виде почти прямого произведения $\mathbb{Q}$-разложимого и $\mathbb{Q}$-анизотропного торов, то легко видеть, что $L^0 = (BS_2)U$, где $B = [H, H]$ — полупростая часть G, откуда следуют все остальные утверждения леммы.

Из леммы 8 и теоремы 13 гл. IV вытекает, что группа $L_{\mathbb{R}}$ является унимодулярной. Поэтому в силу компактности $G_{A_f(\infty)}$ унимодулярной будет и группа $G^{(1)}_{A(\infty)} = L_{\mathbb{R}} \times G_{A_f(\infty)}$. Наша цель — показать, что группа $G^{(1)}_A$ унимодулярна. Для этого рассмотрим функцию модуля $\Delta = \Delta_{G^{(1)}_A}: G^{(1)}_A \to \mathbb{R}^{>0}$, и покажем, что на самом деле $\Delta = 1$. Так как группа $G^{(1)}_{A(\infty)}$ открыта в $G^{(1)}_A$ и унимодулярна, то $\Delta|_{G^{(1)}_{A(\infty)}} = 1$. Покажем, что также $\Delta|_{G_{\mathbb{Q}}} = 1$. Поскольку $G^{(1)}_A$ является нормальным делителем в G_A, то факторпространство $G_A/G^{(1)}_A$, будучи группой, обладает инвариантной мерой, и поэтому Δ совпадает с ограничением на $G^{(1)}_A$ функции модуля Δ_{G_A}. Но тогда для вычисления Δ можно воспользоваться конструкцией меры Тамагавы. Пусть ω — левоинвариантная $\mathbb{Q}$-определенная рациональная дифференциальная форма на G степени $n = \dim G$, ρ_g — морфизм первого сдвига на элемент $g \in G$. Тогда, как мы видели при доказательстве теоремы 13 гл. IV, $\rho_g^*(\omega) = \chi(g)\omega$ для некоторого характера

$\chi \in \mathbf{X}(G)_{\mathbb{Q}}$. Если теперь $v \in V^{\mathbb{Q}}$, ω_v — соответствующая мера Хаара на $G_{\mathbb{Q}_v}$, то для $g \in G_{\mathbb{Q}_v}$ значение модуля $\Delta_{G_{\mathbb{Q}_v}}(g)$ задается формулой $\Delta_{G_{\mathbb{Q}_v}}(g) = \|\chi(g)\|_v^n$. Поэтому для $g \in G_{\mathbb{Q}}$ имеем $\Delta(g) = \prod_v \|\chi(g)\|_v^n = 1$ в силу формулы произведения. Далее, из теоремы 1 вытекает конечность числа двойных классов $G^{(1)}_{A(\infty)} \backslash G^{(1)}_A / G_{\mathbb{Q}}$, поэтому из доказанного выше и того факта, что Δ является гомоморфизмом, получаем, что образ $\Delta(G^{(1)}_A)$ является конечным, следовательно, $\Delta(G^{(1)}_A) = 1$, ибо $\mathbb{R}^{>0}$ не содержит нетривиальных конечных подгрупп. Таким образом, унимодулярность $G^{(1)}_A$ доказана.

Рассмотрим теперь конечное разложение $G^{(1)}_A = \bigcup_{i=1}^{r} G^{(1)}_{A(\infty)} x_i G_{\mathbb{Q}}$. Из леммы 7 вытекает соизмеримость любой группы $x_i^{-1} G^{(1)}_{A(\infty)} x_i$ с $G^{(1)}_{A(\infty)}$, откуда получается существование такого конечного набора $y_1, \ldots, y_l \in G^{(1)}_A$, что $G^{(1)}_A = \bigcup_{j=1}^{l} y_j G^{(1)}_{A(\infty)} G_{\mathbb{Q}}$. Поэтому достаточно установить условие конечности объема (компактности) $G^{(1)}_{A(\infty)} G_{\mathbb{Q}} / G_{\mathbb{Q}}$. Но учитывая разложение $G^{(1)}_{A(\infty)} = L_{\mathbb{R}} \times G_{A_f(\infty)}$ и равенство $G_{\mathbb{Z}} = L_{\mathbb{Z}}$, получаем

$$(G^{(1)}_{A(\infty)} G_{\mathbb{Q}})/G_{\mathbb{Q}} \simeq G^{(1)}_{A(\infty)}/G_{\mathbb{Z}} \simeq L_{\mathbb{R}}/L_{\mathbb{Z}} \times G_{A_f(\infty)},$$

так что в силу компактности $G_{A_f(\infty)}$ все сводится к конечности объема (компактности) $L_{\mathbb{R}}/L_{\mathbb{Z}}$. Но из теоремы 12 и 13 гл. IV с учетом леммы 8 вытекает, что пространство $L_{\mathbb{R}}/L_{\mathbb{Z}}$ всегда имеет конечный объем и компактно в том и только том случае, когда полупростая часть L^0, совпадающая с полупростой частью G, анизотропна над $\mathbb{Q}$. Теорема 6 доказана.

Как и в случае пространства G_A/G_K, меру $\tau^{(1)}$ на пространстве $G^{(1)}_A/G_K$ можно выбирать некоторым каноническим образом, и тогда объем $\tau^{(1)}(G^{(1)}_A/G_K)$ также называется *числом Тамагавы* группы G. Отметим, что если для связной группы G объем пространства G_A/G_K конечен, то $\mathbf{X}(G)_K = 1$ и, следовательно, $G^{(1)}_A = G_A$. Поэтому новое определение действительно является обобщением прежнего на произвольные связные группы.

Вычисление числа Тамагавы алгебраического K-тора T было получено Оно [6], который показал, что $\tau(T) = \frac{[H^1(K, \mathbf{X}(T))]}{[Ш(T)]}$, где $Ш(T) = \operatorname{Ker}\left(H^1(K, T) \to \prod_v H^1(K_v, T)\right)$ — *группа Шафаревича — Тейта тора T*. Используя этот результат, можно построить примеры торов и полупростых групп, для которых число $\tau(T)$ не является целым. Кроме того, можно объединить указанные

выше формулы для чисел Тамагавы полупростых групп и торов (отметим, что для унипотентной группы U всегда $\tau(U)=1$) в одну формулу, которая дает выражение для числа Тамагавы произвольной связной K-группы G в терминах когомологий так называемого модуля Пикара $\operatorname{Pic} G$ (см. Сансюк [1]).

§ 5.4. Теория приведения и структурные теоремы для S-арифметических подгрупп

Опираясь на построенную нами теорию приведения для групп аделей, мы в настоящем параграфе получим аналоги результатов гл. IV для S-арифметических подгрупп. Всюду ниже через S обозначается конечное подмножество V^K, содержащее V_∞^K, $\mathcal{O}(S)$ — кольцо S-целых элементов поля K. Если $G \subset \subset \boldsymbol{GL}_n$ — определенная над K алгебраическая группа, то $G_{\mathcal{O}(S)}$ — группа S-целых точек, иногда называемая *группой S-единиц группы G*. Напомним, что подгруппа $\Gamma \subset G$ называется *S-арифметической*, если она соизмерима с $G_{\mathcal{O}(S)}$. Инвариантность класса S-арифметических подгрупп при K-определенных изоморфизмах можно доказать либо путем подходящей модификации предложения 2 гл. IV, либо вывести из равенства $G_{\mathcal{O}(S)} = G_{A(S)} \cap G_K$, воспользовавшись замечанием, сделанным после леммы 7. Из последнего равенства вытекает также, что группа $G_{\mathcal{O}(S)}$ является дискретной подгруппой группы $G_{A(S)}$. Поскольку $G_{A(S)} = G_S \times G_{A_S(S)}$, и группа $G_{A_S(S)}$ компактна, то $G_{\mathcal{O}(S)}$ является в то же время дискретной подгруппой в $G_S = \prod_{v \in S} G_{K_v}$ (это, естественно, легко доказать и не обращаясь к аделям). Поэтому можно ставить вопрос о построении теории приведения для $G_{\mathcal{O}(S)}$ как в группе $G_{A(S)}$, так и в группе G_S. Определения фундаментальных множеств здесь естественно дать следующим образом (по аналогии с соответствующими определениями для арифметических групп и групп аделей).

Определения. 1) *Подмножество $\Omega \subset G_{A(S)}$ является фундаментальным множеством для $G_{\mathcal{O}(S)}$, если*

$(\mathrm{F1})_{A(S)}$ $\Omega G_{\mathcal{O}(S)} = G_{A(S)}$,

$(\mathrm{F2})_{A(S)}$ *пересечение $\Omega\Omega^{-1} \cap G_{\mathcal{O}(S)}$ конечно.*

2) *Подмножество $\Omega \subset G_S$ является фундаментальным множеством для $G_{\mathcal{O}(S)}$, если*

$(\mathrm{F1})_S$ $\Omega G_{\mathcal{O}(S)} = G_S$,

$(\mathrm{F2})_S$ *для любых $a, b \in G_K$ множество элементов $x \in G_{\mathcal{O}(S)}$ таких, что $\Omega axb \cap \Omega \neq \varnothing$, конечно.*

Легко видеть, что в исследуемом нами случае конечного S задачи построения фундаментальных множеств в группах $G_{A(S)}$,

и G_S фактически эквивалентны. А именно, если $\Omega \subset G_S$ — фундаментальное множество в смысле определения 2), то $\Omega \times G_{A_S(S)} \subset \subset G_{A(S)}$ — фундаментальное множество в смысле определения 1). По этой причине ниже мы будем заниматься только построением фундаментального множества в G_S. Отметим, что для бесконечного S определение 2) теряет смысл, в то же время все результаты для группы $G_{A(S)}$ сохраняют силу (см. Борель [1], § 8).

Предложение 11. *Пусть B — фундаментальное множество для $G_{\mathcal{O}}$ в G_∞. Тогда существует такое открытое компактное подмножество $C \subset G_{S \setminus V_\infty^K}$, что множество $\Omega = B \times C \subset G_S$ является фундаментальным для $G_{\mathcal{O}(S)}$.*

Доказательство проводится аналогично доказательству предложения 9. В самом деле, из теоремы 1 вытекает существование конечного разложения

$$G_{A(S)} = \bigcup_{i=1}^{r} G_{A(\infty)} x_i \left(G_K \cap G_{A(S)}\right) = \bigcup_{i=1}^{r} G_{A(\infty)} x_i G_{\mathcal{O}(S)}, \quad x_i \in G_{S \setminus V_\infty^K},$$

которое индуцирует разложение

$$G_S = \bigcup_{i=1}^{r} D x_i G_{\mathcal{O}(S)},$$

где

$$D = G_\infty \times U, \quad U = \prod_{v \in S \setminus V_\infty^K} G_{\mathcal{O}_v}.$$

Положим $C = \bigcup_{i=1}^{r} U x_i U$. Тогда легко проверяется, что для $\Omega = B \times C$ справедливо равенство $G_S = \Omega G_{\mathcal{O}_S}$, и остается проверить, что для любых $a, b \in G_K$ множество $\Sigma = \{x \in G_{\mathcal{O}(S)} \mid \Omega \cap \cap \Omega axb \neq \varnothing\}$ конечно. Если $x \in \Sigma$, то, переходя к проекции на неархимедову часть, получим, что $x \in a^{-1}C^{-1}Cb^{-1}$; тогда $x^{-1} \in bC^{-1}Ca$. Из компактности множества $C^{-1}C$, как мы уже не раз убеждались, вытекает существование такого $r \in \mathcal{O}$, что $\Sigma \subset G_r = \{x \in G_K \mid rx,\ rx^{-1} \in M_n(\mathcal{O})\}$ (предполагается, что $G \subset \subset \boldsymbol{GL}_n$). Поэтому конечность Σ вытекает из очевидного обобщения леммы 8 гл. IV. Предложение доказано.

Из предложения 11 легко получается

Теорема 7. 1) *Пространство $G_S/G_{\mathcal{O}(S)}$ имеет конечный инвариантный объем в том и только том случае, если $\mathbf{X}(G^0)_K = 1$;*

2) *Пространство $G_S/G_{\mathcal{O}(S)}$ компактно в том и только том случае, если редуктивная часть связной компоненты G анизотропна над K.*

Доказательство. При доказательстве теоремы 5 мы установили, что все группы G_{K_v}, $v \in V^K$, унимодулярны или нет одновременно, так что унимодулярность G_S равносильна унимодулярности G_∞. Взяв тогда в качестве B в предложении 11

замкнутое фундаментальное множество для $G_{\mathcal{O}}$ в G_∞ в смысле § 3.5, мы получим, что пространство $G_S/G_{\mathcal{O}(S)}$ имеет конечный инвариантный объем (компактно) в том и только том случае, если соответствующее свойство имеет место для $G_\infty/G_{\mathcal{O}}$. Поэтому наши утверждения вытекают из соответствующих пунктов теоремы 17 гл. IV. Теорема доказана.

Как в случае арифметических групп, так и в случае групп аделей, мы в качестве приложения теории приведения получали теорему о конечности числа орбит (см. теорему 3 и теорему 9 гл. IV). Такая теорема имеет место и для S-арифметических подгрупп. Чтобы ее сформулировать, условимся называть S-решеткой на пространстве K^n конечнопорожденный $\mathcal{O}(S)$-подмодуль пространства K^n, содержащий его базис.

Теорема 8. *Пусть G — редуктивная алгебраическая группа, ρ: $G \to \boldsymbol{GL}_m$ — представление G, определенное над K. Если для вектора $w \in K^m$ орбита $X = w\rho(G)$ замкнута, то для любой S-решетки $L \subset K^m$, инвариантной относительно группы $G_{\mathcal{O}(S)}$, пересечение $X_S \cap L$ содержится в объединении конечного числа орбит группы $G_{\mathcal{O}(S)}$.*

Доказательство непосредственно вытекает из следующих двух фактов.

Предложение 12. *Пространство X_S состоит из конечного числа орбит группы G_S.*

Предложение 13. *Пересечение $w\rho(G_S) \cap L$ содержится в объединении конечного числа орбит группы $G_{\mathcal{O}(S)}$.*

Доказательство предложения 12 немедленно редуцируется к случаю, когда S состоит из одного нормирования v (напомним, S всюду предполагается конечным). Если нормирование v является комплексным, то G_{K_v} действует на X_{K_v} транзитивно, т. е. имеется всего одна орбита. Для вещественного v требуемая конечность установлена в следствии 2 из теоремы 6 гл. III. В случае неархимедова v единственный известный путь получения конечности числа орбит — вывести ее из теоремы конечности для когомологий Галуа над локально компактными полями, что мы и проделаем в § 6.3.

Доказательство предложения 13 вытекает из конструкции фундаментальных множеств, которая указана в предложении 11. Более подробно, в § 4.7 мы указали, как, используя ограничение основного поля и конструкции фундаментальных множеств в $G_{\mathbb{R}}$ относительно $G_{\mathbb{Z}}$ (см. § 4.3), построить фундаментальное множество $B \subset G_\infty$ относительно $G_{\mathcal{O}}$. Тогда из доказательства теоремы 9 вытекает, что построенное таким образом множество B обладает следующим свойством: если ρ: $G \to \boldsymbol{GL}_m$ — определенное над K представление, то для любого $w \in K^m$ такого, что орбита $X = w\rho(G)$ замкнута, пересечение $w\rho(B) \cap \mathcal{O}^m$ конечно. Взяв тогда фундаментальное множество $B \subset G_\infty$ с этим свойством, найдем, используя предложение 11, такой компакт

$C \subset G_{S \setminus V_\infty^K}$, что множество $\Omega = B \times C$ будет фундаментальным для $G_{\mathcal{O}(S)}$ в G_S. Тогда в силу инвариантности L относительно группы $G_{\mathcal{O}(S)}$ достаточно установить конечность $F = w\rho(\Omega) \cap L$. Из компактности C вытекает существование такого $r \in \mathcal{O}$, что $rF \subset \mathcal{O}^m$. Тогда переходя к проекции на архимедову компоненту, получим, что rF содержится в пересечении $(rw)\rho(B) \cap \mathcal{O}^m$, которое конечно по построению. Предложение 13 доказано.

Из теоремы 8 выводится инвариантность класса S-арифметических подгрупп при произвольных сюръективных морфизмах и конечность числа классов сопряженности конечных подгрупп группы $G_{\mathcal{O}(S)}$.

Теорема 9. *Пусть f: $G \to H$ — сюръективный морфизм алгебраических групп. Тогда для любой S-арифметической подгруппы $\Gamma \subset G$ образ $f(\Gamma)$ является S-арифметической подгруппой в H.*

Доказательство мало чем отличается от доказательства теоремы 4.1. Очевидно, достаточно установить S-арифметичность группы $f(G_{\mathcal{O}(S)})$, причем можно считать, что $f(G_{\mathcal{O}(S)}) \subset H_{\mathcal{O}(S)}$. Докажем конечность индекса $[H_{\mathcal{O}(S)} : f(G_{\mathcal{O}(S)})]$. Покажем сначала, что общий случай сводится к случаю, когда G либо редуктивна, либо унипотентна.

Лемма 9. *Пусть $G = FU$ — разложение Леви. Тогда если B и D — подгруппы конечного индекса в группах $F_{\mathcal{O}(S)}$ и $U_{\mathcal{O}(S)}$ соответственно, причем B нормализует D, то подгруппа BD имеет конечный индекс в $G_{\mathcal{O}(S)}$.*

Доказательство. Дословно повторяя доказательство следствия 2 из предложения 1 гл. IV, мы получаем конечность индекса $[G_{\mathcal{O}(S)} : F_{\mathcal{O}(S)} U_{\mathcal{O}(S)}]$. Пусть теперь $F_{\mathcal{O}(S)} = \bigcup_{i=1}^{r} x_i B$, $U_{\mathcal{O}(S)} = \bigcup_{j=1}^{t} y_j D$. Тогда $F_{\mathcal{O}(S)} U_{\mathcal{O}(S)} = \bigcup_{i=1}^{r} \bigcup_{j=1}^{t} x_i y_j BD$. В самом деле, если $x \in F_{\mathcal{O}(S)}$, $y \in U_{\mathcal{O}(S)}$ и $x = x_i b$, $byb^{-1} = y_j d$, где $b \in B$, $d \in D$, то $xy = x_i by = x_i y_j db = x_i y_j b(b^{-1} db) \in x_i y_j BD$. Таким образом, мы показали, что BD имеет конечный индекс в $F_{\mathcal{O}(S)} U_{\mathcal{O}(S)}$, а значит, и в $G_{\mathcal{O}(S)}$. Лемма 9 доказана.

Пусть $G = FU$ — разложение Леви группы G. Тогда $H = f(F) f(U)$ — разложение Леви группы H. Если конечность индексов $[f(F)_{\mathcal{O}(S)} : f(F_{\mathcal{O}(S)})]$ и $[f(U)_{\mathcal{O}(S)} : f(U_{\mathcal{O}(S)})]$ уже доказана, то из леммы 9 вытекает конечность индекса $[H_{\mathcal{O}(S)} : f(F_{\mathcal{O}(S)} U_{\mathcal{O}(S)})]$, а значит, и конечность индекса $[H_{\mathcal{O}(S)} : f(G_{\mathcal{O}(S)})]$. Тем самым требуемая редукция получена.

Рассмотрим случай унипотентной группы G. Тогда по теореме 7 пространство $G_S / G_{\mathcal{O}(S)}$ компактно. Полагая $U = \operatorname{Ker} f$, будем иметь $H^1(K_v, U) = 1$ для любого $v \in V^K$ (лемма 2.7), поэтому из точной последовательности $1 \to U \to G \to H \to 1$,

переходя к когомологиям, получим $f(G_{K_v})=H_{K_v}$, и, значит, $f(G_S)=H_S$. Отсюда следует, что пространство $H_S/f(G_{\mathcal{O}(S)})$ также компактно. Значит, пространство $H_{\mathcal{O}(S)}/f(G_{\mathcal{O}(S)})$ одновременно является компактным и дискретным, так что индекс $[H_{\mathcal{O}(S)}:f(G_{\mathcal{O}(S)})]$ обязан быть конечным.

Пусть теперь группа G редуктивна. Если $H\subset \boldsymbol{GL}_n$, то использование известного приема позволяет без ограничения общности считать H замкнутой в M_n. Тогда H можно интерпретировать как (замкнутую) орбиту единичной матрицы E_n относительно действия G на M_n, задаваемого формулой $Ag=Af(g)$ $(A\in M_n,\ g\in G)$, где справа стоит умножение матриц. Остается заметить, что решетка $L=M_n(\mathcal{O}(S))$ инвариантна относительно $G_{\mathcal{O}(S)}$, $H_{\mathcal{O}(S)}=H\cap L$ и орбиты $G_{\mathcal{O}(S)}$ на $H_{\mathcal{O}(S)}$ совпадают со смежными классами $H_{\mathcal{O}(S)}/f(G_{\mathcal{O}(S)})$, так что конечность числа орбит, гарантируемая теоремой 8, эквивалентна конечности индекса $[H_{\mathcal{O}(S)}:f(G_{\mathcal{O}(S)})]$. Теорема 9 доказана.

Теорема 10. *Число классов сопряженности конечных подгрупп группы $G_{\mathcal{O}(S)}$ конечно.*

Доказательство. Взяв $v\notin S$ и рассмотрев $G_{\mathcal{O}(S)}$ как подгруппу группы $G_{\mathcal{O}_v}$, мы, как и при доказательстве предложения 5 гл. III, получим конечность числа классов изоморфных конечных подгрупп группы $G_{\mathcal{O}(S)}$. Поэтому достаточно показать, что для фиксированной конечной группы Γ число классов сопряженности подгрупп $G_{\mathcal{O}(S)}$, изоморфных Γ, конечно. Рассмотрим вначале случай редуктивной группы G. Здесь рассуждения фактически повторяют доказательство предложения 3.5. Пусть $R(\Gamma,G)$ — многообразие представлений Γ в G. Тогда G естественным образом действует на $R(\Gamma,G)$ сопряжениями, и требуемое утверждение сводится к доказательству конечности числа орбит группы $G_{\mathcal{O}(S)}$ на $R(\Gamma,G)_{\mathcal{O}(S)}$. Согласно теореме 17 гл. II группа G имеет конечное число орбит на $R(\Gamma,G)$, причем эти орбиты замкнуты в топологии Зарисского. Пусть X — одна из таких орбит, для которой $X_{\mathcal{O}(S)}\neq\varnothing$. Если $G\subset \boldsymbol{GL}_n$ и $[\Gamma]=d$, то X реализуется как замкнутое подмножество пространства $V=M_n\times\ldots\times M_n$ (d сомножителей), причем действие группы G естественным образом продолжается на V. Поэтому, применяя теорему 8 к решетке $L=M_n(\mathcal{O}(S))\times\ldots\times M_n(\mathcal{O}(S))$, мы получаем конечность числа орбит группы $G_{\mathcal{O}(S)}$ на $X_{\mathcal{O}(S)}$, и требуемое доказано.

В общем случае рассмотрим разложение Леви $G=HU$, где U — унипотентный радикал G, а группа H редуктивна. Пусть $\pi\colon G\to G/U$ — каноническая проекция. Можно выбрать такую реализацию группы G/U, что $\pi(G_{\mathcal{O}(S)})\subset(G/U)_{\mathcal{O}(S)}$. Так как индекс $[(G/U)_{\mathcal{O}(S)}:\pi(G_{\mathcal{O}(S)})]$ конечен, и в редуктивном случае теорема 10 уже доказана, то группа $\pi(G_{\mathcal{O}(S)})$ имеет конечное число классов сопряженности конечных подгрупп.

Рассмотрим произвольную конечную подгруппу $\Gamma = \{\gamma_1, \ldots, \gamma_d\} \subset G_{\mathcal{O}(S)}$ и определим замкнутое подмножество $A(\Gamma) \subset G^d$ равенством $A(\Gamma) = R(\Gamma, G) \cap \{(\delta_1, \ldots, \delta_d) \mid \pi(\delta_i) = \pi(\gamma_i)\}$. Группа U естественным образом действует на $A(\Gamma)$ сопряжениями. Для завершения доказательства теоремы достаточно показать, что $A(\Gamma)_{\mathcal{O}(S)}$ состоит из конечного числа орбит группы $U_{\mathcal{O}(S)}$. Рассмотрим морфизм φ: $U \to A(\Gamma)$, $\varphi(g) = g^{-1}\gamma g = (g^{-1}\gamma_1 g, \ldots, g^{-1}\gamma_d g)$, где $\gamma = (\gamma_1, \ldots, \gamma_d)$. Обозначим также через U_1 централизатор Γ в U и выберем такое K-определенное подмногообразие $U_2 \subset U$, что морфизм — произведение $U_1 \times U_2 \to U$ является K-определенным изоморфизмом многообразий (см. лемму 1 гл. II). (Отметим, что выбрать подгруппу $U_2 \subset U$ с таким свойством в общем случае нельзя.)

Лемма 10. *Ограничение* φ: $U_2 \to A(\Gamma)$ *является K-определенным изоморфизмом многообразий.*

Доказательство. Покажем вначале, что U действует на $A(\Gamma)$ транзитивно. Пусть $\delta = (\delta_1, \ldots, \delta_d) \in A(\Gamma)$ и $\Delta = \{\delta_1, \ldots, \delta_d\}$. Тогда Δ является подгруппой в G, и в силу редуктивности подгрупп Γ, $\Delta \subset G$ по теореме 3 главы II найдутся такие $x, y \in U$, что $x^{-1}\Gamma x \subset H$, $y^{-1}\Delta y \subset H$. Для любого $i = 1, \ldots, d$ имеем

$$\pi(x^{-1}\gamma_i x) = \pi(\gamma_i) = \pi(\delta_i) = \pi(y^{-1}\delta_i y),$$

так что из инъективности ограничения $\pi|_H$ вытекает равенство $x^{-1}\gamma_i x = y^{-1}\delta_i y$, т. е. $\delta = g^{-1}\gamma g = \varphi(g)$, где $g = xy^{-1}$. Так как стабилизатором точки γ является в точности подгруппа U_1, то ограничение φ: $U_2 \to A(\Gamma)$ биективно. Остается заметить, что в силу однородности многообразие $A(\Gamma)$ является гладким, так что φ — изоморфизм согласно теореме 14 гл. II.

Пусть теперь U является абелевой группой; тогда в качестве U_2 можно выбрать подходящую подгруппу U (лемма 1 гл. II). Из леммы 10 вытекает, что прообраз $\left(\varphi|_{U_2}\right)^{-1}\left(A(\Gamma)_{A_S(S)}\right)$ является компактным подмножеством в U_{2A_S} и поэтому содержится в объединении конечного числа (левых) смежных классов по подгруппе $U_{2A_S(S)}$. Но тогда $\varphi^{-1}(A(\Gamma)_{\mathcal{O}(S)}) = \varphi^{-1}\left(A(\Gamma)_{A_S(S)}\right) \cap U_{2K}$ содержится в объединении конечного числа смежных классов по подгруппе $U_{2\mathcal{O}(S)} = U_{2A_S(S)} \cap U_{2K}$, что и требовалось.

В общем случае применяем индукцию по размерности унипотентного радикала U. Пусть $Z(U)$ — центр U; рассмотрим $G' = G/Z(U)$. Тогда в $G'_{\mathcal{O}(S)}$ конечные подгруппы разбиваются в конечное число классов сопряженных. Так как образ $G_{\mathcal{O}(S)}$ при каноническом морфизме $G \to G'$ является S-арифметической подгруппой по теореме 9, то отсюда следует конечность числа классов сопряженности в $G_{\mathcal{O}(S)}$ подгрупп вида $\Gamma Z(U)_{\mathcal{O}(S)}$, где Γ — конечная подгруппа $G_{\mathcal{O}(S)}$. Для завершения доказательства теоремы 10 достаточно показать, что конечные подгруппы из

$\Gamma Z(U)_{\mathcal{O}(S)}$ разбиваются в $G_{\mathcal{O}(S)}$ в конечное число сопряженных классов. Но Γ содержится в подходящей максимальной редуктивной K-подгруппе F группы G. Тогда в группе $D = FZ(U)$ унипотентный радикал является абелевым и $D_{\mathcal{O}(S)} \subset G_{\mathcal{O}(S)}$. Поэтому конечные подгруппы $D_{\mathcal{O}(S)}$ разбиваются в конечное число классов сопряженных в $G_{\mathcal{O}(S)}$. Теорема 10 полностью доказана.

Замечание. Для редуктивной группы G можно дать доказательство теоремы 10 в том же духе, что и доказательство аналогичной теоремы 3 гл. IV для арифметических подгрупп, используя основу Брюа — Титса для групп над неархимедовыми локальными полями (см. § 3.4).

Наш завершающий результат связан с доказательством конечной представимости S-арифметических групп.

Теорема 11. *Любая S-арифметическая подгруппа редуктивной группы G является группой с конечным числом образующих и конечным числом определяющих соотношений.*

Доказательство основано на методе Райдемайстера — Шрайера из комбинаторной теории групп (см. Линдон, Шупп [1], гл. 2, § 4), который мы применим к группе $G_{\mathcal{O}(S)}$, рассматривая ее как подгруппу в $\Gamma = G_{S \setminus V_\infty^K}$. В § 3.4 (теорема 15 гл. III) мы показали, что для любого $v \in V_f^K$ группа G_{K_v} является компактно определенной, поэтому, как несложно видеть, компактно определенной будет и группа $\Gamma = \prod_{v \in S \setminus V_\infty^K} G_{K_v}$ (напомним, что последнее означает существование компактного подмножества $D \subset \Gamma$, порождающего Γ и такого, что соотношения вида $ab = c$ для $a, b, c \in D$ составляют множество определяющих соотношений для Γ. Переходя от множества D к множеству $D \cup D^{-1} \cup \{e\}$, где e — единица группы Γ, мы можем в дальнейшем считать, что D содержит e и $D = D^{-1}$). Итак, если через $F(X)$ обозначить свободную группу, порожденную X, и рассмотреть множество D^*, элементы которого находятся в биективном соответствии с элементами множества D относительно отображения $d^* \mapsto d$, то определяемый им гомоморфизм ρ: $F(D^*) \to \Gamma$ сюръективен, а $N = \operatorname{Ker} \rho$ порождается элементами вида $a^* b^* c^{*-1}$, где a^*, b^*, $c^* \in D^*$ и $\rho(a^* b^*) = \rho(c^*)$. Необходимую для применения метода Райдемайстера — Шрайера систему представителей смежных классов $F(D^*)/H$, где $H = \rho^{-1}(G_{\mathcal{O}(S)})$, удобно выбрать, исходя из следующих соображений. Из предложения 11 вытекает существование такого компактного подмножества $C \subset \Gamma$, что $\Gamma = G_{\mathcal{O}(S)} C$, причем можно без потери общности считать, что $e \in C$. Выберем из элементов C систему T представителей смежных классов $\Gamma / G_{\mathcal{O}(S)}$, содержащую e, и обозначим через T^* такую систему представителей классов $F(D^*)/H$, что T^* содержит единицу e^* группы $F(D^*)$ и ρ осуществляет биекцию T^* на T. Вве-

дем функцию $F(D)\to T^*$, $x\mapsto\bar{x}$, сопоставляющую элементу x представитель $\bar{x}$ смежного класса Hx, лежащий в T^*, т. е. такой элемент $\bar{x}\in T^*$, что $Hx=H\bar{x}$. Возьмем теперь произвольный $x\in H$ и запишем его в виде $x=d_1\ldots d_m$, где $d_i\in D^*\cup D^{*-1}$. Тогда $x=(d_1\bar{d}_1^{-1})(\bar{d}_1 d_2(\overline{d_1d_2})^{-1})\ldots(\overline{d_1\ldots d_{m-1}}d_m(\overline{d_1\ldots d_m})^{-1})$, ибо $\overline{d_1\ldots d_m}=\bar{x}=e^*$. Элементы $\overline{d_1\ldots d_{i-1}}d_i(\overline{d_1\ldots d_i})^{-1}$, построенные по методу Райдемайстера — Шрайера, дают в произведении элемент x и лежат в множестве $X=(T^*(D^*\cup D^{*-1})T^{*-1})\cap H$, которое тем самым оказывается системой образующих для H. Далее, по условию N как нормальный делитель в $F(D^*)$ порождается выражениями abc^{-1} для таких троек a, b, $c\in D^*$, что $\rho(ab)=\rho(c)$. Это значит, что любой элемент $n\in N$ допускает представление вида

$$n=\prod_{i=1}^{l} g_i(abc^{-1})^{\varepsilon_i}g_i^{-1},$$

где $g_i\in F(D^*)$, $\varepsilon_i=\pm 1$. Записывая g_i в виде $g_i=h_it_i$, $h_i\in H$, $t_i\in T^*$, мы видим, что N как нормальный делитель в H порождается элементами xyz^{-1}, где x, y, $z\in T^*D^*T^{*-1}$ и $\rho(xy)=\rho(z)$. Имеем

$$xyz^{-1}=(x\bar{x}^{-1})(\bar{x}y\overline{xy}^{-1})(\overline{xy}z^{-1}z\overline{xy}^{-1})^{-1},$$

ибо $\overline{xyz}^{-1}=e^*$, откуда следует, что N, как нормальный делитель в H, порождается элементами вида xyz^{-1}, где x, y, $z\in(T^*)^2D^*(T^*)^{-2}\cap H$. Отсюда видно, что систему образующих X удобно расширить, например, до множества $Y=\rho^{-1}(BC^2DC^{-2}B\cap G_{\mathcal{O}(S)})$, где $B=\prod_{v\in S\setminus V_\infty^K}G_{\mathcal{O}_v}$ (из определения X ясно, что $X\subset Y$). Тогда N как нормальный делитель в H порождается элементами xyz^{-1}, где x, y, $z\in Y$ и $\rho(xy)=\rho(z)$. Покажем теперь, что Y можно уменьшить до получения конечной системы образующих группы $G_{\mathcal{O}(S)}$. Для этого на первом шаге выберем такое подмножество $Z\subset Y$, что ρ индуцирует биекцию $Z\to\rho(Y)$, и определим проекцию π: $Y\to Z$ условием $\rho(x)=\rho(\pi(x))$ для любого $x\in Y$. Рассмотрим свободные группы $F(Y)$, $F(Z)$ и взаимно обратные гомоморфизмы $F(Z)\underset{\alpha_2}{\overset{\alpha_1}{\rightleftarrows}}F(Y)$, индуцируемые вложением $Z\subset Y$ и проекцией π. Из коммутативной диаграммы

$$\begin{tikzcd} F(Z) \arrow[rr, shift left, "\alpha_1"] \arrow[dr, "\rho_2"'] & & F(Y) \arrow[ll, shift left, "\alpha_2"] \arrow[dl, "\rho_1"] \\ & G_{\mathcal{O}(S)} & \end{tikzcd} \qquad (1)$$

в которой $\rho_2 = \rho_1 \circ \alpha_1$, а ρ_1 получается композицией ρ и гомоморфизма τ: $F(Y) \to H$, получаем, что $\operatorname{Ker} \rho_2 = \alpha_2(\operatorname{Ker} \rho_1)$. С другой стороны, $\operatorname{Ker} \rho_1$ порождается $\operatorname{Ker} \tau$ и элементами вида xyz^{-1}, где $x, y, z \in Y$ и $\rho(xy) = \rho(z)$. Отсюда следует, что $\operatorname{Ker} \rho_2$ порождается $\operatorname{Ker}(\tau \circ \alpha_1)$ и элементами вида xyz^{-1}, где $x, y, z \in Z$ и $\rho(xy) = \rho(z)$. По построению ρ осуществляет биекцию между множеством Y и множеством $E \cap G_{\mathcal{O}(S)}$, где $E = BC^2DC^{-2}B$. Но E является компактным подмножеством в Γ и поэтому покрывается конечным числом сдвигов открытой подгруппы B. Поэтому существует такой конечный набор элементов $y_1, \ldots, y_r \in E \cap G_{\mathcal{O}(S)}$, что

$$E \cap G_{\mathcal{O}(S)} = \bigcup_{i=1}^{r} y_i (G_{\mathcal{O}(S)} \cap B) = \bigcup_{i=1}^{r} y_i G_{\mathcal{O}}$$

(отметим, что поскольку $E = BE = EB$, то $E \cap G_{\mathcal{O}(S)} = G_{\mathcal{O}}(E \cap G_{\mathcal{O}(S)}) = (E \cap G_{\mathcal{O}(S)}) G_{\mathcal{O}}$). В силу теоремы 4.17 можно выбрать конечную систему $z_1, \ldots, z_t$ образующих группы $G_{\mathcal{O}}$. Положим тогда $U = \{z_1, \ldots, z_t\}$, $W = \{y_1, \ldots, y_r\} \cup U$ и, пользуясь биекцией между Z и $E \cap G_{\mathcal{O}(S)}$, будем отождествлять эти множества с соответствующими подмножествами в Z. По построению имеем сюръективный гомоморфизм φ: $F(U) \to G_{\mathcal{O}}$. Рассмотрев некоторое сечение ψ: $G_{\mathcal{O}} \to F(U)$ гомоморфизма φ, тождественное на U, можно определить отображение $Z \xrightarrow{\sigma} F(W)$, переводящее $y_i g$, где $g \in G_{\mathcal{O}}$, в $y_i \psi(g)$. Это отображение индуцирует гомоморфизм β_2: $F(Z) \to F(W)$, который является обратным к гомоморфизму β_1: $F(W) \to F(Z)$, определяемому вложением $W \subset Z$. Кроме того, имеем коммутативную диаграмму

$$\begin{tikzcd} F(W) \arrow[r, shift left, "\beta_1"] \arrow[dr, "\rho_3"'] & F(Z) \arrow[l, shift left, "\beta_2"] \arrow[d, "\rho_2"] \\ & G_{\mathcal{O}(S)} \end{tikzcd} \tag{2}$$

в которой $\rho_3 = \rho_2 \circ \beta_1$, где ρ_2 взято из диаграммы (1). Из (2) получаем, что $\operatorname{Ker} \rho_3 = \beta_2(\operatorname{Ker} \rho_2)$. Поэтому $\operatorname{Ker} \rho_3$ порождается $\operatorname{Ker}(\tau \circ \alpha_2 \circ \beta_2)$ и элементами вида xyz^{-1}, где $x, y, z \in \sigma(Z)$ и $\rho_3(xy) = \rho_3(z)$. Покажем, что все элементы вида xyz^{-1} или, эквивалентно, соотношения $xy = z$ для таких x, y, z можно в действительности свести к конечному числу. Для этого рассмотрим вначале такие соотношения, где $x \in \psi(G_{\mathcal{O}})$. Так как $G_{\mathcal{O}}(E \cap G_{\mathcal{O}(S)}) = E \cap G_{\mathcal{O}(S)}$, то $z_i y_j = y_k w_{ij}$ для всех $i = 1, \ldots, t$; $j = 1, \ldots, r$, при подходящих $k \in \{1, \ldots, r\}$, $w_{ij} \in G_{\mathcal{O}}$. Введем тогда соотношения

$$z_i y_j = y_k \psi(w_{ij}), \quad i = 1, \ldots, t; \ j = 1, \ldots, r. \tag{3}$$

Если добавить к (3) конечную систему соотношений между z_i, которые определяют $G_{\mathcal{O}}$ (см. утверждение 2) теоремы 4.17), то мы получим конечную систему соотношений, из которой выводятся все соотношения вида $xy = z$ для $x \in \psi(G_{\mathcal{O}})$. В самом деле, любой $x \in \psi(G_{\mathcal{O}})$ является словом от z_i. Поэтому представив y, z в виде $y = y_j b$, $z = y_k c$, b, $c \in \psi(G_{\mathcal{O}})$ и используя (3) соответствующее число раз, мы приведем соотношение $xy = z$ к виду $y_l ab = y_k c$, где $a \in \psi(G_{\mathcal{O}})$. Из равенства $\rho_3(xy) = \rho_3(z)$ вытекает, что $k = l$, и тогда, сократив на y_k, получим соотношение $ab = c$ между словами от переменных z_i, а все такие соотношения мы по построению уже учли. Взяв теперь произвольный $x \in \sigma(Z)$, представим его в виде $x = y_i a$, $a \in \psi(G_{\mathcal{O}})$. Тогда, используя уже доказанное, любое соотношение вида $xy = z$ можно свести к соотношению

$$y_i y_j = y_k \psi(r_{ij}), \tag{4}$$

где $r_{ij} \in G_{\mathcal{O}}$ — элемент, определяемый из условия $y_i y_j = y_k r_{ij}$ в $G_{\mathcal{O}(S)}$. Таким образом, все соотношения вида $xy = z$, где x, y, $z \in \sigma(Z)$ и $\rho_3(xy) = \rho_3(z)$, выводятся из конечного числа. Эквивалентным образом, нормальный делитель в $F(W)$, порожденный элементами xyz^{-1} для таких троек x, y, z, порождается на самом деле конечным числом таких элементов. Поэтому если рассмотреть подгруппу $\Phi = \alpha_2\beta_2(F(W))$, то из вычисления $\operatorname{Ker}\rho_3$ вытекает, что $\operatorname{Ker}\rho|_{\Phi} = \Phi \cap N$ порождается как нормальный делитель в Φ конечным числом элементов. Остается заметить, что как конечно порожденная подгруппа в $F(D^*)$, Φ является свободной группой конечного ранга (следствие из теоремы Нильсена — Шрайера), поэтому представление $G_{\mathcal{O}(S)} \simeq \Phi/\Phi \cap N$ дает требуемое конечно определенное представление $G_{\mathcal{O}(S)}$. Тогда и любая S-арифметическая подгруппа в G, будучи соизмеримой с $G_{\mathcal{O}(S)}$, также конечно определена. Теорема 11 доказана.

Приведенное нами доказательство теоремы 11 представляет формализованный вариант первоначальных рассуждений Кнезера [7]. Читателю, владеющему комбинаторной теорией групп, такая формализация может местами показаться излишней, в частности, он, видимо, предпочтет не вводить свободных групп $F(Y)$, $F(Z)$ и т. д., а вести рассуждения прямо в группе Γ (это возможно, и именно так поступает Кнезер). Тем не менее и при нашем варианте изложения, рассчитанном на читателя, не имеющего соответствующей подготовки, ясно видна основная идея рассуждений, которая заключается в редукции общего случая к случаю $S = V_\infty^K$, когда $G_{\mathcal{O}(S)} = G_{\mathcal{O}}$, где конечная определенность уже доказана в теореме 4.17. Эту редукцию можно также выполнить путем индукции по $|S \setminus V_\infty^K|$, рассматривая $G_{\mathcal{O}(S)}$ как подгруппу в G_{K_v}, где $v \in S \setminus V_\infty^K$. В некоторых случаях подхо-

дящая модификация такого индуктивного процесса соответственно позволяет в явном виде найти образующие и соотношения для $G_{\mathcal{O}(S)}$, если известно представление группы $G_{\mathcal{O}}$ (для группы $G = \boldsymbol{SL}_2$ см. работу Серра [10]). Имеется и другое доказательство теоремы 11, при котором случай $S = V_\infty^K$ ничем не отличается от остальных (см. Борель, Серр [4]). По форме оно сходно с доказательством теоремы 4.1 и использует дискретное действие группы $G_{\mathcal{O}(S)}$ на подходящем односвязном пространстве, которое является произведением уже знакомого нам факторпространства G_∞ по максимальной компактной подгруппе и основ Брюа — Титса для групп G_{K_v}, $v \in S \setminus V_\infty^K$. Как мы уже отмечали, на этом пути можно получить и другое доказательство теоремы 10 для редуктивных групп.

Обратим внимание на тот факт, что в теореме 4.17 мы не налагали на группу G условия редуктивности. Однако теорема 11 для нередуктивных групп, вообще говоря, неверна. Так, если $S \neq V_\infty^K$, то аддитивная группа кольца $\mathcal{O}(S)$ не является конечно порожденной, поэтому не является конечно порожденной и любая S-арифметическая подгруппа в одномерной унипотентной группе $\boldsymbol{G}_a$. С другой стороны, если $B = \left\{\begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix} \middle| \alpha \neq 0\right\}$ — борелевская подгруппа в $\boldsymbol{SL}_2$, то любая S-арифметическая подгруппа в B конечно порождена. В связи с этим укажем на критерий конечной порожденности (конечной определенности), доказательству которого фактически и посвящена статья Кнезера [7]: S-арифметические подгруппы в G являются конечно порожденными (конечно определенными) в том и только том случае, когда для всех $v \in S \setminus V_\infty^K$ группы G_{K_v} являются компактно порожденными (соответственно, компактно определенными). Так как для редуктивной группы компактная определенность всегда имеет место (теорема 3.15), то критерий компактной порожденности в общем случае можно сформулировать в терминах действия G на унипотентном радикале $R_u(G)$, что мы и предлагаем сделать читателю в качестве упражнения.

Завершает эту главу описание S-арифметических подгрупп в торах. Приводимая ниже теорема содержит в качестве частных случаев как классическую теорему Дирихле о структуре S-единиц в полях алгебраических чисел, так и полученное нами в § 4.5 описание обычных арифметических подгрупп в торах (тем самым ее естественно называть обобщенной теоремой Дирихле). Ее доказательство, опубликованное Широм [2], фактически идентично доказательству теоремы 9 из гл. IV книги А. Вейля [7].

Теорема 12. *Пусть T — тор, определенный над полем алгебраических чисел K, $S \subset V^K$ — конечное подмножество, содержа-*

щее V_∞^K. Тогда группа S-единиц $T_{\mathcal{O}(S)}$ изоморфна произведению конечной группы и свободной абелевой группы ранга $s = \sum_{v \in S} \operatorname{rang}_{K_v} T - \operatorname{rang}_K T$.

Доказательство. В силу равенства $T_{\mathcal{O}(S)} = T_{A(S)} \cap T_K$ группа $T_{\mathcal{O}(S)}$ является дискретной подгруппой в $T_{A(S)}$. Однако отсюда сразу не удается получить информацию о $T_{\mathcal{O}(S)}$, ибо $T_{A(S)}/T_{\mathcal{O}(S)}$ в общем случае некомпактно. Чтобы получить компактное факторпространство, нужно группу $T_{A(S)}$ уменьшить до $T_{A(S)}^{(1)} = T_{A(S)} \cap T_A^{(1)}$, где группа $T_A^{(1)}$ определяется как в § 5.3. Действительно, так как $T_K \subset T_A^{(1)}$, то опять $T_{\mathcal{O}(S)} = T_{A(S)}^{(1)} \cap T_K$, и поэтому факторпространство $T_{A(S)}^{(1)}/T_{\mathcal{O}(S)}$ отождествляется с открыто-замкнутым подпространством в $T_A^{(1)}/T_K$, которое компактно по теореме 6. Выясним теперь точную структуру группы $T_{A(S)}^{(1)}$. По определению $T_{A(S)} = \prod_{v \in S} T_{K_v} \times \prod_{v \notin S} T_{\mathcal{O}_v}$. Для $v \in V_\infty^K$ структура T_{K_v} нам уже известна (см. доказательство следствия 1 из теоремы 4.11): $T_{K_v} \simeq \mathbb{R}^{r_v} \times B$, где $r_v = \operatorname{rang}_{K_v} T$, а группа B компактна. Пусть теперь $v \in S \setminus V_\infty^K$. Рассмотрим разложение $T = T_1 T_2$ в почти прямое произведение максимального K_v-разложимого подтора T_1 и максимального K_v-анизотропного тора T_2 (см. § 2.1, п. 7). Пусть $B \subset T_{K_v}$ — максимальная компактная подгруппа. Так как T_{2K_v} — компакт (теорема 3.1), то $T_{2K_v} \subset B$. Поэтому если φ: $T \to T_3 = T/T_2$ — соответствующее факторотображение, то $T_{K_v}/B \simeq \varphi(T_{K_v})/\varphi(B)$. Но тор T_3 разложим над K_v и, следовательно, $(T_3)_{K_v} \simeq (K_v^*)^{r_v} \simeq \mathbb{Z}^{r_v} \times U$, где $r_v = \dim T_3 = \operatorname{rang}_{K_v} T$, а группа U компактна. Из максимальности B вытекает равенство $\varphi(B) = U \cap \varphi(T_{K_v})$, так что $\varphi(T_{K_v})/\varphi(B) \subset \mathbb{Z}^{r_v}$ и $\varphi(T_{K_v})/\varphi(B) \simeq \mathbb{Z}^t$ для некоторого $t \leqslant r_v$. С другой стороны, T_1 также является K_v-разложимым подтором ранга r_v, откуда $T_{1K_v} \simeq \mathbb{Z}^{r_v} \times U_1$ для некоторой компактной подгруппы U_1. При этом изоморфная $\mathbb{Z}^{r_v}$ подгруппа в T_{1K_v} является дискретной и поэтому не пересекается с B, так что T_{K_v}/B содержит свободную абелеву группу ранга r_v. Окончательно, $T_{K_v}/B \simeq \mathbb{Z}^{r_v}$, откуда без труда вытекает разложение $T_{K_v} \simeq \mathbb{Z}^{r_v} \times B$. Собирая

воедино информацию об архимедовых и неархимедовых компонентах, получим следующее разложение для $T_{A(S)}$:

$$T_{A(S)} \simeq \mathbb{R}^{\alpha} \times \mathbb{Z}^{\beta} \times W,$$

где $\alpha = \sum_{v \in V_\infty^K} \operatorname{rang}_{K_v} T$, $\beta = \sum_{v \in S \setminus V_\infty^K} \operatorname{rang}_{K_v} T$, а группа W компактна. Теперь уже несложно описать структуру группы $T_{A(S)}^{(1)}$. Напомним предварительно, что группа $T_A^{(1)}$ вводилась нами как пересечение ядер непрерывных гомоморфизмов $c_K(\chi)$: $T_A \to \mathbb{R}^{>0}$, которые определялись исходя из характеров $\chi \in \mathbf{X}(T)_K$ по формуле $c_K(\chi)((g_v)) = \prod_v \|\chi(g_v)\|_v$. Пусть $\chi_1, \ldots, \chi_r$ $(r = \operatorname{rang}_K T)$ образуют базис $\mathbf{X}(T)_K$. Тогда имеем непрерывный гомоморфизм θ: $T_A \to (\mathbb{R}^{>0})^r$, $g \overset{\theta}{\longmapsto} (c_K(\chi_1)(g), \ldots, c_K(\chi_r)(g))$, причем $T_A^{(1)} = \operatorname{Ker}\theta$. Утверждается, что $\theta(T_{A(S)}) = (\mathbb{R}^{>0})^r$ для любого $S \supset V_\infty^K$. Действительно, так как $\chi_1, \ldots, \chi_r$ образуют базис $\mathbf{X}(T)_K$, то морфизм φ: $T \to \mathbf{G}_m^r$, $g \overset{\varphi}{\longmapsto} (\chi_1(g), \ldots, \chi_r(g))$ сюръективен. Поэтому, применяя следствие 1 из предложения 3.3, получим, что для любого $v \in V_\infty^K$ образ $\varphi(T_{K_v})$ открыт и, следовательно, содержит связную компоненту группы $(K_v^*)^r$, которая совпадает с $(\mathbb{R}^{>0})^r$ для вещественного v и с $\mathbb{C}^{*r}$ для комплексного v. Остается заметить, что ограничение θ на группу T_{K_v}, соответствующим образом вложенную в T_A, совпадает с композицией φ и отображения нормализованного нормирования $\|\ \|_v$: $K_v^* \to \mathbb{R}^{>0}$, так что уже $\theta(T_{K_v})$ совпадает с $(\mathbb{R}^{>0})^r$ для любого $v \in V_\infty^K$. Учитывая изоморфность $\mathbb{R}$ и $\mathbb{R}^{>0}$, мы видим, что в нашей ситуации применима

Лемма 11. *Пусть* $\Gamma = \mathbb{R}^{\alpha} \times \mathbb{Z}^{\beta} \times W$, *где группа* W *компактна. Тогда если* θ: $\Gamma \to \mathbb{R}^{\gamma}$ — *непрерывный сюръективный гомоморфизм, то* $\gamma \leqslant \alpha$, *и* $\operatorname{Ker}\theta \simeq \mathbb{R}^{\alpha-\gamma} \times \mathbb{Z}^{\beta} \times W$.

Доказательство оставляется читателю в качестве упражнения.

Таким образом, для группы $T_{A(S)}^{(1)}$ получаем представление

$$T_{A(S)}^{(1)} \simeq \mathbb{R}^{\alpha-r} \times \mathbb{Z}^{\beta} \times W.$$

Выше мы показали, что группа $T_{\mathcal{O}(S)}$ является дискретной подгруппой в $T_{A(S)}^{(1)}$, причем факторпространство $T_{A(S)}^{(1)}/T_{\mathcal{O}(S)}$ ком-

пактно. Поэтому утверждение теоремы 12 вытекает из леммы 4.17, если заметить, что $(\alpha - r) + \beta$ совпадает с числом s в ее формулировке.

Следствие (теорема Дирихле об S-единицах). *Пусть K — поле алгебраических чисел, S — конечное подмножество в V^K, содержащее V_∞^K. Тогда группа S-единиц $E(S) = \{x \in K^* \mid |x|_v = 1$ для всех $v \notin S\}$ изоморфна произведению группы E корней из единицы, содержащихся в K, и свободной абелевой группы ранга $[S] - 1$.*

Библиографические замечания. Основные результаты теории приведения для групп аделей и S-арифметических подгрупп в числовом случае содержатся в статье Бореля [1]. При этом Борель в существенной степени использовал построенную им и Хариш-Чандрой теорию приведения для арифметических подгрупп. Позднее Годеман [1] показал, как те же самые теоремы могут быть получены другим путем, не зависящим от теорем редукции для арифметических групп. Усовершенствование метода Годемана позволило Хардеру [5] построить теорию приведения для групп аделей над глобальными полями положительной характеристики. Основные теоремы здесь те же самые, что и в числовом случае, с той лишь разницей, что аналог теоремы 1 принимает вид: если S — непустое подмножество в V^K, то число двойных смежных классов $G_{A(S)} \backslash G_A / G_K$ конечно. С другой стороны, вопрос о конечной порожденности S-арифметических подгрупп редуктивной алгебраической группы G, определенной над функциональным глобальным полем K, не имеет столь однозначного ответа, как в числовом случае, ибо существуют не конечно порожденные S-арифметические группы. Почти полное решение вопроса о конечной порожденности содержится в работе Бера [4]; случай классических групп рассматривался ранее О'Мирой [2]. Вопрос о конечной определенности S-арифметических групп над функциональным полем K в общей форме положительно решен лишь для K-анизотропных групп (см. Борель — Серр [4]). Для K-изотропных групп ситуация окончательно не прояснилась до сих пор. Известно, однако, что группа $SL_3(k[t])$, где k — конечное поле, конечно порождена, но не является конечно определенной (Бер [6]), а группа $SL_2(\mathcal{O}(S))$ конечно определена тогда и только тогда, когда $[S] > 2$ (Штулер [1]).

ГЛАВА VI

КОГОМОЛОГИИ ГАЛУА

Настоящая глава посвящена изложению результатов об описании множества 1-когомологий Галуа $H^1(K, G)$ алгебраической K-группы G над полями арифметического типа. Кроме того, мы включили ряд необходимых нам результатов о когомологиях групп целых v-адических точек и адельных групп. Материал настоящей главы будет использоваться в гл. VII, VIII, поэтому знакомство с ним необходимо для дальнейшего чтения книги. В то же время в целом когомологии Галуа играют в книге вспомогательную роль, и в наши планы не входило изложение всех аспектов теории когомологий. Поэтому мы сосредоточили внимание на тех вопросах, которые связаны с классическими теоретико-числовыми концепциями (такими, как, например, локально-глобальный принцип), либо вплотную примыкают к другим результатам арифметической теории алгебраических групп. В этом смысле настоящая глава дополняет известную книгу Серра [1], посвященную изложению собственно теории когомологий. К этой книге мы и будем отсылать читателя за доказательствами используемых нами фактов общего характера.

Ряд результатов публикуется здесь впервые. Например, мы впервые приводим полное доказательство принципа Хассе для односвязных групп.

§ 6.1. Основные результаты

В этом параграфе собраны основные результаты об описании множества $H^1(K, G)$ одномерных когомологий Галуа алгебраической K-группы G, где в качестве K выступает конечное, локальное либо числовое поле. Последующие параграфы содержат доказательства сформулированных здесь теорем. Некоторые приложения полученных результатов и их связь с классическими фактами о классификации квадратичных, эрмитовых и др. форм будут даны в § 6.5—6.6. Основные определения, связанные с некоммутативными когомологиями Галуа, см. в § 1.3 (более систематическое изложение читатель может найти в книге Серра [1]). Отметим, что доказательства ряда теорем этой главы о когомологиях полупростых групп весьма техничны, и их можно опустить при первом чтении (в действительности для понимания большей части книги достаточно знакомства с настоящим параграфом).

Мы начинаем с конечного поля K, для которого исчерпывающее описание $H^1(K, G)$ дает

Теорема 1 (Ленг [1]). *Пусть G — связная алгебраическая группа, определенная над конечным полем K. Тогда $H^1(K, G) = 1$.*

Доказательство будет дано в § 6.2. Там же будет приведен ряд следствий из теоремы 1. В частности, будет показано, что любая связная группа над конечным полем K является квазиразложимой, т. е. обладает K-определенной подгруппой Бореля. Отсюда при помощи леммы Гензеля выводится следующий важный результат: если связная группа G определена над числовым полем K, то для почти всех $v \in V_f^K$ она квазиразложима над пополнением K_v.

Кроме того, из теоремы 1 вытекает ряд необходимых для дальнейшего фактов о когомологиях групп целых v-адических точек и адельных групп. Отметим, что как следует из одного результата Стейнберга (см. теорему 23), утверждение теоремы 1 сохраняет силу и в более общей ситуации полей K, у которых так называемая когомологическая размерность $\mathrm{cd}(K)$ не превосходит 1. В остальных случаях множество $H^1(K, G)$, вообще говоря, нетривиально, и поэтому возникает задача его описания. Как следует из предложения 2.9, ее достаточно решить для редуктивной группы G. Согласно теореме 2.4 такая группа является почти прямым произведением тора и полупростой группы, и поэтому вычисление $H^1(K, G)$ в значительной степени сводится к двум основным случаям: (а) G — тор; (б) G — полупростая группа, которыми мы и будем заниматься. Результаты для полупростых групп по своей природе существенно отличаются от случая торов, причем в действительности факты о когомологиях торов используются при вычислении когомологий в полупростом случае. По этой причине мы рассмотрим вначале случай алгебраических торов.

Известно (см. § 2.1, п. 7), что любой K-тор T с точностью до изоморфизма определяется заданием на группе характеров $\mathbf{X}(T)$ структуры модуля над абсолютной группой Галуа $\mathrm{Gal}\,(\bar{K}/K)$ (напоминаем, что у нас поле K всюду предполагается совершенным, причем в большинстве случаев $\mathrm{char}\, K = 0$). Поэтому естественно попытаться связать группы когомологий $H^1(K, T)$ и $H^1(K, \mathbf{X}(T))$. Здесь прежде всего удобно заменить когомологии проконечной группы $\mathrm{Gal}(\bar{K}/K)$ когомологиями некоторой конечной факторгруппы. Для этого следует заметить (см. лемму 8), что $H^1(K, T) = H^1(L/K, T)$ и $H^1(K, T) = H^1(L/K, \mathbf{X}(T))$, где L — некоторое поле разложения для T (т. е. конечное расширение Галуа поля K, над которым тор T становится разложимым).

В дальнейшем удобно перейти от обычных когомологий Галуа к так называемым *модифицированным*, которые были

введены Тейтом. Точное определение групп когомологий Тейта $\hat{H}^i(G, A)$ коммутативного модуля A над конечной группой G мы приведем в § 6.3, а пока ограничимся указанием на тот факт, что группы $\hat{H}^i(G, A)$ существуют для всех целых значений i, причем $\hat{H}^i(G, A) = H^i(G, A)$ для $i \geqslant 1$. Кроме того, для когомологий Тейта остается в силе основное свойство когомологий: точной последовательности G-модулей $0 \to A \to B \to C \to 0$ отвечает бесконечная в обе стороны точная последовательность:

$$\ldots \to \hat{H}^q(G, A) \to \hat{H}^q(G, B) \to \hat{H}^q(G, C) \to \hat{H}^{q+1}(G, A) \to \ldots$$

В этих обозначениях справедлива

Теорема 2 (Накаяма — Тейт; локальный вариант). *Пусть K — локальное поле. Тогда для любого K-определенного тора T с полем разложения L и любого целого i имеет место изоморфизм*

$$\hat{H}^i(L/K, T) \simeq \hat{H}^{2-i}(L/K, \mathbf{X}(T)).$$

В частности, $H^1(L/K, T) \simeq H^1(L/K, \mathbf{X}(T))$.

Следует отметить, что изоморфизм в теореме 2 имеет характер изоморфизма конечной абелевой группы со своей двойственной. Для получения естественного изоморфизма вместо группы характеров $\mathbf{X}(T)$ следует рассмотреть двойственную группу кохарактеров (однопараметрических подгрупп) $\mathbf{X}_*(T) = \mathrm{Hom}(\mathbf{G}_m, T)$ (см. § 2.1, п. 7), и тогда $\hat{H}^{i-2}(L/K, \mathbf{X}_*(T)) \simeq \hat{H}(L/K, T)$, причем изоморфизм индуцируется $\smile$-умножением на образующую группы

$$\hat{H}^2(L/K, L^*) = \mathrm{Br}(L/K) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z},$$

где $n = [L : K]$ (подробности см. в § 6.3).

Из теоремы 2 вытекает, что для *локального поля* K группа $H^1(K, T)$ конечна. Ниже мы увидим, что этот результат остается справедливым, если заменить T на любую алгебраическую K-группу.

Изучение группы $H^1(K, T)$ для тора T над числовым полем K базируется на рассмотрении отображения $H^1(L/K, T) \to \prod_v H^1(L_w/K_v, T)$ (для каждого v выбирается одно продолжение $w|v$). Легко видеть, что его образ лежит в группе $H^1(L/K, T_{A_L})$, где A_L — кольцо аделей поля L, так что на самом деле мы имеем отображение $H^1(L/K, T) \xrightarrow{\varphi} H^1(L/K, T_{A_L})$. Для вычисления его ядра и коядра рассматривается точная последовательность

$$1 \to T_L \to T_{A_L} \to C_L(T) \to 1,$$

где $C_L(T) = T_{A_L}/T_L$ — группа классов аделей тора T над L, и соответствующая когомологическая последовательность

$$H^0(L/K, C_L(T)) \to H^1(L/K, T) \xrightarrow{\varphi} H^1(L/K, T_{A_L}) \to H^1(L/K, C_L(T)).$$

Описание групп когомологий $\hat{H}^i(L/K, C_L(T))$ дает

Теорема 3 (Накаяма — Тейт; глобальный вариант). *Пусть K — числовое поле. Тогда для любого K-определенного тора T с полем разложения L и любого целого i имеет место изоморфизм*

$$\hat{H}^i(L/K, C_L(T)) \simeq \hat{H}^{2-i}(L/K, \mathbf{X}(T)).$$

К теореме 3 в полной мере относится замечание, сделанное после формулировки теоремы 2. Кроме того, следует отметить, что несмотря на различие объектов, участвующих в формулировках теорем 2 и 3, в основе их доказательства лежит один и тот же когомологический формализм (так называемая теорема Тейта, см. § 6.3), возможность использования которого обосновывается соответственно локальной и глобальной теорией полей классов. Отметим также, что в § 6.3 мы изучим взаимоотношения между изоморфизмами в теоремах 2 и 3.

Из теоремы 3 вытекает, что ядро и коядро морфизма φ конечны. Группа $\operatorname{Ker}\varphi$ носит название *группы Шафаревича — Тейта* тора T и обозначается $Ш(T)$. Если $Ш(T) = 1$, то говорят, что для тора T выполняется *локально-глобальный принцип*, или *принцип Хассе*; в общем случае $Ш(T)$ выражает отклонение от локально-глобального принципа. Эта терминология естественна, ибо для норменного тора $T = \mathbf{R}^{(1)}_{L/K}(\boldsymbol{G}_m)$ тривиальность $Ш(T)$ равносильна выполнению классического норменного принципа Хассе в расширении L/K. Используя теоремы 2 и 3, Тейт показал, что для расширения Галуа L/K с группой Галуа $\mathscr{G}$ группа Шафаревича — Тейта $Ш(T)$ тора $T = \mathbf{R}^{(1)}_{L/K}(\boldsymbol{G}_m)$ изоморфна ядру канонического гомоморфизма $H^3(\mathscr{G}, \mathbf{Z}) \to \prod_v H^3(\mathscr{G}_v, \mathbf{Z})$, где $\mathscr{G}_v$ — группа разложения в $\mathscr{G}$ некоторого продолжения нормирования v. Однако до недавнего времени не существовало исследования $Ш(T)$ для норменного тора $T = \mathbf{R}^{(1)}_{L/K}(\boldsymbol{G}_m)$ в случае, когда L/K не является расширением Галуа. Такое исследование было выполнено в работах Платонова, Дракохруста [1], [2], Дракохруста, Платонова [1] и Дракохруста [1]; эти результаты излагаются в § 6.3.

С качественной точки зрения теоремы 2 и 3 дают два основных факта о когомологиях Галуа алгебраических торов: конечность $H^1(K, T)$ для торов над локальным полем K и конечность $Ш(T)$ для торов над числовым полем K. В § 6.4 мы установим, что эти два факта остаются справедливыми для произвольных

алгебраических групп. Естественно, что в основе доказательства этих результатов в общей ситуации лежат соображения, совершенно отличные от тех, которые используются при доказательстве теорем 2, 3. А именно, оказывается, что конечность $H^1(K, G)$ для локального поля K (теорема 14) фактически не зависит от структуры группы G, а является следствием одного специального свойства абсолютной группы Галуа $\mathrm{Gal}(\bar{K}/K)$ поля K (так называемого свойства (F)). С другой стороны, конечность ядра $Ш(G)$ отображения $H^1(K, G) \to \prod_v H^1(K_v, G)$ *) (теорема 15), вытекает из теории приведения для групп аделей, которую мы построили в гл. V.

Рассмотрим теперь вопрос о точном вычислении когомологий. Как мы уже отмечали, здесь можно ограничиться случаем редуктивных групп, а последний — по модулю имеющихся результатов о когомологиях торов — сводится к случаю полупростых групп.

Если G — полупростая группа над локальным полем K, то, в отличие от случая конечного поля, уже не всегда $H^1(K, G) = 1$, однако справедлива следующая

Теорема 4. *Пусть G — односвязная полупростая группа над неархимедовым локальным полем K. Тогда $H^1(K, G) = 1$.*

Чтобы вычислить $H^1(K, G)$ для произвольной полупростой группы G над локальным полем K, рассмотрим универсальное K-определенное накрытие $\tilde{G} \xrightarrow{\pi} G$ (см. предложение 2.10). Из точной последовательности $1 \to F \to \tilde{G} \xrightarrow{\pi} G \to 1$, где $F = \mathrm{Ker}\,\pi$ — фундаментальная группа G, в силу центральности F получается отображение δ: $H^1(K, G) \to H^2(K, F)$ (см. § 2.2, п. 3). Тогда основной результат состоит в том, что δ биективно (отметим, что инъективность δ вытекает из теоремы 4, а сюръективность устанавливается в теореме 20). В частности, множество с отмеченным элементом $H^1(K, G)$ снабжается «естественной» структурой абелевой группы. Приводимое нами в § 6.7—6.8 доказательство теоремы 4 использует структурную информацию о полупростых группах и элементы их классификации. Существует также единообразное доказательство теоремы 4, основывающееся на теории Брюа — Титса (см. Брюа — Титс [2]).

В процессе доказательства теоремы 4 будет получен также следующий важный результат.

Теорема 5. *Пусть G — простая односвязная анизотропная группа над локальным полем K. Тогда $G = \mathbf{SL}_1(D)$ для некоторой конечномерной алгебры с делением D над K.*

Теорема 5 также может быть выведена из теории Брюа — Титса, однако мы, излагая доказательство теорем 4, 5, избрали

*) Напомним, что в некоммутативных когомологиях ядро понимается как прообраз отмеченного элемента, т. е. класса эквивалентности тривиального коцикла.

структурный вариант рассуждений, ибо он пригоден и для изучения когомологии над числовыми полями (где альтернативного доказательства соответствующих результатов до сих пор не существует). Отметим высказанное Серром [1] предположение о том, что утверждение, аналогичное теореме 4, должно выполняться всякий раз, когда когомологическая размерность $\mathrm{cd}(K)$ не превосходит 2. С другой стороны, вопрос о справедливости в данной ситуации теоремы 20 (т. е. вопрос о сюръективности кограничного отображения δ) сводится к классическому в теории простых алгебр вопросу о совпадении экспоненты и индекса простых K-алгебр. Для так называемых C_2-полей, класс которых фактически совпадает с классом полей когомологической размерности, не превосходящей 2, это утверждение высказано в качестве гипотезы в статье М. Артина [1].

Из теоремы 4 вытекают также некоторые факты о классификации простых групп, которые понадобятся нам в гл. VII при доказательстве гипотезы Кнезера — Титса над локальными полями. Так, например, любая группа типа ${}^2E_6$ над локальным полем оказывается квазиразложимой, а любая группа типа E_7 становится разложимой над произвольным квадратичным расширением K.

Вычисление $H^1(K, G)$ над числовым полем K, как и в случае торов, базируется на рассмотрении канонического отображения $H^1(K, G) \xrightarrow{\rho} \prod_v H^1(K_v, G)$. В случае когда ρ инъективно, естественно говорить, что для группы G выполняется *принцип Хассе*, ибо, скажем, инъективность ρ для ортогональной группы $G = \boldsymbol{O}_n(f)$ равносильна справедливости локально-глобального принципа в вопросе эквивалентности квадратичных форм. К сожалению, отображение ρ не всегда инъективно, однако уже довольно давно была выдвинута гипотеза (см. Серр [1]), что оно инъективно, если группа G односвязна. Доказательство этого факта для классических групп (см. Кнезер [12]) тесно связано с классическими результатами о классификации квадратичных, эрмитовых и т. д. форм. Исключительные группы, кроме типа E_8, были исследованы Хардером [1], [2]. Случай групп типа E_8 оставался не рассмотренным более двадцати лет. Доказательство здесь было получено совсем недавно Черноусовым [6]. Таким образом, мы впервые излагаем полное доказательство принципа Хассе для односвязных групп (см. § 6.7—6.8).

Согласно теореме 4 для односвязной группы G имеем $H^1(K_v, G) = 1$, если v — неархимедово, поэтому в действительности ρ сводится к отображению

$$H^1(K, G) \xrightarrow{\theta} \prod_{v \in V_\infty^K} H^1(K_v, G),$$

которое инъективно в силу справедливости принципа Хассе. Оказывается, что здесь справедлив следующий точный результат.

Теорема 6. *Для односвязной K-группы G отображение θ биективно.*

Для полноты картины остается описать вещественные когомологии $H^1(\mathbb{R}, G)$ простой односвязной $\mathbb{R}$-группы G. В случае, когда группа $G_{\mathbb{R}}$ компактна, это проделано в книге Серра [1] (см. гл. 3, § 4.5). Общий случай был недавно рассмотрен Боровым [2].

Вычисление $H^1(K, G)$ для произвольной полупростой группы G, как и в локальном случае, получается исходя из точной последовательности $1 \to F \to \tilde{G} \to G \to 1$, где $\tilde{G}$ односвязна, а $F = \operatorname{Ker} \pi$ — фундаментальная группа G. А именно, можно показать, что в получающейся когомологической точной последовательности $H^1(K, \tilde{G}) \to H^1(K, G) \xrightarrow{\delta} H^2(K, F)$ отображение δ сюръективно (теорема 20). Отметим также, что над вполне мнимым числовым полем остается справедливым утверждение, аналогичное теореме 5.

Из справедливости принципа Хассе для односвязных групп вытекает его справедливость и для присоединенных групп (см. § 6.5). С его помощью выводятся также некоторые факты о классификации простых групп над числовыми полями. В частности, *любая простая группа над числовым полем K, относящаяся к одному из типов B_n, C_n, E_8, F_4, G_2, разложима над некоторым квадратичным расширением K.*

Описанные результаты позволяют вычислять множество $H^1(K, G)$ для любой связной алгебраической группы G над локальным или числовым полем K. Как заметил Боровой, используя введенное им понятие фундаментальной группы произвольной связной алгебраической группы и результаты Коттвица [1], [2], эти факты можно сформулировать единообразно в духе теорем 2, 3.

§ 6.2. Когомологии алгебраических групп над конечными полями

Начнем с доказательства теоремы Ленга о том, что $H^1(K, G) = 1$ для любой связной алгебраической группы G, определенной над конечным полем K (теорема 1). Достаточно показать, что $H^1(L/K, G) = 1$ для любого конечного расширения Галуа L/K. Известно, что группа Галуа $\operatorname{Gal}(L/K)$ циклическая и порождается так называемым автоморфизмом Фробениуса φ: $x \mapsto x^q$, $x \in L$, где $q = [K]$ — число элементов поля K. (Отметим, что последняя формула определяет одновременно автоморфизм из $\operatorname{Gal}(\bar{K}/K)$, который мы также будем называть автоморфизмом Фробениуса и обозначать той же буквой φ; ясно, что φ

является топологической образующей группы $\mathrm{Gal}(\bar{K}/K)$.) Пусть $g=\{g_\sigma\}\in Z^1(L/K, G)$ — некоторый коцикл. Утверждается, что для доказательства тривиальности g достаточно найти элемент $x\in G_{\bar{K}}$ со свойством $g_\varphi = x^{-1}\varphi(x)$. Действительно, тогда

$$g_{\varphi^2} = g_\varphi \varphi(g_\varphi) = x^{-1}\varphi(x)\varphi(x^{-1}\varphi(x)) = x^{-1}\varphi^2(x),$$

и, рассуждая аналогично при помощи очевидной индукции, легко получить, что $g_{\varphi^i} = x^{-1}\varphi^i(x)$ для любого i. При этом если $n = [L:K]$, то $g_{\varphi^n} = g_e = 1$, с другой стороны — $g_{\varphi^n} = x^{-1}\varphi^n(x)$, откуда $\varphi^n(x) = x$, т. е. $x\in G_L$, и тривиальность коцикла g в $Z^1(L/K, G)$ установлена. Таким образом, завершает доказательство теоремы Ленга

Лемма 1. *Если K-группа G связна, то множество $X = \{x^{-1}\varphi(x) \mid x\in G_{\bar{K}}\}$ совпадает с $G_{\bar{K}}$.*

Доказательство основано на интерпретации действия автоморфизма Фробениуса φ на $G_{\bar{K}}$ как регулярного K-определенного морфизма многообразий. А именно, для произвольного K-определенного подмногообразия $V\subset \mathbb{A}^n$ и любой точки $x=(x_1, \ldots, x_n)\in V_{\bar{K}}$ положим $x^{(q)} = (x_1^q, \ldots, x_n^q)$. Тогда $x^{(q)}\in V_{\bar{K}}$, так что отображение f_q: $x\mapsto x^{(q)}$ задает K-определенный регулярный эндоморфизм многообразия V, который на $\bar{K}$-точках совпадает с автоморфизмом Фробениуса (отметим, что f_q биективен и не зависит от выбора аффинной реализации V). Непосредственное вычисление показывает, что дифференциал $d_x f_q$ в любой точке $x\in V$ является нулевым отображением. Применим эти факты к связной K-определенной алгебраической группе G.

Лемма 2. *Пусть $a\in G$. Тогда отображение s_a: $G\to G$, $s_a(g) = g^{-1}ag^{(q)}$ сепарабельно. Его образ открыт и замкнут.*

Доказательство. Имеем

$$d_e s_a(X) = -Xa + d_e f_q(X) = -Xa, \quad X\in T_e(G),$$

так что дифференциал $d_e s_a$: $T_e(G)\to T_a(G)$ определяет изоморфизм касательных пространств. Отсюда следует, что s_a является доминантным сепарабельным морфизмом (см. Борель [8], гл. АГ, теорема 17.3). В частности, образ $s_a(G)$ содержит открытое в G подмножество. Но $s_a(G)$ можно интерпретировать как орбиту относительно действия $G\times G\to G$, $(g, h)\mapsto g^{-1}hg^{(q)}$, так что все множество $s_a(G)$ открыто в G. Поскольку это верно для любого a, то множества $s_a(G)$ одновременно и замкнуты. Лемма 2 доказана.

В силу связности G из леммы 2 вытекает, что $s_a(G) = G$ для любого $a\in G$; в частности, $s_e(G) = G$ и $s_e(G_{\bar{K}}) = G_{\bar{K}}$. С другой стороны, легко видеть, что множество $s_e(G_{\bar{K}})$ совпадает

с множеством X в формулировке леммы 1. Таким образом, лемма 1 и теорема Ленга доказаны.

Несмотря на свою простоту, теорема Ленга имеет ряд важных следствий.

Предложение 1. *Пусть G — связная алгебраическая группа над конечным полем K. Тогда G является K-квазиразложимой, т. е. обладает K-определенной подгруппой Бореля. При этом две K-определенные подгруппы Бореля в G сопряжены с помощью элемента из G_K.*

Доказательство. Пусть $B \subset G$ — подгруппа Бореля, определенная над $\bar{K}$, φ — автоморфизм Фробениуса из $\mathrm{Gal}(\bar{K}/K)$ и B^φ — подгруппа Бореля, получаемая применением φ. По теореме сопряженности найдется такой $g \in G_{\bar{K}}$, что $gB^\varphi g^{-1} = B$, причем, в силу леммы 1, $g = x^{-1}\varphi(x)$ для некоторого $x \in G_{\bar{K}}$. Полагая тогда $H = xBx^{-1}$, мы получим подгруппу Бореля в G, которая в силу соотношения $H^\varphi = \varphi(x)B^\varphi\varphi(x)^{-1} = xgB^\varphi g^{-1}x^{-1} = H$ будет K-определенной. Пусть теперь B_1, B_2 — две K-определенные подгруппы Бореля в G. Тогда $B_2 = gB_1g^{-1}$ для подходящего $g \in G_{\bar{K}}$. В силу K-определенности $B_i^\varphi = B_i$, $i = 1, 2$, откуда

$$\varphi(g)\, B_1^\varphi \varphi(g)^{-1} = gB_1g^{-1},$$

так что элемент $g^{-1}\varphi(g)$ попадает в нормализатор $N_G(B_1)$, который по теореме Шевалле (см. Борель [8], § 11) совпадает с B_1. Применяя лемму 1 к группе B_1, получим, что $g^{-1}\varphi(g) = b^{-1}\varphi(b)$ для подходящего $b \in (B_1)_{\bar{K}}$. Тогда, полагая $h = gb^{-1}$, будем иметь $\varphi(h) = h$, т. е. $h \in G_K$, и $hB_1h^{-1} = gB_1g^{-1} = B_2$. Предложение 1 доказано.

Следствие 1 (теорема Фробениуса). *Пусть K — конечное поле. Тогда над K не существует некоммутативных конечномерных центральных алгебр с делением.*

Действительно, пусть D — конечномерная центральная алгебра с делением над K. Рассмотрим группу $G = \boldsymbol{SL}_1(D)$ (см. § 2.3). Если предположить, что $D \neq K$, то G является нетривиальной простой K-анизотропной группой (предложение 2.7). С другой стороны, согласно предложению 1 группа G обязана быть квазиразложимой, в частности, $\mathrm{rang}_K G > 0$, — противоречие. Другое доказательство можно получить, воспользовавшись тем обстоятельством, что классы изоморфизма простых центральных алгебр над K размерности n^2 находятся в биективном соответствии с элементами множества $H^1(K, H)$, где $H = \boldsymbol{PGL}_n$. Так как $H^1(K, H) = 1$, то существует лишь одна такая алгебра, а именно $M_n(K)$, которая не является алгеброй с делением.

Предложение 2. *Пусть G — связная группа над конечным полем K, W — непустое K-многообразие, на котором группа G действует транзитивно и K-рационально (однородное пространство*

группы G). Тогда $W_K \neq \varnothing$. Кроме того, если стабилизатор $G(x)$ некоторой точки $x \in W$ связен, то группа G_K действует на W_K транзитивно.

Доказательство. Пусть $y \in W_K$. Воспользовавшись транзитивностью действия, найдем такой элемент $g \in G_{\bar{K}}$, что $g\varphi(y) = y$ (где φ, как и выше, автоморфизм Фробениуса), и по лемме 1 представим его в виде $g = h^{-1}\varphi(h)$, где $h \in G_{\bar{K}}$. Тогда $\varphi(hy) = hy$, т. е. $z = hy \in W_K$. Если теперь стабилизатор $G(x)$ некоторой точки $x \in W$ связен, то в силу однородности W стабилизатор любой точки связен; в частности, связна группа $H = G(z)$. Как известно (см. § 1.3, п. 2), орбиты группы G_K на W_K взаимно однозначно соответствуют элементам $\operatorname{Ker}(H^1(K, H) \to H^1(K, G))$. Но поскольку $H^1(K, H) = 1$, то в действительности имеется лишь одна орбита. (Отметим, что предложение 1 является на самом деле непосредственным следствием предложения 2, ибо согласно теореме 2.19 множество всех подгрупп Бореля связной K-группы G наделяется естественной структурой K-определенного однородного пространства группы G, однако мы предпочли дать независимое рассуждение.)

Следствие 2. *Пусть L — конечное расширение конечного поля K. Тогда норменное отображение $N_{L/K}\colon L^* \to K^*$ сюръективно.*

Пусть $a \in K^*$. Тогда норменная гиперповерхность $W = \left\{x \in L \bigotimes_K \bar{K} \mid N_{L/K}(x) = a\right\}$ является однородным пространством норменного тора $T = \mathbf{R}^{(1)}_{L/K}(\boldsymbol{G}_m)$, и поэтому $W_K \neq \varnothing$, т. е. $a \in N_{L/K}(L^*)$. Можно также воспользоваться теоремой 1 и тем обстоятельством, что $H^1(K, T) = K^*/N_{L/K}(L^*)$ (см. лемму 2.5).

Следствие 3. *Пусть f — невырожденная квадратичная форма над конечным полем K от $n \geqslant 2$ переменных. Тогда f представляет любой элемент поля K. Следовательно, любая форма от $n \geqslant 3$ переменных представляет над K нуль.*

В самом деле, если $a \in K^*$, то, как следует из теоремы Витта (см. теорему 2.10), при $n \geqslant 2$ квадрика $W = \{x \in \bar{K}^n \mid f(x) = a\}$ является однородным пространством связной группы $G = \boldsymbol{SO}_n(f)$, и поэтому наше утверждение вытекает из предложения 2. Изотропность невырожденной формы от $n \geqslant 3$ переменных является следствием предложения 2.14 и факта, что группа $G = \boldsymbol{SO}_n(f)$ является K-квазиразложимой (предложение 1) и в частности, K-изотропной.

Чтобы завершить описание основных свойств квадратичных форм над конечными полями, напомним (см. предложение 2.8), что множество $H^1(K, \boldsymbol{SO}_n(f))$ классифицирует классы эквивалентности n-мерных квадратичных форм над K, дискриминант которых совпадает с дискриминантом f. Поэтому из теоремы 1 получаем

Следствие 4. *Две невырожденные n-мерные квадратичные формы над K эквивалентны в том и только том случае, если они имеют одинаковый дискриминант. Таким образом, для любого n имеется в точности 2 класса эквивалентности невырожденных n-мерных форм.*

Отметим, что второе утверждение следствия вытекает из первого и того, что $[K^*/K^{*2}]=2$, ибо группа K^* циклическая.

Предложение 3 (теорема Ленга об изогениях). *Пусть G, H — связные K-группы, π: $G\to H$ — изогения, определенная над K. Тогда группы G_K и H_K содержат одинаковое число элементов.*

Доказательство. Положим $F=\operatorname{Ker}\pi$ и рассмотрим точную последовательность $1\to F_{\bar K}\to G_{\bar K}\to H_{\bar K}=1$. Переходя к когомологиям, мы в силу совершенности K получим точную последовательность $F_K\to G_K\to H_K\to H^1(K,F)\to H^1(K,G)$. Так как $H^1(K,G)=1$ (теорема 1), то мы приходим к следующему соотношению для порядков:

$$[H_K]=[G_K]\frac{[H^1(K,F)]}{[F_K]},$$

и достаточно показать, что $[H^1(K,F)]=[F_K]$. Но поскольку $\operatorname{Gal}(\bar K/K)\simeq\hat{\mathbb{Z}}$ (где $\hat{\mathbb{Z}}$ — проконечное пополнение группы $\mathbb{Z}$), это вытекает из следующего утверждения.

Лемма 3. *Для любого конечного $\hat{\mathbb{Z}}$-модуля F справедливо равенство $[H^0(\hat{\mathbb{Z}},F)]=[H^1(\hat{\mathbb{Z}},F)]$.*

Доказательство является простым следствием свойств индекса Эрбрана (см., например, [АТЧ], гл. IV, § 8), но можно рассуждать и непосредственно. Обозначим через σ образующую $\hat{\mathbb{Z}}$. Из конечности F вытекает существование такого m, что σ^m действует на F тривиально. Тогда для любого $x\in F$ произведение $\prod_{i=0}^{m-1}\sigma^i(x)$ лежит в группе неподвижных точек F^σ. Поэтому, полагая $n=mf$, где $f=[F^\sigma]$, будем иметь

$$\prod_{i=0}^{n-1}\sigma^i(x)=\prod_{j=0}^{f-1}\sigma^{jm}\left(\prod_{i=0}^{m-1}\sigma^i(x)\right)=\left(\prod_{i=0}^{m-1}\sigma^i(x)\right)^f=1. \qquad (1)$$

Покажем теперь, что ограничение любого коцикла из $Z^1(\hat{\mathbb{Z}},F)$ на $n\hat{\mathbb{Z}}$ тривиально. Действительно, по построению группа $m\hat{\mathbb{Z}}$ действует на F тривиально, и поэтому ограничение коцикла $\zeta\in Z^1(\hat{\mathbb{Z}},F)$ на $m\hat{\mathbb{Z}}$ является гомоморфизмом $m\hat{\mathbb{Z}}$ в F. Но тогда ограничение ζ на $n\hat{\mathbb{Z}}=f(m\hat{\mathbb{Z}})$ тривиально. Из последовательности Хохшильда — Серра (см. (4) в § 1.3) теперь вытекает, что $H^1(\hat{\mathbb{Z}},F)=H^1(\mathbb{Z}/n\mathbb{Z},F)$ в смысле индуцированного действия $\mathbb{Z}/n\mathbb{Z}=\hat{\mathbb{Z}}/n\hat{\mathbb{Z}}$ на F. Кроме того, $H^0(\hat{\mathbb{Z}},F)=H^0(\mathbb{Z}/n\mathbb{Z},F)$.

Пусть τ — образ σ в $\mathbb{Z}/n\mathbb{Z}$. Так как $H^1(\mathbb{Z}/n\mathbb{Z}, F) = N/F^{(1-\tau)}$, где $N = \left\{x \in F \,\middle|\, \prod_{i=0}^{n-1} \tau^i(x) = 1\right\}$, $F^{(1-\tau)} = \{x/\tau(x) \mid x \in F\}$, то с учетом (1) получаем

$$[H^1(\mathbb{Z}/n\mathbb{Z}, F)] = \frac{[F]}{[F^{(1-\tau)}]} = \frac{[F]}{[F]/[F^\tau]} = [F^\tau] = [H^0(\mathbb{Z}/n\mathbb{Z}, F)].$$

Лемма доказана.

Теорема 1 может быть применена также для классификации простых K-определенных групп (при этом достаточно рассматривать только односвязные группы). Так как в силу предложения 2 любая K-группа является квазиразложимой, то все K-формы простой односвязной K-группы с системой корней R классифицируются элементами множества $H^1(K, \mathrm{Sym}(R))$, где $\mathrm{Sym}(R)$ — группа симметрий диаграммы Дынкина системы R (см. § 2.2, п. 4). Учитывая, что $\mathrm{Gal}(\overline{K}/K) = \hat{\mathbb{Z}}$, отсюда получаем, что любая K-группа типов B_n, C_n, E_7, E_8, F_4, G_2 разложима над K; для каждого из типов $A_n (n \geqslant 2)$, $D_n (n \geqslant 5)$, E_6 существует в точности 2 неизоморфные K-группы — разложимая и неразложимая (отметим, что последняя является квазиразложимой и разложимой над квадратичным расширением K); для типа D_4 имеется 3 неизоморфные K-группы — разложимая и 2 неразложимые, которые становятся разложимыми соответственно над квадратичным и кубическим расширением K.

Из теоремы Ленга и леммы Гензеля вытекает следующий важный результат для групп над числовыми полями.

Теорема 7. *Пусть G — связная группа над числовым полем K. Тогда для почти всех $v \in V_f^K$ группа G является K_v-квазиразложимой.*

Доказательство. Пусть $\mathscr{B}$ — многообразие борелевских подгрупп группы G (см. § 2.4, п. 9). Тогда из предложения 3.19 вытекает, что для почти всех $v \in V_f^K$ существуют гладкие редукции $\underline{G}^{(v)}$ и $\underline{\mathscr{B}}^{(v)}$. Утверждается, что для почти всех v редукция $\underline{\mathscr{B}}^{(v)}$ совпадает с многообразием борелевских подгрупп группы $\underline{G}^{(v)}$ (отметим, что согласно теореме 3.12 редукция $\underline{G}^{(v)}$ является связной группой для почти всех v, а поэтому понятие «многообразие борелевских подгрупп» имеет смысл). В самом деле, пусть L/K — такое конечное расширение, что существует L-определенная подгруппа Бореля $B \subset G$. Тогда $\mathscr{B} = G/B$ над L и поэтому для почти всех $w \in V_f^L$ имеем $\underline{\mathscr{B}}^{(w)} = \underline{G}^{(w)}/\underline{B}^{(w)}$ (см. предложение 3.22). Так как многообразие $\underline{\mathscr{B}}^{(w)}$ проективно, то группа $\underline{B}^{(w)}$, будучи разрешимой, является подгруппой Бореля в $\underline{G}^{(w)}$. Поэтому для почти всех $w \in V_f^L$ редукция $\underline{\mathscr{B}}^{(w)}$ является мно-

гообразием подгрупп Бореля группы $\underline{G}^{(w)}$. Но известно (лемма 3.11), что для почти всех $v \in V_f^K$ и соответствующих $w \in V_f^L$, $w \mid v$, $\underline{G}^{(w)} = \underline{G}^{(v)}$ и $\underline{\mathscr{B}}^{(w)} = \underline{\mathscr{B}}^{(v)}$. Из доказанного в силу предложения 1 вытекает, что $\underline{\mathscr{B}}_{k_v}^{(v)} \neq \varnothing$, где k_v — поле вычетов K относительно v. Так как $\underline{\mathscr{B}}^{(v)}$ гладко, то применяя проективный аналог леммы Гензеля, получим, что $\mathscr{B}_{\mathcal{O}_v} \neq \varnothing$; в частности, $\mathscr{B}_{K_v} \neq \varnothing$, т. е. G обладает K_v-определенной подгруппой Бореля. Теорема 7 доказана.

Наконец, используя теорему Ленга, мы сейчас получим необходимые для дальнейшего результаты о когомологиях групп целых v-адических точек и адельных групп. Пусть G — алгебраическая группа, определенная над локальным полем K_v и L_w/K_v — конечное расширение Галуа. Тогда группа целых w-адических точек $G_{\mathcal{O}_w}$ (где $\mathcal{O}_w = \mathcal{O}_{L_w}$) инвариантна относительно группы Галуа $\mathrm{Gal}(L_w/K_v)$, так что определено множество 1-когомологий $H^1(L_w/K_v, G_{\mathcal{O}_w})$.

Теорема 8. *Если связная группа G имеет связную гладкую редукцию $\underline{G}^{(v)}$ и расширение L_w/K_v неразветвлено, то $H^1(L_w/K_v, G_{\mathcal{O}_w}) = 1$.*

Доказательство. Обозначим через $\mathfrak{p}_v$ и $\mathfrak{P}_w$ максимальные идеалы в кольцах $\mathcal{O}_v$ и $\mathcal{O}_w$ соответственно, и пусть k_v и l_w — соответствующие поля вычетов. Поскольку редукция $\underline{G}^{(v)}$ гладкая, из леммы Гензеля вытекает точность последовательности

$$1 \to G_{\mathcal{O}_w}(\mathfrak{P}_w) \to G_{\mathcal{O}_w} \to \underline{G}_{l_w}^{(v)} \to 1. \tag{2}$$

В силу неразветвленности L_w/K_v группы Галуа $\mathrm{Gal}(L_w/K_v)$ и $\mathrm{Gal}(l_w/k_v)$ изоморфны, причем их действие на группы, входящие в (2), согласованно. Поэтому из (2) получаем точную последовательность когомологий

$$H^1(L_w/K_v, G_{\mathcal{O}_w}(\mathfrak{P}_w)) \to H^1(L_w/K_v, G_{\mathcal{O}_w}) \to H^1(l_w/k_v, \underline{G}_{l_w}^{(v)}). \tag{3}$$

По теореме Ленга последний член в (3) тривиален, так что достаточно установить тривиальность $H^1(L_w/K_v, G_{\mathcal{O}_w}(\mathfrak{P}_w))$.

Лемма 4. *Для любого целого $j \geqslant 1$ имеем*

$$H^1\left(L_w/K_v, G_{\mathcal{O}_w}(\mathfrak{P}_w^j)/G_{\mathcal{O}_w}(\mathfrak{P}_w^{j+1})\right) = 1.$$

Доказательство. Пусть $G \subset \boldsymbol{GL}_n$. Рассмотрим отображение $GL_n(\mathcal{O}_w, \mathfrak{P}_w^j) \xrightarrow{\theta} M_n(l_w)$, определяемое формулой $\theta(1 + \pi^j A) = \bar{A}$, где π — униформизующий элемент в K_v, который в силу неразветвленности L_w/K_v является одновременно униформизующим и в L_w, а для матрицы $A \in M_n(\mathcal{O}_w)$ через $\bar{A}$ обозначена редукция по модулю $\mathfrak{P}_w$. Легко проверяется, что θ является сюръективным гомоморфизмом, а его ядром служит конгруэнц-под-

группа $GL_n(\mathcal{O}_w, \mathfrak{P}_w^{j+1})$. При этом θ согласован с естественным изоморфизмом групп $\mathrm{Gal}(L_w/K_v)$ и $\mathrm{Gal}(l_w/k_v)$. Отсюда следует существование изоморфизма

$$H^1\left(L_w/K_v,\ G_{\mathcal{O}_w}(\mathfrak{P}_w^j)/G_{\mathcal{O}_w}(\mathfrak{P}_w^{j+1})\right) \simeq H^1\left(l_w/k_v,\ \theta\left(G_{\mathcal{O}_w}(\mathfrak{P}_w^j)\right)\right).$$

Ниже мы покажем, что $B = \theta\left(G_{\mathcal{O}_w}(\mathfrak{P}_w^j)\right)$ совпадает с редукцией по модулю $\mathfrak{P}_w$ пересечения $\mathfrak{g}_{\mathcal{O}_w} = \mathfrak{g} \cap M_n(\mathcal{O}_w)$, где $\mathfrak{g}$ — алгебра Ли группы G. Это, в частности, означает, что B является векторным пространством над полем l_w, и для доказательства леммы 4 остается заметить, что $H^1(l_w/k_v, W) = 0$ для любого конечномерного k_v-определенного векторного пространства W над полем l_w. Последний факт является следствием тривиальности $H^1(l_w/k_v, l_w)$ (аддитивная форма теоремы 90 Гильберта, см. доказательство леммы 2.7) и разложения $W = W_0 \otimes_{k_v} l_w$, где $W_0 = W^{\mathrm{Gal}(l_w/k_v)}$ — пространство неподвижных точек.

Осталось показать, что $B = \overline{\mathfrak{g}}_{\mathcal{O}_w}$. Для этого рассмотрим идеал $\mathfrak{a}$ в кольце регулярных функций $K_v[\boldsymbol{GL}_n]$, состоящий из функций, обращающихся в нуль на G, и выберем конечную систему образующих $f_1(X), \ldots, f_r(X)$ пересечения $\mathfrak{a} \cap \mathcal{O}_v[\boldsymbol{GL}_n]$ как идеала в кольце $\mathcal{O}_v[\boldsymbol{GL}_n]$. Положим $F_i(X, t) = t^{-1} f_i(E_n + tX)$. Поскольку $f_i(E_n) = 0$, то $F_i(X, t)$ лежит в кольце $\mathcal{O}_v[\boldsymbol{GL}_n][t]$. Тогда $G_{\mathcal{O}_w}(\mathfrak{P}_w^j)$ состоит из элементов вида $E_n + \pi^j A$, где $A \in M_n(\mathcal{O}_w)$ удовлетворяет системе

$$F_i(X, \pi^j) = 0, \quad i = 1, \ldots, r. \tag{4}$$

С другой стороны, $\mathfrak{g}_{\mathcal{O}_w}$ состоит из целых w-адических решений системы

$$d_{E_n} f_i(X) = 0, \quad i = 1, \ldots, r. \tag{5}$$

Поскольку редукция $\overline{G}^{(v)}$ является гладкой, то ранг линейной системы (5) совпадает с рангом соответствующей редуцированной системы. Но легко видеть, что редукции систем (4) и (5) одинаковы, откуда следует, что многообразие, определяемое системой (4), имеет гладкую редукцию. Поэтому из леммы Гензеля вытекает, что B и $\overline{\mathfrak{g}}_{\mathcal{O}_w}$ состоят из всех решений в $M_n(l_w)$ одной и той же системы, которая получается редукцией любой из систем (4), (5). Таким образом, $B = \overline{\mathfrak{g}}_{\mathcal{O}_w}$, и лемма 4 доказана.

Из леммы 4 вытекает, что $H^1\left(L_w/K_v,\ G_{\mathcal{O}_w}(\mathfrak{P}_w)/G_{\mathcal{O}_w}(\mathfrak{P}_w^j)\right) = 1$ для любого $j \geqslant 1$. В самом деле, для $j = 2$ это непосредственно

видно из леммы 4. Для бо́льших j рассматривается точная последовательность

$$1 \to G_{\mathfrak{S}_w}(\mathfrak{P}_w^{j-1}) / G_{\mathfrak{S}_w}(\mathfrak{P}_w^j) \to G_{\mathfrak{S}_w}(\mathfrak{P}_w) / G_{\mathfrak{S}_w}(\mathfrak{P}_w^j) \to$$
$$\to G_{\mathfrak{S}_w}(\mathfrak{P}_w) / G_{\mathfrak{S}_w}(\mathfrak{P}_w^{j-1}) \to 1$$

и отвечающая ей точная последовательность когомологий

$$H^1\left(L_w/K_v,\ G_{\mathfrak{S}_w}(\mathfrak{P}_w^{j-1}) / G_{\mathfrak{S}_w}(\mathfrak{P}_w^j)\right) \to$$
$$\to H^1\left(L_w/K_v,\ G_{\mathfrak{S}_w}(\mathfrak{P}_w) / G_{\mathfrak{S}_w}(\mathfrak{P}_{\mathfrak{S}_w}^j)\right) \to$$
$$\to H^1\left(L_w/K_v,\ G_{\mathfrak{S}_w}(\mathfrak{P}_w) / G_{\mathfrak{S}_w}(\mathfrak{P}_w^{j-1})\right). \quad (6)$$

Так как левый член в (6) тривиален в силу леммы 4, то требуемое получается при помощи очевидного индуктивного рассуждения. Таким образом, для любого коцикла $a = \{a_\sigma\} \in Z^1(L_w/K_v, G_{\mathfrak{S}_w}(\mathfrak{P}_w))$ и любого целого $j \geqslant 1$ найдется такой элемент $b_j \in G_{\mathfrak{S}_w}(\mathfrak{P}_w)$, что $b_j^{-1} a_\sigma b_j^\sigma \in G_{\mathfrak{S}_w}(\mathfrak{P}_w^j)$ для всех $\sigma \in \mathrm{Gal}(L_w/K_v)$. В силу компактности $G_{\mathfrak{S}_w}(\mathfrak{P}_w)$ из последовательности $\{b_j\}_{j=1}^\infty$ можно выделить последовательность $\{b_{j_l}\}_{l=1}^\infty$, сходящуюся к некоторому элементу $b \in G_{\mathfrak{S}_w}(\mathfrak{P}_w)$. Тогда

$$b^{-1} a_\sigma b^\sigma = \lim_{\substack{l \to \infty \\ l \geqslant l_0}} b_{j_l}^{-1} a_\sigma b_{j_l}^\sigma \in G_{\mathfrak{S}_w}\left(\mathfrak{P}_w^{j_{l_0}}\right)$$

для любого целого $l_0 \geqslant 1$. Поэтому $b^{-1} a_\sigma b^\sigma \in \prod_{j=1}^\infty G_{\mathfrak{S}_w}\left(\mathfrak{P}_w^{j_l}\right) = \{E_n\}$, откуда $a_\sigma = b(b^{-1})^\sigma$, и коцикл a тривиален. Теорема 8 доказана.

Следствие. *Пусть G — связная алгебраическая группа над полем алгебраических чисел K, L — его конечное расширение Галуа. Тогда для почти всех $v \in V_f^K$ и любого $w|v$ имеем $H^1(L_w/K_v, G_{\mathfrak{S}_w}) = 1$.*

Теорема 8 и еще ряд других результатов о когомологиях групп целых w-адических точек содержится в статье Рольфса [1]. Так как остальные результаты нам в этой книге не понадобятся, мы ограничимся указанием на следующую теорему конечности: для любого расширения L_w/K_v и любой группы G множество когомологий $H^1(L_w/K_v, G_{\mathfrak{S}_w})$ конечно.

До сих пор мы рассматривали когомологии Галуа относительно конечного расширения L_w/K_v, но можно распространить определение и на произвольное расширение Галуа L_w/K_v,

полагая

$$H^1(L_w/K_v, G_{\mathcal{O}_w}) = \varinjlim H^1(P/K_v, G_{\mathcal{O}_P}),$$

где индуктивный предел берется по всем конечным расширениям Галуа P поля K, содержащимся в L_w. Можно также определить $H^1(L_w/K_v, G_{\mathcal{O}_w})$ как группу непрерывных когомологий проконечной группы $\mathrm{Gal}(L_w/K_v)$ с коэффициентами в дискретной группе $G_{\mathcal{O}_w}$. С учетом этого теорему 8 можно переформулировать следующим образом.

Теорема 8′. *Пусть G — связная алгебраическая группа над полем K_v, имеющая связную гладкую редукцию. Тогда*

$$H^1\left(K_v^{\text{нр}}/K_v, G_{\mathcal{O}_{K_v^{\text{нр}}}}\right) = 1,$$

где $K_v^{\text{нр}}$ — максимальное неразветвленное расширение поля K_v. (Другими словами, группа целых точек имеет тривиальные неразветвленные когомологии.)

Выведем из теоремы 8′ одно утверждение об образе группы целых v-адических точек при кограничном морфизме, которое понадобится нам в гл. VII, VIII. Для этого предварительно исследуем более общую ситуацию. Пусть

$$1 \to F \to G \xrightarrow{\pi} H \to 1 \tag{7}$$

— точная последовательность K_v-определенных алгебраических групп. Рассмотрим следующие два условия:

1) существуют гладкие редукции $\underline{F}^{(v)}$, $\underline{G}^{(v)}$ и $\underline{H}^{(v)}$,

2) морфизм π определен над $\mathcal{O}_v$, и индуцированная последовательность $1 \to \underline{F}^{(v)} \to \underline{G}^{(v)} \xrightarrow{\pi^{(v)}} \underline{H}^{(v)} \to 1$ точна.

Лемма 5. *При выполнении условий 1), 2) последовательность*

$$1 \to F_{\mathcal{O}_{K_v^{\text{нр}}}} \to G_{\mathcal{O}_{K_v^{\text{нр}}}} \xrightarrow{\pi} H_{\mathcal{O}_{K_v^{\text{нр}}}} \to 1 \tag{8}$$

точна.

В доказательстве нуждается лишь равенство $\pi\left(G_{\mathcal{O}_{K_v^{\text{нр}}}}\right) = H_{\mathcal{O}_{K_v^{\text{нр}}}}$. Для его проверки заметим, что при $a \in H_{\mathcal{O}_{K_v^{\text{нр}}}}$ уравнение $\pi(x) = a$ определяет подмногообразие в G, которое в силу условий 1), 2) имеет гладкую редукцию. Так как редуцированное уравнение $\pi^{(v)}(x) = \bar{a}$ имеет решение в $\underline{G}^{(v)}_{k_v}$, то по лемме Гензеля исходное уравнение $\pi(x) = a$ имеет решение $x \in G_{\mathcal{O}_{K_v^{\text{нр}}}}$, ибо любое конечное расширение l поля k_v является полем вычетов для конечного неразветвленного расширения L поля K_v.

Проверка условий 1), 2) для индивидуального нормирования v может оказаться затруднительной, однако если группы в (7) определены над числовым полем K, то в важных для дальнейшего случаях эти условия выполнены для почти всех v.

Лемма 6. *Пусть группы F, G, H и морфизм π в (7) определены над числовым полем K, причем группа G связна. Тогда если группа F конечна либо связна, то для почти всех $v \in V_f^K$ выполняются условия* 1), 2).

Доказательство. Принимая во внимание предложение 3.19 и теорему 3.12, мы видим, что достаточно установить выполнимость для почти всех v условия 2), причем можно считать группы $\underline{G}^{(v)}$ и $\underline{H}^{(v)}$ связными. Тогда для конечной группы F сюръективность $\pi^{(v)}$ вытекает из совпадения размерностей $\underline{G}^{(v)}$ и $\underline{H}^{(v)}$, а равенство $\operatorname{Ker}\pi^{(v)} = \underline{F}^{(v)}$ доказывается следующим образом. Многообразие, определяемое уравнением $\pi(x) = e$, должно иметь гладкую редукцию для почти всех v, и тогда по лемме Гензеля все точки из $\operatorname{Ker}\pi^{(v)}$ должны получаться редукцией точек из $\operatorname{Ker}\pi = F$; поэтому $[\operatorname{Ker}\pi^{(v)}] \leqslant [F]$. С другой стороны, для почти всех v $[\underline{F}^{(v)}] = [F]$ и $\underline{F}^{(v)} \subset \operatorname{Ker}\pi^{(v)}$, так что окончательно $\operatorname{Ker}\pi^{(v)} = \underline{F}^{(v)}$. В случае связной группы F утверждение леммы непосредственно вытекает из предложения 3.22.

Предположим теперь, что для точной последовательности (7) выполнены условия 1), 2). Тогда, рассматривая естественное действие группы $\operatorname{Gal}(K_v^{\text{нр}}/K_v)$ на группах, входящих в соответствующую точную последовательность (8), и переходя к когомологиям, мы получим точную последовательность

$$G_{\sigma_v} \xrightarrow{\pi} H_{\sigma_v} \xrightarrow{\psi_{\sigma_v}} H^1\left(K_v^{\text{нр}}/K_v,\ F_{\sigma_{K_v^{\text{нр}}}}\right) \to H^1\left(K_v^{\text{нр}}/K_v,\ G_{\sigma_{K_v^{\text{нр}}}}\right) = 1, \quad (9)$$

где ψ_{σ_v} — кограничное отображение.

Пусть теперь группа F конечна. Тогда в силу связности G, группа F центральна, причем для почти всех v справедливо включение $F \subset G_{\sigma_{K_v^{\text{нр}}}}$. С другой стороны, кограничное отображение ψ_{σ_v}, которое вследствие центральности F оказывается гомоморфизмом, совпадает с ограничением на G_{σ_v} кограничного морфизма ψ_{K_v}: $H_{K_v} \to H^1(K_v, F)$, который получается из точной последовательности $1 \to F \to G \to H \to 1$ путем перехода к обычным когомологиям Галуа. Отождествляя группу неразветвленных когомологий $H^1(K_v^{\text{нр}}/K_v, F)$ с подгруппой в $H^1(K_v, F)$ при помощи отображения инфляции, мы приходим к следующему утверждению.

Предложение 4. *Пусть π: $G \to H$ — изогения связных групп над полем алгебраических чисел K, $F = \operatorname{Ker}\pi$. Тогда для почти*

всех $v \in V_f^K$ *имеем* $\psi_{K_v}(H_{\mathcal{O}_v}) = H^1(K_v^{\text{нр}}/K_v, F)$, *где* $\psi_{K_v}\colon H_{K_v} \to H^1(K_v, F)$ — *кограничный морфизм, отвечающий точной последовательности* $1 \to F \to G \to H \to 1$. *Следовательно, для почти всех* v *порядки групп* $\psi_{K_v}(H_{\mathcal{O}_v})$ *и* F_{K_v} *совпадают. При этом если* $F \subset G_{K_v}$, *то* $\psi_{K_v}(H_{\mathcal{O}_v}) \simeq F$.

Первое утверждение предложения уже было доказано. Второе непосредственно вытекает из первого и леммы 3. Наконец, для доказательства третьего достаточно заметить, что в случае $F \subset G_{K_v}$ имеем $H^1(K_v^{\text{нр}}/K_v, F) = \operatorname{Hom}(\hat{\mathbb{Z}}, F) \simeq F$.

Рассмотрим теперь случай связной группы F. Тогда $H^1\left(K_v^{\text{нр}}/K_v, F_{\mathcal{O}_{K_v^{\text{нр}}}}\right) = 1$ для почти всех v, и поэтому из (9) имеем $\pi(G_{\mathcal{O}_v}) = H_{\mathcal{O}_v}$. Вспоминая определение адельной топологии и используя следствие 1 из предложения 3.3, мы получаем

Предложение 5. *Пусть* $\pi\colon G \to H$ — *сюръективный морфизм связных алгебраических групп над полем алгебраических чисел* K. *Предположим, что ядро* $\operatorname{Ker}\pi$ *связно. Тогда для почти всех* v $\pi(G_{\mathcal{O}_v}) = H_{\mathcal{O}_v}$, *и поэтому соответствующее адельное отображение* $\pi_A\colon G_A \to H_A$ *является открытым.*

Перейдем теперь к когомологиям групп аделей. Пусть G — алгебраическая группа, определенная над числовым полем K. Для любого конечного расширения Галуа L/K рассмотрим кольцо A_L аделей поля L. Известно (см. § 1.2, п. 3), что A_L можно отождествить с тензорным произведением $A_K \otimes L$, и тем самым определить на A_L действие группы Галуа $\operatorname{Gal}(L/K)$. Интерпретируя группу аделей G_{A_L} как группу точек G над кольцом A_L и учитывая K-определенность G, мы получаем действие $\operatorname{Gal}(L/K)$ на G_{A_L}. Тем самым определено множество первых когомологий $H^1(L/K, G_{A_L})$. Для произвольного расширения Галуа L/K адельные когомологии можно определить двумя эквивалентными способами: либо как индуктивный предел $\varinjlim H^1(P/K, G_{A_P})$ по всем конечным подрасширениям Галуа P/K, содержащимся в L, либо как множество непрерывных первых когомологий проконечной группы $\operatorname{Gal}(L/K)$ с коэффициентами в (дискретной) группе G_{A_L}. При этом последняя группа опять-таки допускает двоякое описание: либо как индуктивный предел (объединение) адельных групп G_{A_P} по всем конечным подрасширениям $P \subset L$ относительно естественных вложений $G_{A_{P_1}} \subset G_{A_{P_2}}$ при $P_1 \subset P_2$, либо как группа точек G над кольцом $A_L = A_K \otimes_K L$ (при этом кольцо $A_{\bar{K}}$ обозначается через $\bar{A}$). Мы не будем подробно рассматривать формализм адельных когомологий (см.

Коттвиц [1], [2], ибо в этой книге он нам фактически не понадобится. Основные факты здесь выглядят следующим образом. Любой точной последовательности $1 \to F \to G \to H \to 1$ связных K-групп и K-гомоморфизмов отвечает точная последовательность $1 \to F_{\overline{A}} \to G_{\overline{A}} \to H_{\overline{A}} \to 1$ (это легко вытекает из предложения 5), и можно рассматривать соответствующие производные когомологические последовательности. (Отметим, что в случае несвязной, в частности, конечной группы F последовательность $1 \to F_{\overline{A}} \to G_{\overline{A}} \to H_{\overline{A}} \to 1$ точной, вообще говоря, не является.) При этом адельные когомологии связной группы G описываются следующим образом.

Предложение 6. *Пусть G — связная группа над числовым полем K, L — его конечное расширение Галуа. Тогда множество $H^1(L/K, G_{A_L})$ можно отождествить с подмножеством X прямого произведения $\prod_v H^1(L_w/K_v, G)$ *), состоящим из таких $x = (x_v)$, что x_v тривиален в $H^1(L_w/K_v, G)$ для почти всех $v \in V^K$.*

(Подражая терминологии из теории групп, можно сказать, что $H^1(L/K, G_{A_L})$ является *прямой суммой* множеств $H^1(L_w/K_v, G)$. Заметим, что в случае коммутативной группы G мы действительно имеем обычную прямую сумму групп.)

Доказательство. Для каждого подмножества $S \subset V^K$ обозначим через $\overline{S}$ совокупность всех продолжений нормирований из S на L. Тогда $G_{A_L} = \bigcup_S G_{A_L(\overline{S})}$, где объединение групп $\overline{S}$-целых аделей $G_{A_L(\overline{S})}$ берется по всем конечным подмножествам $S \subset V^K$, содержащим V^K_∞, и поэтому

$$H^1(L/K, G_{A_L}) = \bigcup_S H^1(L/K, G_{A_L(\overline{S})}).$$

Мы покажем, что для любого S справедливо включение $H^1(L/K, G_{A_L(\overline{S})}) \subset X$. Без ограничения общности можно рассматривать лишь такие S, что для $v \notin S$ существует гладкая редукция $\underline{G}^{(v)}$ и расширение L_w/K_v неразветвлено. Из разложения $G_{A_L(\overline{S})} = G_{\overline{S}} \times \prod_{w \notin \overline{S}} G_{\mathcal{O}_w}$ получаем, что

$$H^1(L/K, G_{A_L(\overline{S})}) = \prod_{v \in S} H^1\Big(L/K, \prod_{w|v} G_{L_w}\Big) \times \prod_{v \notin S} H^1\Big(L/K, \prod_{w|v} G_{\mathcal{O}_w}\Big).$$

Но из леммы 1.4 вытекает, что для $v \in S$ (соответственно, $v \notin S$) группа $\prod_{w|v} G_{L_w}$ (соответственно, $\prod_{w|v} G_{\mathcal{O}_w}$) является индуцированной с G_{L_w} (соответственно, $G_{\mathcal{O}_w}$) для некоторого фиксированного продолжения $w|v$. Кроме того, по построению для

*) Произведение берется по всем $v \in V^K$, причем для каждого v выбирается одно продолжение $w \in V^L$.

$v \notin S$ выполнены условия теоремы 8, так что $H^1(L_w/K_v, G_{\mathcal{O}_w}) = 1$. Окончательно получаем, что

$$H^1\left(L/K, G_{A_L(\bar{S})}\right) = \prod_{v \in S} H^1(L_w/K_v, G) \times \{1\}.$$

Переходя к объединению, мы получаем включение $H^1(L/K, G_{A_L}) \subset X$. Обратное включение очевидно.

Следствие 5. *Множество $H^1(K, G_{\bar{A}})$ можно отождествить с подмножеством прямого произведения $\prod_v H^1(K_v, G)$, состоящим из таких $x = (x_v)$, что x_v тривиален в $H^1(K_v, G)$ для почти всех $v \in V^K$.*

Если группа G коммутативна, то определены все группы когомологий $H^i(L/K, G_{A_L})$ $(i \geqslant 0)$. Оказывается, что они допускают описание, аналогичное предложению 6.

Предложение 7. *Пусть G — коммутативная алгебраическая группа над числовым полем K, L — его конечное расширение Галуа. Тогда для любого $i \geqslant 1$*

$$H^i(L/K, G_{A_L}) \simeq \sum_v H^i(L_w/K_v, G).$$

Доказательство. Как видно из доказательства предложения 6, достаточно установить, что $H^i(L_w/K_v, G_{\mathcal{O}_w}) = 1$ для почти всех v. Мы можем ограничиться рассмотрением тех v, для которых расширение L_w/K_v неразветвлено. Тогда группа Галуа $\mathrm{Gal}(L_w/K_v)$ циклична, и в силу периодичности когомологий циклических групп мы получаем изоморфизмы

$$H^i(L_w/K_v, G_{\mathcal{O}_w}) \simeq H^1(L_w/K_v, G_{\mathcal{O}_w}) \quad \text{для нечетных } i,$$
$$H^i(L_w/K_v, G_{\mathcal{O}_w}) \simeq H^2(L_w/K_v, G_{\mathcal{O}_w}) \quad \text{для четных } i.$$

Из этих изоморфизмов и теоремы 8 мы получаем тривиальность i-х неразветвленных когомологий групп целых w-адических точек любой связной коммутативной группы для нечетных i, причем для доказательства предложения достаточно установить тривиальность $H^2(L_w/K_v, G_{\mathcal{O}_w})$. Для этого мы воспользуемся конструкцией, с которой еще не раз встретимся в дальнейшем. Положим $H = \mathbf{R}_{L/K}(G)$ и рассмотрим «норменное» отображение φ: $H \to G$, которое является композицией изоморфизма (4) в § 2.1 (отметим, что в силу K-определенности G имеем $G^\sigma = G$ для любого $\sigma \in \mathcal{G} = \mathrm{Gal}(L/K)$) и морфизма-произведения (легко видеть, что ограничение φ на $H_K \simeq G_L$ совпадает с обычным норменным отображением $N_{L/K}(g) = \prod_{\sigma \in \mathcal{G}} \sigma(g)$). Морфизм φ определен над K, и его ядро $F = \mathrm{Ker}\,\varphi$ является связной

K-определенной группой. Тем самым имеем точную последовательность связных K-групп:

$$1 \to F \to G \to H \to 1.$$

Из предложения 5 вытекает, что для почти всех $v \in V_f^K$ и соответствующих $w|v$ точна последовательность

$$1 \to F_{\mathcal{O}_w} \to H_{\mathcal{O}_w} \to G_{\mathcal{O}_w} \to 1. \tag{10}$$

Переходя в (10) к когомологиям, получим точную последовательность

$$\ldots \to H^2(L_w/K_v, H_{\mathcal{O}_w}) \to H^2(L_w/K_v, G_{\mathcal{O}_w}) \to H^3(L_w/K_v, F_{\mathcal{O}_w}). \tag{11}$$

Из сказанного выше вытекает, что последний член в (11) тривиален для почти всех v, и поэтому достаточно установить тривиальность $H^2(L_w/K_v, H_{\mathcal{O}_w})$. Но это является следствием того факта, что в силу наших построений $\mathrm{Gal}(L_w/K_v)$-модуль $H_{\mathcal{O}_w}$ является индуцированным. Предложение 7 доказано.

Диагональное вложение $L \to A_L$ согласовано с действием группы Галуа $\mathrm{Gal}(L/K)$, поэтому для любой алгебраической K-группы G имеем отображение когомологий $H^1(L/K, G) \to H^1(L/K, G_{A_L})$. Тогда из описания адельных когомологий мы получаем

Следствие 6. *Пусть G — связная алгебраическая K-группа, L/K — конечное расширение Галуа. Тогда произвольный коцикл $x \in H^1(L/K, G)$ имеет тривиальные образы в $H^1(L_w/K_v, G)$ для почти всех $v \in V_f^K$. В частности, любой коцикл $x \in H^1(K, G)$ имеет тривиальные образы в $H^1(K_v, G)$ для почти всех $v \in V_f^K$.*

Отметим, что если группа G коммутативна, то аналогичное утверждение имеет место для всех групп когомологий.

Упражнение. На примерах показать, что условие связности группы G в утверждении следствия 6 существенно.

§ 6.3. Когомологии Галуа алгебраических торов

Как мы уже отмечали в § 6.1, при работе с алгебраическими торами вместо обычных когомологий удобно использовать модифицированные когомологии (когомологии Тейта). Напомним их определение и основные свойства (систематическое изложение этих вопросов читатель может найти в книге Брауна [1], гл. VI или в [АТЧ], гл. IV). Итак пусть G — конечная группа, A — некоторый G-модуль. Введем «норменное» отображение $N\colon A \to A$, задав его формулой $N(a) = \sum_{g \in G} ga$. Ясно, что $N(A) \subset \subset A^G$ и $A' \subset \mathrm{Ker}\, N$, где A' — подмодуль в A, порожденный элементами вида $ga - a$ для всех $g \in G$, $a \in A$. Тогда группы

когомологий Тейта $\hat{H}^i(G, A)$ определяются следующим образом:

$$\hat{H}^i(G, A) = H^i(G, A), \quad \text{если} \quad i \geqslant 1,$$
$$\hat{H}^0(G, A) = A^G/N(A),$$
$$\hat{H}^{-1}(G, A) = \operatorname{Ker} N/A',$$
$$\hat{H}^{-i}(G, A) = H_{i-1}(G, A), \quad \text{если} \quad i \geqslant 2,$$

где H_i обозначает i-ю группу гомологий. Доказывается, что модифицированные когомологии сохраняют все основные свойства обычных когомологий, а именно: 1) для них выполняется лемма Шапиро, и, в частности, когомологии индуцированного модуля тривиальны; 2) любой точной последовательности G-модулей $0 \to A \to B \to C \to 0$ отвечает бесконечная в обе стороны точная последовательность

$$\ldots \to \hat{H}^i(G, A) \to \hat{H}^i(G, B) \to \hat{H}^i(G, C) \to \hat{H}^{i+1}(G, A) \to \ldots$$

Преимущества, которые мы получаем, перейдя от обычных когомологий к модифицированным, заключаются в том, что для последних имеет место очень полезная в нашей ситуации теорема Тейта (см. ниже теорему 9).

После этих предварительных замечаний мы переходим непосредственно к доказательству теорем Накаямы — Тейта.

Начнем с рассмотрения частного случая $T = \boldsymbol{G}_m$. Этот случай, тривиальный с точки зрения теории торов, вбирает в себя наиболее содержательную часть рассуждений, ибо указанные в теоремах 2, 3 изоморфизмы для $i = 0, 1, 2$ представляют основные результаты соответственно локальной и глобальной теорий полей классов. После этого переход к случаю произвольных торов осуществляется уже сравнительно легко при помощи теоремы Тейта. Разберем вначале случай локального поля K. При $i = 0$ мы должны получить изоморфизм $\hat{H}^0(L/K, \mathbb{Z}) \simeq \hat{H}^2(L/K, L^*)$, ибо здесь $\mathbf{X}(T) = \mathbb{Z}$ с тривиальным действием $\mathcal{G} = \operatorname{Gal}(L/K)$. Но, очевидно, $\hat{H}^0(L/K, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$, где $n = [L:K]$, а $\hat{H}^2(L/K, L^*) \simeq \operatorname{Br}(L/K) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}$, причем последний изоморфизм осуществляется отображением inv (см. теорему 1.7). Прообраз элемента $1/n$ при этом изоморфизме называется *фундаментальным классом* расширения L/K и обозначается $u_{L/K}$. Если F — некоторое промежуточное подполе, то $u_{L/F}$ является образом $u_{L/K}$ при отображении ограничения $\hat{H}^2(L/K, L^*) \to \hat{H}^2(L/F, L^*)$. Далее, при $i = 1$ обе группы $\hat{H}^1(L/K, \mathbb{Z})$ и $\hat{H}^1(L/K, L^*)$ тривиальны. Наконец, разберем случай $i = 2$. Здесь $\hat{H}^2(L/K, \mathbb{Z}) \simeq H^1(L/K, \mathbb{Q}/\mathbb{Z})$ (см. лемму 1.3), а последняя группа совпадает с абелинизацией $\mathcal{G}$. С другой стороны, $\hat{H}^0(L/K, L^*) = K^*/N_{L/K}(L^*)$. Таким образом, здесь

изоморфизм в теореме 2 принимает вид $\mathcal{G}^{ab} \simeq K^*/N_{L/K}(L^*)$, в частности $\mathcal{G} \simeq K^*/N_{L/K}(L^*)$, если группа $\mathcal{G}$ абелева. Последний факт, дополненный теоремой существования (любая открытая подгруппа в K^* конечного индекса является норменной, т. е. имеет вид $N_{L/K}(L^*)$ для подходящего абелева расширения L/K), является главным достижением локальной теории полей классов (см. лекцию Серра в [АТЧ]). Отметим, что хотя основным объектом локальной теории полей классов являются неархимедовы локальные поля, ее результаты формально остаются справедливыми и в архимедовом случае, т. е. когда K есть $\mathbb{R}$ или $\mathbb{C}$.

Сходные результаты имеют место и в глобальном случае, однако используемые объекты и доказательство основных утверждений имеют более сложную природу, в частности, мультипликативная группа L^* заменяется здесь на группу классов иделей $C_L = J_L/L^*$. Опять для $i=0$ имеем $H^2(L/K, C_L) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}$, где $n = [L:K]$ (изоморфизм строится, исходя из локальных отображений inv, см. [АТЧ], гл. VII, § 11), так что утверждение теоремы 3 для $i=0$ здесь выполняется. Прообраз $u_{L/K}$ элемента $1/n$ при этом изоморфизме, как и в локальном случае, называется *фундаментальным классом* расширения L/K. Он также обладает тем свойством, что для любого промежуточного подполя F фундаментальный класс $u_{L/F}$ является ограничением $u_{L/K}$. При $i=1$ группа $Ha(L/K, C_L)$ тривиальна, так что теорема 3 здесь выполняется. (Отметим, что тривиальность $H^1(L/K, C_L)$ имеет ряд важных арифметических следствий. В частности, переходя в точной последовательности $1 \to L^* \to J_L \to C_L \to 1$ к когомологиям, получим, что отображение $\mathrm{Br}(L/K) = H^2(L/K, L^*) \to H^2(L/K, J_L) = \sum_v \mathrm{Br}(L_w/K_v)$ является инъективным, что равносильно теореме Хассе — Брауэра — Нётер из § 1.5.) Наконец, при $i=2$ мы должны получить изоморфизм $\mathcal{G}^{ab} \simeq C_K/N_{L/K}(C_L)$, а это есть основной изоморфизм глобальной теории полей классов (см. лекцию Тейта в [АТЧ]).

Нельзя не отметить аналогии в основных результатах локальной и глобальной теорий; она находит свое формальное выражение в аксиоматическом описании так называемых *формаций классов* (см. Серр [3]).

Теперь у нас есть все необходимое, чтобы завершить доказательство теорем 2, 3 в общем случае. Оно основывается на следующем утверждении.

Теорема 9 (Тейт [1]). *Пусть G — конечная группа, M — некоторый G-модуль и u — элемент из $H^2(G, M)$. Для каждого простого p обозначим через G_p силовскую p-подгруппу в G и предположим, что выполнены следующие условия:*

1) $H^1(G_p, M) = 1$;

2) *$H^2(G_p, M)$ является циклической группой с образующей $\mathrm{Res}^G_{G_p}(u)$, где $\mathrm{Res}^G_{G_p}(u)$: $H^2(G, M) \to H^2(G_p, M)$ — морфизм ограничения, и порядком, равным порядку G_p. Тогда для любого конечно порожденного G-модуля N без кручения и любой подгруппы $\mathscr{H} \subset \mathscr{G}$ $\cup$-умножение на u индуцирует изоморфизм $\hat{H}^i(\mathscr{H}, N) \to \hat{H}^{i+2}(\mathscr{H}, M \otimes N)$ для любого целого i.*

(Определение $\cup$-умножения и доказательство теоремы 9 читатель может найти в [АТЧ], гл. IV, § 10. В дальнейшем эти факты нам не понадобятся.)

Для того чтобы воспользоваться теоремой 9, для данного K-тора T, разложимого над конечным расширением Галуа L/K с группой Галуа $\mathscr{G} = \mathrm{Gal}(L/K)$, рассмотрим группу кохарактеров (однопараметрических подгрупп) $\mathbf{X}_*(T) = \mathrm{Hom}(\boldsymbol{G}_m, T)$, которая также является $\mathscr{G}$-модулем (см. § 2.1, п. 7). Оказывается, что зная группу $\mathbf{X}_*(T)$, легко восстановить группу L-точек T_L. А именно, рассмотрим гомоморфизм θ: $\mathbf{X}_*(T) \otimes L^* \to T_L$, определяемый соответствием $\theta(\varphi \otimes x) = \varphi(x)$. Группа $\mathscr{G}$ действует на $\mathbf{X}_*(T) \otimes L^*$ посредством действия на сомножителях, и без труда проверяется, что θ является $\mathscr{G}$-гомоморфизмом. С другой стороны, легко показать, что для разложимого тора θ является изоморфизмом абстрактных групп. Поэтому, учитывая, что над L тор T становится разложимым, мы приходим к следующему результату.

Лемма 7. *Построенный гомоморфизм θ: $\mathbf{X}_*(T) \otimes L^* \to T_L$ является изоморфизмом $\mathscr{G}$-модулей.*

Теперь уже совсем легко доказать локальную теорему Накаямы — Тейта. А именно, предположим, что K — локальное поле. Тогда из нашего обсуждения локальной теории полей классов вытекает, что для модуля $M = L^*$ и фундаментального класса $u_{L/K} \in H^2(L/K, L^*)$ выполняются условия теоремы Тейта. Поэтому, применяя ее с учетом леммы 6, получаем изоморфизмы

$$\hat{H}^i(L/K, \mathbf{X}_*(T)) \simeq \hat{H}^{i+2}(L/K, \mathbf{X}_*(T) \otimes L^*) \simeq \hat{H}^{i+2}(L/K, T_L). \qquad (1)$$

(Отметим, что этот изоморфизм индуцируется $\cup$-умножением на $u_{L/K}$ и поэтому обладает необходимыми функториальными свойствами.) С другой стороны, из теоремы двойственности для когомологий (см., например, Картан, Эйленберг [1]) получаем, что конечные абелевы группы $\hat{H}^i(L/K, \mathbf{X}_*(T))$ и $\hat{H}^{-i}(L/K, \mathbf{X}(T))$ являются двойственными друг другу и, следовательно, изоморфными для любого целого i. Из этого факта и цепочки изоморфизмов (1) вытекает утверждение теоремы 2. Отметим, что приведенное доказательство теоремы 2 проходит для всех

локальных полей, включая архимедовы, однако для случая $K = \mathbb{R}$ ее можно легко доказать непосредственно, используя классификацию вещественных торов (см. § 2.2, п. 4), что мы и предлагаем проделать читателю в качестве упражнения.

Следует указать на то обстоятельство, что построенный в доказательстве теоремы 2 изоморфизм имеет характер изоморфизма конечной абелевой группы со своей двойственной. Эта двойственность может быть описана и непосредственно, без использования группы $\mathbf{X}_*(T)$. А именно, $\smile$-умножение индуцирует спаривание $\hat{H}^i(L/K, T) \times \hat{H}^{2-i}(L/K, \mathbf{X}(T)) \to \hat{H}^2(L/K, T_L \otimes \otimes_{\mathbf{Z}} \mathbf{X}(T))$, а последняя группа отображается в $\hat{H}^2(L/K, L^*) \simeq \simeq \mathbf{Z}/n\mathbf{Z}$, где $n = [L:K]$, посредством отображения $T_L \otimes_{\mathbf{Z}} \mathbf{X}(T) \to \to L^*$, $t \otimes \chi \mapsto \chi(t)$. Получающееся в итоге спаривание $\hat{H}^i(L/K, T) \times H^{2-i}(L/K, \mathbf{X}(T)) \to \mathbf{Z}/n\mathbf{Z}$ оказывается невырожденным и тем самым доставляет изоморфизм в теореме 2.

Доказательство теоремы 3 формально совпадает с доказательством теоремы 2, с той разницей, что для глобального поля K используется модуль $M = C_L$. Тот факт, что для M и соответствующего фундаментального класса $u_{L/K} \in H^2(L/K, M)$ выполняются условия теоремы Накаямы — Тейта, вытекает из глобальной теории полей классов. Мы предлагаем читателю в качестве упражнения показать, что $\mathcal{G}$-модули $\mathbf{X}_*(T) \otimes_{\mathbf{Z}} C_L$ и $C_L(T) = T_{A_L}/T_L$ изоморфны (имитировать доказательство леммы 7). Тогда

$$\hat{H}^i(L/K, \mathbf{X}_*(T)) \simeq \hat{H}^{i+2}(L/K, \mathbf{X}_*(T) \otimes_{\mathbf{Z}} C_L) \simeq \hat{H}^{i+2}(L/K, C_L(T)), \quad (2)$$

причем изоморфизм осуществляет $\smile$-умножение на $u_{L/K}$. Опять используя двойственность между группами $\hat{H}^i(L/K, \mathbf{X}_*(T))$ и $\hat{H}^{-i}(L/K, \mathbf{X}(T))$, мы и получаем теорему 3. Отметим, что здесь также имеется невырожденное спаривание между группами $\hat{H}^i(L/K, C_L(T))$ и $\hat{H}^{2-i}(L/K, \mathbf{X}(T))$, получаемое как сквозное отображение

$$\hat{H}^i(L/K, C_L(T)) \times \hat{H}^{2-i}(L/K, \mathbf{X}(T)) \to$$
$$\to \hat{H}^2(L/K, C_L(T) \otimes_{\mathbf{Z}} \mathbf{X}(T)) \to \hat{H}^2(L/K, C_L) \simeq \mathbf{Z}/n\mathbf{Z},$$

где $n = [L:K]$.

Следует сделать одно важное замечание. Так как изоморфизмы в теоремах 2, 3 имеют характер изоморфизма конечной абелевой группы со своей двойственной, то они не являются каноническими. Поэтому при исследовании функториальных свойств вместо изоморфизмов из теорем 2, 3 следует рассматривать изоморфизмы (1), (2), в которых участвуют когомологии группы $\mathbf{X}_*(T)$, ибо они индуцируются $\smile$-произведением и, сле-

довательно, являются естественными. При этом когомологии групп $\mathbf{X}_*(T)$ и $\mathbf{X}(T)$ связаны соотношениями двойственности. В качестве примера рассмотрим вопрос о связи локальных и глобальных изоморфизмов в теоремах Накаямы — Тейта. А именно, пусть K — числовое поле, $v \in V^K$, $T_{K_v \otimes_K L} \to T_{A_K \otimes_K L} = T_{A_L}$ — естественное вложение и τ: $\hat{H}^i(L/K, T_{K_v \otimes_K L}) \to \hat{H}^i(L/K, C_L(T))$ — отображение когомологий, индуцированное указанным вложением и проекцией $T_{A_L} \to C_L(T)$. Так как $K_v \otimes_K L \simeq \prod_{w|v} L_w$, причем различные продолжения сопряжены относительно группы $\mathcal{G}$, то $T_{K_v \otimes_K L} \simeq \prod_{w|v} T_{L_w}$ является индуцированной группой, и поэтому по лемме Шапиро $\hat{H}^i(L/K, T_{K_v \otimes_K L}) = \hat{H}^i(L_w/K_v, T)$. Но $\hat{H}^i(L/K, C_L(T)) \simeq \hat{H}^{2-i}(L/K, \mathbf{X}(T))$, $\hat{H}^i(L_w/K_v, T) \simeq \hat{H}^{2-i}(L_w/K_v, \mathbf{X}(T))$, так что естественно возникает соблазн описать отвечающее τ отображение $\hat{H}^{2-i}(L_w/K_v, \mathbf{X}(T)) \to \hat{H}^{2-i}(L/K, \mathbf{X}(T))$. Однако при такой постановке задача не допускает вполне определенного ответа, ибо указанные изоморфизмы нельзя определить канонически. Правильная постановка выглядит следующим образом: найти гомоморфизм σ: $\hat{H}^{i-2}(L_w/K_v, \mathbf{X}_*(T)) \to \hat{H}^{i-2}(L/K, \mathbf{X}(T))$, превращающий диаграмму

$$\begin{array}{ccc} \hat{H}^i(L_w/K_v, T) & \xrightarrow{\tau} & \hat{H}^i(L/K, C_L(T)) \\ \uparrow & & \uparrow \\ \hat{H}^{i-2}(L_w/K_v, \mathbf{X}_*(T)) & \xrightarrow{\sigma} & \hat{H}^{i-2}(L/K, \mathbf{X}_*(T)) \end{array} \tag{3}$$

в коммутативную (вертикальные стрелки являются изоморфизмами, получаемыми из (1), (2)).

Предложение 8. *Гомоморфизм σ является гомоморфизмом коограничения $\mathrm{Cor}^{\mathcal{G}}_{\mathcal{G}(w)}$, где $\mathcal{G}(w) = \mathrm{Gal}(L_w/K_v)$ — группа разложения нормирования w.*

Доказательство начнем с установления связи между локальным и глобальным фундаментальными классами. Положим $P = L^{\mathcal{G}(w)}$. Тогда из результатов [АТЧ], гл. VII, § 11, вытекает, что отображение $L_w \to C_L$ индуцирует изоморфизм $H^2(L_w/P_w, L_w) \simeq H^2(L/P, C_L)$ (отметим, что $P_w = K_v$); при этом локальный фундаментальный класс $u_{L_w/P_w} = u_{L_w/K_v}$ переходит в глобальный фундаментальный класс $u_{L/P}$, который, как мы знаем, совпадает с $\mathrm{Res}^{\mathcal{G}}_{\mathcal{G}(w)}(u_{L/K})$. Отсюда следует коммутативность

диаграмм

$$\begin{array}{ccc} \hat{H}^{i-2}(\mathcal{G}(w), \mathbf{X}_*(T)) & \to & \hat{H}^i(\mathcal{G}(w), T) \\ \| & & \downarrow \\ \hat{H}^{i-2}(\mathcal{G}(w), \mathbf{X}_*(T)) & \to & \hat{H}^i(\mathcal{G}(w), C_L(T)) \end{array}$$

и

$$\begin{array}{ccc} \hat{H}^{i-2}(\mathcal{G}(w), \mathbf{X}_*(T)) & \to & \hat{H}^i(\mathcal{G}(w), C_L(T)) \\ \downarrow{\scriptstyle \mathrm{Cor}^{\mathcal{G}}_{\mathcal{G}(w)}} & & \downarrow{\scriptstyle \mathrm{Cor}^{\mathcal{G}}_{\mathcal{G}(w)}} \\ \hat{H}^{i-2}(\mathcal{G}, \mathbf{X}_*(T)) & \to & \hat{H}^i(\mathcal{G}, C_L(T)) \end{array}$$

(доказательство коммутативности второй диаграммы использует следующее свойство $\smile$-произведения:

$$\mathrm{Cor}(\mathrm{Res}(x) \smile y) = x \smile \mathrm{Cor}(y), \tag{4}$$

справедливость которого установлена в [АТЧ], гл. IV, § 7). Сравнивая эти диаграммы и учитывая коммутативность диаграммы

$$\begin{array}{ccc} \hat{H}^i(\mathcal{G}(w), T) & \to & \hat{H}^i(\mathcal{G}(w), C_L(T)) \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle \mathrm{Cor}^{\mathcal{G}}_{\mathcal{G}(w)}} \\ \hat{H}^i\left(\mathcal{G}, \prod\limits_{w|v} T_{L_w}\right) & \to & \hat{H}^i(\mathcal{G}, C_L(T)), \end{array}$$

где i — изоморфизм из леммы Шапиро, приходим к требуемому утверждению. (Мы оставляем читателю в качестве упражнения восстановить детали рассуждений.)

Как мы уже отмечали в § 6.1, из теорем 2, 3 вытекает конечность группы $H^1(K, T)$ над локальным полем K и конечность ядра $Ш(T)$ канонического гомоморфизма $H^1(K, T) \to \prod\limits_{v \in V^K} H^1(K_v, T)$ для числового поля K. На самом деле эти утверждения сохраняют силу не только для первых, но и для любых когомологий.

Предложение 9. *Пусть T — алгебраический тор, определенный над полем K и разложимый над его конечным расширением Галуа L. Тогда для любого i выполняются утверждения:*

1) *группа $\hat{H}^i(L/K, T)$ конечна, если K — локальное поле;*

2) *группа* $P^i(L/K, T) = \mathrm{Ker}\left(\hat{H}^i(L/K, T) \to \prod\limits_v \hat{H}(L_w/K_v, T)\right)$ *конечна, если K — числовое поле.*

Доказательство легко вытекает из следующего замечания: для любого i группа $\hat{H}^i(L/K, \mathbf{X}(T))$ является конечно порожденной абелевой группой конечной экспоненты (см. [АТЧ], гл. IV, § 6) и поэтому конечна. Утверждение 1) является непосредственным следствием этого факта, если воспользоваться изоморфизмом из теоремы 2. Для доказательства 2) следует

рассмотреть точную последовательность $1 \to T_L \to T_{A_L} \to C_L(T) \to \to 1$ и следующий фрагмент соответствующей когомологической последовательности:

$$\hat{H}^{i-1}(L/K, T_{A_L}) \xrightarrow{g} \hat{H}^{i-1}(L/K, C_L(T)) \to$$
$$\to \hat{H}^i(L/K, T) \xrightarrow{f} \hat{H}^i(L/K, T_{A_L}). \quad (5)$$

Тогда $P^i(L/K, T) = \operatorname{Ker} f$ является факторгруппой группы $\hat{H}^{i-1}(L/K, C_L(T))$, а последняя группа согласно теореме 3 изоморфна $\hat{H}^{3-i}(L/K, \mathbf{X}(T))$ и, следовательно, конечна.

Следствие. *В условиях предложения 9 справедливы следующие утверждения:*

1) *группа $H^1(K, T)$ конечна, если K — локальное поле;*

2) *группа* $Ш(T) = \operatorname{Ker}\left(H^1(K, T) \to \prod_v H^1(K_v, T)\right)$ *конечна, если K — числовое поле.*

Доказательство вытекает из предложения 9 и следующего факта.

Лемма 8. *Если K-тор T разложим над расширением Галуа L/K, то $H^1(K, T) = H^1(L/K, T)$.*

Действительно, по теореме 90 Гильберта $H^1(L, T) = 1$, поэтому, записав начальный отрезок спектральной последовательности Хохшильда — Серра

$$1 \to H^1(L/K, T) \to H^1(K, T) \to H^1(L, T),$$

мы и получим требуемое.

Некоторое уточнение рассуждений, использованных при доказательстве предложения 9, позволяет получить точные формулы для вычисления группы $P^i(L/K, T)$. Действительно, из точной последовательности (5) вытекает, что $P^i(L/K, T) = \operatorname{Ker} f$ изоморфно коядру $\operatorname{Coker} g$. Но $\hat{H}^{i-1}(L/K, T_{A_L}) = \sum_v \hat{H}^{i-1}(L_w/K_v, T)$ (предложение 7), поэтому, используя изоморфизмы $\hat{H}^{i-1}(L/K, C_L(T)) \simeq \hat{H}^{i-3}(L/K, \mathbf{X}_*(T))$, $\hat{H}^{i-1}(L_w/K_v, T) \simeq \hat{H}^{i-3}(L_w/K_v, \mathbf{X}_*(T))$ и предложение 8, получаем, что $P^i(L/K, T)$ изоморфно коядру отображения

$$\sum_v \hat{H}^{i-3}(L_w/K_v, \mathbf{X}_*(T)) \to \hat{H}^{i-3}(L/K, \mathbf{X}_*(T)), \quad (6)$$

индуцированного коограничениями $\operatorname{Cor}^{\mathcal{G}}_{\mathcal{G}(w)}$. Переходя при помощи теоремы двойственности к когомологиям группы $\mathbf{X}(T)$ и учитывая, что при этом морфизм коограничения перейдет в морфизм ограничения, мы получаем следующий результат.

Теорема 10 (Тейт). $P^i(L/K, T) \simeq \operatorname{Ker}(H^{3-i}(L/K, \mathbf{X}(T)) \to \to \prod_v H^{3-i}(L_w/K_v, \mathbf{X}(T)))$.

(Отметим, что изоморфизм в теореме 10 не является каноническим, а индуцирован двойственностью.)

В приложениях наиболее часто встречается группа $Ш(T) = P^1(L/K, T)$, называемая *группой Шафаревича — Тейта* тора T. Говорят, что для тора T выполняется *принцип Хассе*, если $Ш(T) = 1$. Покажем, что здесь мы имеем дело с естественным обобщением классического норменного принципа Хассе в расширениях числовых полей. Пусть P — конечное расширение числового поля K, $S = \mathbf{R}_{P/K}(\boldsymbol{G}_m)$ и $T = \mathbf{R}^{(1)}_{P/K}(\boldsymbol{G}_m)$ — соответствующий норменный тор. Тогда из точной последовательности

$$1 \to T \to S \xrightarrow{N} \boldsymbol{G}_m \to 1, \tag{7}$$

где N — норменное отображение, переходя к когомологиям, получим точную последовательность

$$P^* \xrightarrow{N_{P/K}} K^* \to H^1(K, T) \to H^1(K, S).$$

Но $H^1(K, S) = 1$ (лемма 2.4), поэтому $H^1(K, T) \simeq K^*/N_{P/K}(P^*)$. Рассуждая аналогично, получим, что $H^1(K, T_{\overline{A}}) \simeq J_K/N_{P/K}(J_P)$. Отсюда следует, что $Ш(T) \simeq (K^* \cap N_{P/K}(J_P))/N_{P/K}(P^*)$. Сопоставляя этот факт с классическим определением выполнимости норменного принципа Хассе в расширении P/K (см. § 1.2, п. 3), мы видим, что в данном случае последний эквивалентен справедливости принципа Хассе для когомологий Галуа соответствующего норменного тора $T = \mathbf{R}^{(1)}_{P/K}(\boldsymbol{G}_m)$. Тем самым теорема 10 дает эффективный способ проверки норменного принципа Хассе. Соответствующие вычисления приобретают наиболее простой вид, когда P/K — расширение Галуа. В этом случае в качестве поля разложения L тора $T = \mathbf{R}^{(1)}_{P/K}(\boldsymbol{G}_m)$ можно взять само поле P. Обозначим через $\mathcal{G}$ группу Галуа $\mathrm{Gal}(P/K)$. Тогда модуль характеров $\mathbf{X}(T)$ определяется из точной последовательности

$$0 \to \mathbb{Z} \to \mathbb{Z}[\mathcal{G}] \to \mathbf{X}(T) \to 0, \tag{8}$$

которая получается из последовательности (7). Переходя в (8) к когомологиям, мы придем к последовательности

$$H^2(\mathcal{G}, \mathbb{Z}[\mathcal{G}]) \to H^2(\mathcal{G}, \mathbf{X}(T)) \to H^3(\mathcal{G}, \mathbb{Z}) \to H^3(\mathcal{G}, \mathbb{Z}[\mathcal{G}]).$$

Но групповое кольцо $\mathbb{Z}[\mathcal{G}]$ является индуцированным $\mathcal{G}$-модулем, так что $H^i(\mathcal{G}, \mathbb{Z}[\mathcal{G}]) = 0$ для $i = 2, 3$, и поэтому $H^2(\mathcal{G}, \mathbf{X}(T)) = H^3(\mathcal{G}, \mathbb{Z})$. Аналогично, зафиксировав для каждого v некоторое продолжение $w|v$ и обозначив через $\mathcal{G}_v$ соответствующую группу разложения $\mathcal{G}(w)$, будем иметь $H^2(\mathcal{G}_v, \mathbf{X}(T)) = H^3(\mathcal{G}_v, \mathbb{Z})$. Таким образом, применяя теорему 10, получаем следующее утверждение:

Теорема 11 (Тейт). *Для норменного тора $T = \mathbf{R}^{(1)}_{P/K}(\mathbf{G}_m)$, отвечающего расширению Галуа P/K, группа $Ш(T)$ изоморфна ядру канонического отображения*

$$H^3(\mathcal{G}, Z) \to \prod_v H^3(\mathcal{G}_v, Z). \tag{9}$$

В частности, для P/K выполняется норменный принцип Хассе в том и только том случае, если отображение (9) *инъективно.*

Если группа $\mathcal{G}$ циклична, то $H^3(\mathcal{G}, Z) = H^1(\mathcal{G}, Z) = 0$, и мы приходим к следующему результату Хассе [2].

Следствие (теорема Хассе о нормах). *Для циклического расширения P/K всегда выполняется норменный локально-глобальный принцип.*

Если же расширение P/K не является циклическим, то возможны разные случаи.

Пример 1. Положим $K = \mathbb{Q}$, $P = \mathbb{Q}(\sqrt{13}, \sqrt{17})$. Здесь $\mathcal{G} = Z/2Z \times Z/2Z$, а все группы $\mathcal{G}_v$ циклические. Поэтому $H^3(\mathcal{G}, Z) = Z/2Z$, но $H^3(\mathcal{G}_v, Z) = 0$ для любого v. Тогда $Ш(T) = Z/2Z$, и норменный принцип для P/K не выполняется, что согласуется со сказанным в п. 3 § 1.2.

Пример 2. Положим $K = \mathbb{Q}$, $P = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. Тогда $\mathcal{G} = \mathcal{G}_2 = Z/2Z \times Z/2Z$, так что (9) инъективно, и для P/K выполняется принцип Хассе.

Если вопрос о норменном принципе Хассе для расширений Галуа теоретически решается теоремой 11, то для расширений, не являющихся нормальными, до недавнего времени существовало очень мало результатов. Конечно, в данной ситуации к возникающему здесь норменному тору также применимы, с одной стороны, теорема 10 (соответствующие вычисления см. ниже), с другой — общие методы, связанные с изучением геометрии алгебраических торов (см. Воскресенский [3], а также конец § 7.3). Однако при этом остается определенное чувство неудовлетворенности, вызванное тем обстоятельством, что арифметическая по своей природе задача о норменном принципе Хассе имеет ответ в чисто гомологической форме, которая, фактически, никак не учитывает арифметику самого расширения. Комплексное исследование норменного принципа Хассе для произвольных расширений, сочетающее как гомологические, так и арифметические методы, было недавно выполнено в работах Платонова, Дракохруста [1], [2], Дракохруста, Платонова [1] и Дракохруста [1]. Отправным пунктом для этого исследования послужила следующая проблема Бартельса [3, с. 198]: будет ли верен принцип Хассе для расширения L/K, если L — максимальное подполе в некотором теле D с центром K. Такие расширения называются *K-адекватными* (Шахер [1]). Эта гипотеза казалась весьма правдоподобной. Так, любое расширение простой

степени K-адекватно, и для него выполняется принцип Хассе (см. предложение 10 ниже). Гурак [2] доказал предположение Бартельса для расширений Галуа (этот результат можно рассматривать как арифметическую интерпретацию критерия из теоремы 11). Сам Бартельс [4] установил справедливость принципа Хассе для K-адекватных расширений степени 4 (как показывает пример 1, для произвольного расширения четвертой степени принцип Хассе может нарушаться). Кроме того, норменный локально-глобальный принцип выполняется для всего тела D, содержащего L (теорема Эйхлера, см. § 1.4).

Тем не менее оказалось, что в общем случае проблема Бартельса имеет отрицательное решение. Первый контрпример, построенный в работе Платонова, Дракохруста [1], является расширением степени 10. Естественно возник вопрос о минимальности этого примера, а также об арифметической природе тех значений степени расширения, при которых гипотеза Бартельса выполняется (так как 10 является произведением двух различных простых чисел, а для расширений простой степени принцип Хассе выполняется всегда, то можно предположить, что гипотеза Бартельса справедлива для расширений примарной степени). Детальному исследованию этих вопросов посвящена работа Дракохруста, Платонова [1]. В ней, в частности, показано, что проблема Бартельса справедлива для расширений L/K степени p^2 (p простое), в то же время при $[L:K]=p^r$, $r\geqslant 3$, ответ на проблему Бартельса отрицательный. Оказалось также, что она справедлива для расширений степени 6. Поэтому минимальные контрпримеры доставляют расширения восьмой степени.

Исследование принципа Хассе в цитированных работах базируется на введенном там понятии *первого препятствия*. В нашем контексте эта конструкция получается следующим образом. Пусть P/K — конечное расширение. Тогда в качестве поля разложения норменного тора $T=\mathbf{R}^{(1)}_{P/K}(\boldsymbol{G}_m)$ можно взять любое расширение Галуа L поля K, содержащее P. Обозначим через $\mathscr{G}$ группу Галуа $\mathrm{Gal}(L/K)$, и пусть $\mathscr{H}$ — подгруппа в $\mathscr{G}$, отвечающая P. Переходя в последовательности (7) к характерам, получим следующую точную последовательность, содержащую $\mathbf{X}(T)$:

$$0\to\mathbf{Z}\to\mathbf{Z}[\mathscr{G}/\mathscr{H}]\to\mathbf{X}(T)\to 0. \tag{10}$$

Чтобы вычислить $Ш(T)$ с помощью теоремы 10, рассмотрим получающуюся из (10) коммутативную диаграмму

$$\begin{tikzcd}
H^2(\mathscr{G},\mathbf{Z}) \arrow[r, "\varphi_1"] \arrow[d, "\alpha_1"] & H^2(\mathscr{G},\mathbf{Z}[\mathscr{G}/\mathscr{H}]) \arrow[r, "\varphi_2"] \arrow[d, "\alpha_2"] & {} \\
\prod\limits_v H^2(\mathscr{G}_v,\mathbf{Z}) \arrow[r, "\psi_1"] & \prod\limits_v H^2(\mathscr{G}_v,\mathbf{Z}[\mathscr{G}/H]) \arrow[r, "\psi_2"] & {}
\end{tikzcd}$$

$$\begin{array}{ccccc} \xrightarrow{\Phi_2} H^2(\mathcal{G}, \mathbf{X}(T)) & \xrightarrow{\Phi_3} & H^3(\mathcal{G}, Z) & \xrightarrow{\Phi_4} & H^3(\mathcal{G}, Z[\mathcal{G}/\mathcal{H}]) \\ \downarrow \alpha_2 & & \downarrow \alpha_4 & & \downarrow \alpha_5 \\ \xrightarrow{\Psi_2} \prod_v H^2(\mathcal{G}_v, \mathbf{X}(T)) & \xrightarrow{\Psi_3} & \prod_v H^3(\mathcal{G}_v, Z) & \xrightarrow{\Psi_4} & \prod_v H^3(\mathcal{G}_v, Z[\mathcal{G}/\mathcal{H}]) \end{array} \tag{11}$$

Согласно теореме 10, $Ш(T) = P^1(L/K, T) \simeq \operatorname{Ker} \alpha_3$. Из диаграммы (11) тогда вытекает, что существует вложение группы $\Phi = \alpha_2^{-1}(\operatorname{Im} \psi_1)/\operatorname{Im} \varphi_1$ в $Ш(T)$. Группа Φ изоморфна *первому препятствию* к принципу Хассе, которое было определено в работе Платонова, Дракохруста [1] в арифметических терминах как факторгруппа $K^* \cap N_{P/K}(J_P)/N_{P/K}(P^*) \cdot (K^* \cap N_{L/K}(J_L))$. В цитированной статье указан способ вычисления первого препятствия, который можно получить также из диаграммы (11). Для этого заметим, что $Z[\mathcal{G}/\mathcal{H}] = \operatorname{Ind}_{\mathcal{H}}^{\mathcal{G}}(Z)$, и поэтому по лемме Шапиро $H^2(\mathcal{G}, Z[\mathcal{G}/\mathcal{H}]) = H^2(\mathcal{H}, Z)$. Аналогично, для каждого v $Z[\mathcal{G}/\mathcal{H}] = \sum_{i=1}^{r_v} Z[\mathcal{K}_i^v/\mathcal{H}]$ — прямая сумма $\mathcal{G}_v$ модулей, где $\mathcal{K}_i^v = \mathcal{G}_v x_i^v \mathcal{H}$ $(i = 1, \ldots, r_v)$ — различные двойные смежные классы в разложении группы $\mathcal{G}$ по подгруппам $\mathcal{G}_v$ и $\mathcal{H}$. При этом, очевидно, $Z[\mathcal{K}_i^v/\mathcal{H}] = \operatorname{Ind}_{\mathcal{H}_i^v}^{\mathcal{G}_v}(Z)$, где $\mathcal{H}_i^v = x_i^v \mathcal{H} (x_i^v)^{-1} \cap \mathcal{G}_v$. Таким образом, $H^2(\mathcal{G}_v, Z[\mathcal{G}/\mathcal{H}]) = \sum_{i=1}^{r_v} H^2(\mathcal{H}_i^v, Z)$. Применяя теперь сдвиг размерности (см. лемму 1.3), мы видим, что первый квадрат в (11) эквивалентен следующей диаграмме:

$$\begin{array}{ccc} H^1(\mathcal{G}, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & H^1(\mathcal{H}, \mathbb{Q}/\mathbb{Z}) \\ \downarrow \beta_1 & & \downarrow \beta_2 \\ \prod_v H^1(\mathcal{G}_v, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\psi} & \prod_v \left(\sum_{i=1}^{r_v} H^1(\mathcal{H}_i^v, \mathbb{Q}/\mathbb{Z}) \right), \end{array} \tag{12}$$

в которой все стрелки являются отображениями ограничения; в частности, $\Phi \simeq \beta_2^{-1}(\operatorname{Im} \psi)/\operatorname{Im} \varphi$. Но для конечной группы $\mathcal{F}$ группа $H^1(\mathcal{F}, \mathbb{Q}/\mathbb{Z})$ совпадает с двойственной к абелинизации $\mathcal{F}^{ab} = \mathcal{F}/[\mathcal{F}, \mathcal{F}]$, поэтому диаграмма (12) является двойственной к диаграмме

$$\begin{array}{ccc} \mathcal{G}/[\mathcal{G}, \mathcal{G}] & \xleftarrow{\mu} & \mathcal{H}/[\mathcal{H}, \mathcal{H}] \\ \uparrow \gamma & & \uparrow \delta \\ \sum_v \mathcal{G}_v/[\mathcal{G}_v, \mathcal{G}_v] & \xleftarrow{\eta} & \sum_v \left(\sum_{i=1}^{r_v} \mathcal{H}_i^v/[\mathcal{H}_i^v, \mathcal{H}_i^v] \right), \end{array} \tag{13}$$

в которой все стрелки индуцированы соответствующими включениями. С использованием элементарных фактов о двойственности абелевых групп из (13) получается

Теорема 12. *В обозначениях диаграммы* (13)

$$\Phi \simeq \operatorname{Ker} \mu/\delta(\operatorname{Ker} \eta).$$

Теорема 12 позволяет эффективно вычислять первое препятствие Ф. (Впрочем, читателю, желающему повысить «степень эффективности», рекомендуем получить арифметическую интерпретацию числа r_v и групп $\mathscr{H}_i^v$.) При этом если $\Phi \neq 1$, то принцип Хассе для расширения P/K заведомо не может иметь место. Эти факты лежат в основе построения первого контрпримера к проблеме Бартельса. А именно, вначале строится такое расширение Галуа L/K с группой Галуа $\mathscr{G} = A_6$, что множество нормирований поля K, имеющих в L нециклическую группу разложения, содержит не менее двух элементов и все нециклические группы разложения изоморфны $(\mathbb{Z}/2\mathbb{Z})^2$. Группа $\mathscr{G}$ обладает подгруппой $\mathscr{H}$ индекса 10, которая порождена подстановками (123), (456), (1425), (36) и, следовательно, изоморфна полупрямому произведению $(\mathbb{Z}/3\mathbb{Z})^2 \lambda \mathbb{Z}/4\mathbb{Z}$. Положим $P = L^{\mathscr{H}}$. Тогда при помощи критерия из п. 1 § 1.5 устанавливается, что P является K-адекватным. С другой стороны, прямое вычисление показывает, что первое препятствие в данном случае нетривиально, и, следовательно, принцип Хассе для P/K не выполняется.

Первое препятствие оказывается эффективным не только при построении контрпримеров, но и при доказательстве справедливости принципа Хассе для расширений того или иного типа. Так, например, обстоит дело, если первое препятствие совпадает со всей группой Ш(T), которую естественно называть *полным препятствием*. В работе Дракохруста, Платонова [1] установлено совпадение первого и полного препятствий для расширений бесквадратной степени и для K-адекватных расширений степени p^2. Отсюда путем вычисления первого препятствия выводится справедливость принципа Хассе для K-адекватных расширений, степень которых либо равна шести, либо имеет вид p^2. Полное препятствие не всегда совпадает с первым, однако, как показал Дракохруст [1], оно может быть вычислено аналогично с использованием так называемых обобщенных групп представлений. Основы теории групп представлений были заложены Шуром [1], а современная трактовка этих вопросов изложена в книге Бейля и Таппа [1]. Так, конечная группа $\overline{\mathscr{G}}$ называется *обобщенной группой представления* конечной группы $\mathscr{G}$, если имеется центральное расширение $1 \to M \to \overline{\mathscr{G}} \xrightarrow{\lambda} \mathscr{G} \to 1$, причем пересечение $M \cap [\overline{\mathscr{G}}, \overline{\mathscr{G}}]$ изоморфно группе $H^3(\mathscr{G}, \mathbb{Z})$, которая носит название *мультипликатора Шура* группы $\mathscr{G}$. (От-

метим, что в силу леммы 1.3 $H^3(\mathscr{G}, \mathbb{Z}) = H^2(\mathscr{G}, \mathbb{Q}/\mathbb{Z})$.) Для сравнения укажем, что в классическом определении группы представления требовалось выполнение включения $M \subset [\overline{\mathscr{G}}, \overline{\mathscr{G}}]$. Пусть $\overline{\mathscr{G}}$ — произвольная обобщенная группа представления для $\mathscr{G}$. Для любой подгруппы $\mathscr{F} \subset \mathscr{G}$ будем обозначать через $\overline{\mathscr{F}}$ ее прообраз $\lambda^{-1}(\mathscr{F})$. Рассмотрим следующую диаграмму, аналогичную (13):

$$\begin{tikzcd}
\overline{\mathscr{G}}/[\overline{\mathscr{G}}, \overline{\mathscr{G}}] & \overline{\mathscr{H}}/[\overline{\mathscr{H}}, \overline{\mathscr{H}}] \arrow[l, "\pi"'] \\
\sum\limits_v \overline{\mathscr{G}}_v/[\overline{\mathscr{G}}_v, \overline{\mathscr{G}}_v] \arrow[u] & \sum\limits_v \left(\sum\limits_{i=1}^{r_v} \overline{\mathscr{H}}_i^v/[\overline{\mathscr{H}}_i^v, \overline{\mathscr{H}}_i^v] \right) \arrow[l, "\rho"'] \arrow[u, "\varepsilon"']
\end{tikzcd}$$

В этих обозначениях имеет место

Теорема 13 (Дракохруст [1]). *Для норменного тора* $T = \mathbf{R}^{(1)}_{P/K}(\boldsymbol{G}_m)$ *имеем* $Ш(T) \simeq \operatorname{Ker} \pi/\varepsilon(\operatorname{Ker} \rho)$.

Примеры конкретных вычислений $Ш(T)$ при помощи этой формулы читатель может найти в указанной работе Дракохруста. Завершим наш обзор результатов, касающихся норменного принципа Хассе, следующим утверждением (см. Бартельс [3], Платонов [20], Платонов, Рапинчук [4]).

Предложение 10. *Пусть P/K — расширение простой степени p. Тогда для P/K выполняется норменный принцип Хассе.*

Доказательство. Обозначим через L минимальное расширение Галуа, содержащее P, и положим $\mathscr{G} = \operatorname{Gal}(L/K)$, $\mathscr{H} = \operatorname{Gal}(L/P)$. Тогда $\mathscr{G}$ является подгруппой симметрической группы S_p, и поэтому $[\mathscr{G}]$ делится лишь на первую степень p. Следовательно, $([\mathscr{H}], p) = 1$, и силовская p-подгруппа $\mathscr{G}_p$ группы $\mathscr{G}$ является циклической порядка p. Обратимся теперь к диаграмме (11), построенной для тора $T = \mathbf{R}^{(1)}_{P/K}(\boldsymbol{G}_m)$. Так как $Ш(T) \simeq \operatorname{Ker} \alpha_3$ является группой экспоненты p (напомним, что $Ш(T) \simeq (K^* \cap N_{P/K}(J_P))/N_{P/K}(P^*)$, то достаточно показать, что p-часть группы $H^2(\mathscr{G}, \mathbf{X}(T))$ тривиальна. Но $H^2(\mathscr{G}, \mathbb{Z}[\mathscr{G}/\mathscr{H}]) \simeq H^2(\mathscr{H}, \mathbb{Z})$ аннулируется умножением на $[\mathscr{H}]$ и поэтому имеет экспоненту, взаимно простую с p. С другой стороны, p-часть в $H^3(\mathscr{G}, \mathbb{Z})$ изоморфна $H^3(\mathscr{G}_p, \mathbb{Z}) = 0$, ибо группа $\mathscr{G}_p$ циклична. Таким образом, требуемое утверждение вытекает из точности верхней строки в (11).

Можно предложить и более арифметический вариант рассуждений. Сохраняя предыдущие обозначения, положим дополнительно $F = L^{\mathscr{G}_p}$. Тогда, очевидно, $L = FP$ и $F \cap P = K$. Если $a \in K^* \cap N_{P/K}(J_P)$, то $a \in F^* \cap N_{L/F}(J_L)$ и, следовательно, $a \in N_{L/F}(L^*)$ в силу теоремы Хассе о нормах, ибо расширение L/F циклическое. Поэтому

$$a^{[F:K]} = N_{F/K}(a) \in N_{L/K}(L^*) = N_{P/K}(N_{L/P}(L^*)) \subset N_{P/K}(P^*).$$

С другой стороны, $a^p \in N_{P/K}(P^*)$. Так как числа $[F:K]$ и p взаимно просты, то отсюда вытекает, что $a \in N_{P/K}(P^*)$. Предложение 10 доказано.

На практике кроме норменных торов встречаются еще и *мультинорменные* (см. § 2.1, п. 7). Напомним, что так мы называем ядро T морфизма φ: $\mathbf{R}_{P_1/K}(\boldsymbol{G}_m) \times \ldots \times \mathbf{R}_{P_l/K}(\boldsymbol{G}_m) \to \boldsymbol{G}_m$, являющегося произведением норменных отображений из конечных расширений P_i/K $(i=1, \ldots, l)$.

Упражнение. Показать, что любой максимальный K-тор группы $G = \boldsymbol{SL}_n$ является мультинорменным, т. е. соответствует некоторому набору $P_1, \ldots, P_l$ конечных расширений поля K таких, что $\sum_{i=1}^{l} [P_i : K] = n$.

Из точной последовательности $1 \to T \to \prod_{i=1}^{l} \mathbf{R}_{P_i/K}(\boldsymbol{G}_m) \to \boldsymbol{G}_m \to 1$ легко получить, что $Ш(T) \simeq (K^* \cap N_{P_1/K}(J_{P_1}) \ldots N_{P_l/K}(J_{P_l}))/N_{P_1/K}(P_1^*) \ldots N_{P_l/K}(P_l^*)$. Поэтому справедливость принципа Хассе для тора T означает, что элемент $a \in K^*$, локально представимый в виде произведения норм из полей P_i, представим в таком же виде глобально. По этой причине локально-глобальный принцип в данной ситуации естественно называть *мультинорменным*. Этот принцип прежде нигде детально не рассматривался, однако у нас он играет весьма существенную роль. В частности, с его помощью удалось существенно модифицировать доказательство принципа Хассе для групп типа ${}^2A_n$. Еще одно его применение связано с исследованием структуры групп рациональных точек простых групп типа ${}^1A_n$ (см. § 9.2). Для наших целей вполне хватает следующего достаточного признака справедливости мультинорменного принципа, который для случая расширений Галуа принадлежит Ю. А. Дракохрусту:

Предложение 11. *Пусть P_i $(i=1, 2)$ — два конечных расширения поля K, L_i — их нормальные замыкания. Предположим, что выполняются следующие условия:*

1) $L_1 \cap L_2 = K$;

2) *P_1/K удовлетворяет норменному принципу Хассе.*

Тогда $K^* \cap (N_{P_1/K}(J_{P_1}) N_{P_2/K}(J_{P_2})) = N_{P_1/K}(P_1^*) N_{P_2/K}(P_2^*)$.

Доказательство. Пусть $P = P_1P_2$, $L = L_1L_2$, $\mathcal{G}_i = \mathrm{Gal}(L_i/K)$, $\mathcal{G} = \mathrm{Gal}(L/K) = \mathcal{G}_1 \times \mathcal{G}_2$, $\mathcal{H}_i = \mathrm{Gal}(L_i/P_i)$ и $\mathcal{H} = \mathrm{Gal}(L/P) = \mathcal{H}_1 \times \mathcal{H}_2$. Далее, обозначим через M_i максимальное абелево расширение поля K, содержащееся в P_i. Сразу же заметим, что $\mathcal{H}[\mathcal{G}, \mathcal{G}] = \mathcal{H}_1[\mathcal{G}_1, \mathcal{G}_1] \times \mathcal{H}_2[\mathcal{G}_2, \mathcal{G}_2]$, откуда по теории Галуа следует, что максимальное абелево расширение M поля K, содержащееся в P, имеет вид $M = M_1M_2$. Кроме того,

из равенства

$$[\mathscr{H}_1 \times \mathscr{G}_2, \mathscr{H}_1 \times \mathscr{G}_2](\mathscr{H}_1 \times \mathscr{H}_2) = \mathscr{H}_1 \times (\mathscr{H}_2[\mathscr{G}_2, \mathscr{G}_2])$$

вытекает, что максимальное абелево расширение поля P_1, содержащееся в P, имеет вид P_1M_2, и аналогично с заменой P_1 на P_2, M_2 на M_1.

Рассмотрим отображение

$$\varphi\colon J_{P_1}/P_1^*N_{P/P_1}(J_P) \times J_{P_2}/P_2^*N_{P/P_2}(J_P) \to J_K/K^*N_{P/K}(J_P),$$

которое индуцируется произведением норменных отображений $N_{P_1/K}$ и $N_{P_2/K}$. Наша цель — показать, что φ инъективно. Для этого мы покажем, что φ сюръективно и порядки отображаемых групп совпадают. С этой целью рассмотрим аналогичное вспомогательное отображение

$$\psi\colon J_{M_1}/M_1^*N_{M/M_1}(J_M) \times J_{M_2}/M_2^*N_{M/M_2}(J_M) \to J_K/K^*N_{M/K}(J_M).$$

Используя изоморфизмы теории полей классов $J_{M_i}/M_i^*N_{M/M_i}(J_M) \simeq \simeq \mathrm{Gal}(M/M_i)$, $J_K/K^*N_{M/K}(J_M) \simeq \mathrm{Gal}(M/K)$ и тот факт, что $\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(M/M_1) \times \mathrm{Gal}(M/M_2)$, мы видим, что ψ является изоморфизмом. Следовательно, ψ сюръективно, т. е.

$$J_K = N_{M_1/K}(J_{M_1})\, N_{M_2/K}(J_{M_2})\, K^*, \tag{14}$$

и порядки отображаемых групп равны. Воспользуемся теперь тем фактом, что для произвольного конечного расширения E/F числовых полей имеем $F^*N_{E/F}(J_E) = F^*N_{N/F}(J_N)$, где N — максимальное абелево расширение поля F, содержащееся в E, (см. [АТЧ], упр. 8). В частности, $K^*N_{P_i/K}(J_{P_i}) = K^*N_{M_i/K}(J_{M_i})$, откуда с учетом (14) вытекает, что $J_K = N_{P_1/K}(J_{P_1})\, N_{P_2/K}(J_{P_2})\, K^*$, и φ сюръективно. Далее, $[J_{P_1}/P_1^*N_{P/P_1}(J_P)] = [J_{P_1}/P_1^*N_{P_1M_2/P_1}(J_{P_1M_2})] = = [P_1M_2 : P_1] = [M_2 : K] = [M : M_1] = [J_{M_1}/M_1^*N_{M/M_1}(J_M)]$, ибо P_1M_2 — максимальное абелево расширение P_1, содержащееся в P; аналогично, $[J_{P_2}/P_2^*N_{P/P_2}(J_P)] = [J_{M_2}/M_2^*N_{M/M_2}(J_M)]$, $[J_K/K^*N_{P/K}(J_P)] = [J_K/K^*N_{M/K}(J_M)]$. Из этих равенств вытекает, что $[J_{P_1}/P_1^*N_{P/P_1}(J_P)]\,[J_{P_2}/P_2^*N_{P/P_2}(J_P)] = [J_K/K^*N_{P/K}(J_P)]$, и доказательство инъективности φ завершено.

Пусть теперь $a \in K^*$, $a = N_{P_1/K}(x_1)\, N_{P_2/K}(x_2)$, где $x_i \in J_{P_i}$. Тогда пара $(x_1P_1^*N_{P/P_1}(J_P),\ x_2P_2^*N_{P/P_2}(J_P))$ лежит в ядре φ, так что $x_i = y_iN_{P/P_i}(z_i)$, где $y_i \in P_i^*$, $z_i \in J_P$, $i = 1, 2$. В этих обозначениях $a = N_{P_1/K}(y_2)\, N_{P_2/K}(y_2)\, N_{P/K}(z_1z_2)$, и поэтому

$$aN_{P_1/K}(y_1)^{-1}\, N_{P_2/K}(y_2)^{-1} \in K^* \cap N_{P/K}(J_P) \subset K^* \cap N_{P_1/K}(J_{P_1}) = = N_{P_1/K}(P_1^*),$$

ибо для P_1/K выполняется принцип Хассе. Из этих вычислений вытекает, что $a \in N_{P_1/K}(P_1^*) N_{P_2/K}(P_2^*)$. Предложение 11 доказано.

К сожалению, полного исследования вопроса о мультинорменном принципе пока нет.

Завершает этот параграф одно техническое утверждение о группе $P^2(L/K, T)$, которое понадобится нам при исследовании кограничного отображения для полупростых групп.

Предложение 12 (Кнезер [12]). *Пусть T — тор, определенный над числовым полем K и разложимый над конечным расширением Галуа L/K. Предположим, что для некоторого нормирования $v_0 \in V^K$ тор T является K_{v_0}- анизотропным. Тогда $P^2(L/K, T) = 0$.*

Доказательство естественно попытаться получить из теоремы 10. Однако, как показывает анализ, на этом пути мы встречаемся со значительными трудностями. Более предпочтительным оказывается подход, использующий двойственное описание $P^2(L/K, T)$ как коядра отображения $\sum_v \widehat{H}^{-1}(L_w/K_v, \mathbf{X}_*(T)) \to \widehat{H}^{-1}(L/K, \mathbf{X}_*(T))$, индуцированного кограничениями $\mathrm{Cor}^{\mathscr{G}}_{\mathscr{G}_v}$. (Этот результат был получен нами в процессе доказательства теоремы 10.) Тогда для доказательства предложения достаточно установить сюръективность отображения

$$\mathrm{Cor}^{\mathscr{G}}_{\mathscr{G}_{v_0}}\colon \widehat{H}^{-1}(L_{w_0}/K_{v_0}, \mathbf{X}_*(T)) \to \widehat{H}^{-1}(L/K, \mathbf{X}_*(T)).$$

В силу K_{v_0}-анизотропности T мы имеем $\mathbf{X}_*(T)^{\mathscr{G}_{v_0}} = 0$. С другой стороны, образ норменного отображения $N_{v_0}\colon \mathbf{X}_*(T) \to \mathbf{X}_*(T)$, $N_{v_0}(x) = \sum_{g \in \mathscr{G}_{v_0}} gx$, очевидно, лежит в $\mathbf{X}_*(T)^{\mathscr{G}_{v_0}}$, поэтому $\mathrm{Ker}\, N_{v_0} = \mathbf{X}_*(T)$. Так как по определению $\widehat{H}^{-1}(L_{w_0}/K_{v_0}, \mathbf{X}_*(T)) = \mathrm{Ker}\, N_{v_0}/(\mathbf{X}_*(T)'_{v_0}$, $\widehat{H}^{-1}(L/K, \mathbf{X}_*(T)) = \mathrm{Ker}\, N/\mathbf{X}_*(T)'$, где $N\colon \mathbf{X}_*(T) \to \mathbf{X}_*(T)$ — норменное отображение, отвечающее группе $\mathscr{G}$, $\mathbf{X}_*(T)'$ (соответственно $\mathbf{X}_*(T)'_{v_0}$) — подгруппа в $\mathbf{X}_*(T)$, порожденная элементами вида $g\chi - \chi$, где $\chi \in \mathbf{X}_*(T)$, а g пробегает $\mathscr{G}$ (соответственно $\mathscr{G}_{v_0}$). Учитывая, что $\mathrm{Cor}^{\mathscr{G}}_{\mathscr{G}_{v_0}}$ в данной ситуации индуцировано вложением $\mathrm{Ker}\, N_{v_0}$ в $\mathrm{Ker}\, N$, мы получаем, что $\mathrm{Cor}^{\mathscr{G}}_{\mathscr{G}_{v_0}}$ сюръективно. Предложение 12 доказано.

§ 6.4. Теоремы конечности для когомологий Галуа

В этом параграфе мы распространим факты о конечности для когомологий Галуа, которые были получены в § 6.3 для случая алгебраических торов при помощи теорем Накаямы — Тейта, на произвольные алгебраические группы.

Теорема 14. *Пусть G — алгебраическая группа, определенная над локальным полем K. Тогда множество $H^1(K, G)$ конечно.*

Теорема 15. *Пусть G — алгебраическая группа, определенная над числовым полем K. Тогда ядро канонического отображения $H^1(K, G) \to \prod_v H^1(K_v, G)$ конечно.*

Если в случае торов доказательства этих теорем содержали ряд общих моментов, то в общем случае они основаны на совершенно различных подходах. Так, для доказательства теоремы 15 приходится привлекать построенную в гл. V теорию приведения для групп аделей, в то время как теорема 14 является формальным следствием одного свойства группы Галуа локального поля.

Определение. *Будем говорить, что проконечная группа $\mathcal{G}$ имеет тип (F), если для любого целого n она имеет лишь конечное число открытых подгрупп индекса n. Поле K имеет тип (F), если оно совершенно, и его абсолютная группа Галуа $\mathcal{G} = \mathrm{Gal}(\bar{K}/K)$ имеет тип (F).*

Ясно, что совершенное поле K имеет тип (F) в том и только том случае, если для любого целого n оно имеет лишь конечное число расширений степени n. Отсюда вытекает, что примерами полей типа (F) являются: а) поле вещественных чисел; б) конечное поле; в) поле формальных степенных рядов $P\langle t\rangle$ от одной переменной над алгебраически замкнутым полем констант P характеристики 0. (В последнем случае известно (теорема Пюизе), что для любого n поле $P\langle t\rangle$ обладает единственным расширением степени n, которое имеет вид $P\langle\sqrt[n]{t}\rangle$.) Для нас существенное значение имеет тот факт, что тип (F) имеет локальное поле.

Предложение 13. *Пусть K — конечное расширение поля $\mathbb{Q}_p$. Тогда K имеет тип (F).*

Доказательство. Так как для каждого n существует единственное неразветвленное расширение поля K степени n, а любое конечное расширение поля K представимо в виде башни неразветвленного и вполне разветвленного расширений (см. [АТЧ], гл. I), то достаточно показать, что любое локальное поле имеет конечное число вполне разветвленных расширений. Чтобы не вводить дополнительных обозначений, мы установим последний факт для поля K.

Известно (см. предложение 1.4), что любое вполне разветвленное расширение K степени n задается корнем некоторого многочлена Эйзенштейна $t^n + a_{n-1}t^{n-1} + \ldots + a_0 = 0$. С другой стороны, множество M коэффициентов $(a_{n-1}, \ldots, a_0)$ всевозможных многочленов Эйзенштейна, очевидно, компактно как подмножество в K^n. Поэтому стандартное рассуждение показывает, что требуемое утверждение вытекает из следующего факта,

известного как *лемма Краснера*: если f — неприводимый полином над K степени n со старшим коэффициентом единица, то любой полином g над K, коэффициенты которого достаточно близки к коэффициентам f, также неприводим, причем f и g задают изоморфные расширения K. Обычное доказательство леммы Краснера читатель может найти в книге Ленга [2]. Мы покажем, как это утверждение получается в нашем контексте. Для полинома $f(t)=t^n+a_{n-1}t^{n-1}+\ldots+a_0$ обозначим через $a(f)$ матрицу

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & \ldots & \ldots \\ 0 & 1 & 0 & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}.$$

Тогда легко проверить, что $f(a(f))=0$. Ясно, что если f неприводим, то K-алгебра $K[a(f)]$, порожденная $a(f)$, изоморфна расширению K_f поля K степени n, задаваемому полиномом f. При этом мультипликативная группа $K[a(f)]^*$ совпадает с множеством K-точек тора $T=\mathbf{R}_{K_f/K}(\boldsymbol{G}_m)$. Положим $G=\boldsymbol{GL}_n$ и обозначим через U открытое подмногообразие в T, состоящее из регулярных в G элементов (см. § 2.1, п. 11). Рассмотрим, далее, отображение φ: $G\times U\to G$, $\varphi(g,u)=gug^{-1}$. Тогда образ φ в точности совпадает со множеством полупростых регулярных элементов G, и поэтому открыт в G в топологии Зарисского; в частности, морфизм φ является доминантным. Поэтому из предложения 3.3 вытекает, что $W=\varphi(G_K\times U_K)$ является открытым подмножеством G_K относительно v-адической топологии. С другой стороны, ясно, что для любого $x\in W$ K-алгебра $K[x]$ сопряжена относительно G_K с алгеброй $K[a(f)]$. Так как $a(f)\in U_K\subset W$, то для всех полиномов g, достаточно близких к f, точка $a(g)$ также попадает в W, и поэтому алгебры $K[a(f)]$ и $K[a(g)]$ сопряжены, следовательно, поля K_f и K_g изоморфны. Предложение 13 доказано.

Теорема 14 вытекает теперь из следующего общего результата.

Теорема 16. *Пусть K — поле типа (F), G — линейная алгебраическая группа, определенная над K. Тогда множество $H^1(K,G)$ конечно.*

Доказательство проведем вначале для конечной группы G. Обозначим через $\mathscr{H}$ открытый нормальный делитель группы $\mathscr{G}=\mathrm{Gal}(\bar{K}/K)$, тривиально действующий на $G=G_{\bar{K}}$. В силу определения группы типа (F), существует лишь конечное число открытых подгрупп в $\mathscr{G}$, содержащихся в $\mathscr{H}$ и имеющих в $\mathscr{H}$ индекс, не превосходящий $n=[G]$. Их пересечение, которое мы обозначим через $\mathscr{F}$, является открытым нормальным делителем

группы $\mathscr{G}$, содержащимся в $\mathscr{H}$. Утверждается, что отображение ограничения φ: $H^1(\mathscr{G}, G_{\overline{K}}) \to H^1(\mathscr{F}, G_{\overline{K}})$ тривиально. Действительно, если f: $\mathscr{G} \to G_{\overline{K}}$ — непрерывный 1-коцикл, то ограничение $g = f|_{\mathscr{H}}$ является непрерывным гомоморфизмом $\mathscr{H} \to G_{\overline{K}}$, ибо $\mathscr{H}$ тривиально действует на $G_{\overline{K}}$. Тогда $[\mathscr{H} : \operatorname{Ker} g] \leqslant n$, так что по построению $\mathscr{F} \subset \operatorname{Ker} g$, т. е. $g(\mathscr{F}) = \{e\}$, что и требовалось. Рассмотрим теперь некоммутативный аналог спектральной последовательности Хохшильда — Серра (см. § 1.3, п. 2):

$$1 \to H^1(\mathscr{G}/\mathscr{F}, G_{\overline{K}}) \xrightarrow{\varepsilon} H^1(\mathscr{G}, G_{\overline{K}}) \xrightarrow{\varphi} H^1(\mathscr{F}, G_{\overline{K}}). \qquad (1)$$

Из тривиальности φ и точности (1) вытекает сюръективность ε. Но множество $H^1(\mathscr{G}/\mathscr{F}, G_{\overline{K}})$, очевидно, конечно, поэтому конечно и множество $H^1(\mathscr{G}, G_{\overline{K}}) = H^1(K, G)$.

Следующая лемма, примененная к $N = G^0$, вместе с уже доказанным фактом позволяет получить редукцию теоремы 16 к случаю связных групп.

Лемма 9. *Пусть G — K-определенная алгебраическая группа, N — ее K-определенный нормальный делитель. Предположим, что конечно множество $H^1(K, G/N)$, и для любого коцикла $\mu \in Z^1(K, G)$ конечно множество $H^1(K, {}_\mu N)$, где ${}_\mu N$ — группа, получаемая из N скручиванием при помощи μ *). Тогда множество $H^1(K, G)$ также конечно.*

В самом деле, точная последовательность K-групп $1 \to N \to G \to G/N \to 1$ индуцирует отображение первых когомологий $H^1(K, G) \xrightarrow{\pi} H^1(K, G/N)$, которое обладает свойством: для $\mu \in H^1(K, G)$ слой $\pi^{-1}(\pi(\mu))$ сюръективно накрывается множеством $H^1(K, {}_\mu N)$ (см. § 1.3, п.2). Поэтому если $\pi(H^1(K, G)) = \pi(\{\mu_1, \ldots, \mu_r\})$, то $H^1(K, G) = \bigcup_{i=1}^{r} \pi^{-1}(\pi(\mu_i))$ — конечное множество, ибо каждое из множеств $\pi^{-1}(\pi(\mu_i))$ конечно в силу предположения о конечности $H^1(K, {}_{\mu_i} N)$.

Итак, мы можем предполагать группу G связной. В этом случае, как показывает предложение 2.9, $H^1(K, G) = H^1(K, H)$ для максимальной редуктивной K-подгруппы $H \subset G$, поэтому в рассмотрении нуждается лишь случай связной редуктивной группы G. Разберем вначале случай, когда $G = T$ — алгебраический тор. (Отметим, что здесь для локального поля K конечность $H^1(K, T)$ была установлена в § 6.3, однако мы намерены получить общее доказательство, которое «работает» для всех полей типа (F).) Обозначим через L конечное расширение Галуа поля K, над которым T становится разложимым, и положим $n =$

---

*) Имеется в виду естественное действие G на N посредством сопряжения.

$=[L:K]$. Тогда группа $H^1(K,T)$ совпадает с $H^1(L/K,T)$ (лемма 8), и поэтому является группой экспоненты n. Рассмотрим морфизм η: $T\to T$, $\eta(t)=t^n$ и обозначим через S его ядро. Имеет место следующая точная последовательность групп когомологий $H^1(K,S)\to H^1(K,T)\xrightarrow{\theta} H^1(K,T)$, где гомоморфизм θ индуцирован η. Из сказанного выше вытекает, что θ является тривиальным отображением, поэтому $H^1(K,T)$ накрывается группой $H^1(K,S)$. Но группа $H^1(K,S)$ конечна, ибо, как легко видеть, конечна группа S.

Случай произвольных связных редуктивных групп в теореме 16 может быть легко сведен к торам. С этой целью заметим, что комбинируя лемму 9 с уже доказанным результатом о конечности H^1 для конечных групп и торов, получаем конечность H^1 для групп, связная компонента которых является тором. Этот результат применим, в частности, к нормализатору $N=N_G(T)$ произвольного K-определенного тора T данной связной редуктивной K-группы G. Поэтому завершает доказательство теоремы 16

Лемма 10. *Естественное отображение $H^1(K,N)\to H^1(K,G)$ сюръективно.*

Доказательство. Пусть $\mathscr{T}=G/N$ — многообразие максимальных торов группы G (см. § 2.4, п. 5). Для произвольного коцикла $g\in Z^1(K,G)$ рассмотрим группу ${}_gG$ и многообразие ${}_g\mathscr{T}$, получаемые применением скручивания (см. § 1.3, п. 2), где группа G действует на себе сопряжениями, а на многообразии $\mathscr{T}$ — сдвигами. Очевидно, имеется K-определенное действие ${}_gG$ на ${}_g\mathscr{T}$, причем стабилизатор точки является нормализатором максимального тора. Тогда, используя тот факт, что ${}_gG$ всегда обладает максимальным K-определенным тором (см. § 2.1, п. 9), легко показать, что $({}_g\mathscr{T})_K\neq\varnothing$, и поэтому из леммы 1.6 вытекает, что g лежит в образе отображения $H^1(K,N)\to H^1(K,G)$. Лемма 9 доказана.

Следствие 1. *Пусть K — поле типа (F). Тогда с точностью до K-изоморфизма существует лишь конечное число K-форм данной полупростой K-группы G.*

Действительно, мы знаем (см. § 2.2), что K-формы данной K-группы G с точностью до K-изоморфизма классифицируются элементами множества $H^1(K,\mathrm{Aut}_{\overline{K}}(G))$. С другой стороны, для полупростой группы G группа $\mathrm{Aut}_{\overline{K}}(G)$ является конечным расширением группы внутренних автоморфизмов, которая изоморфна соответствующей присоединенной группе, и поэтому может рассматриваться как алгебраическая K-группа. Тогда согласно теореме 14 множество $H^1(K,\mathrm{Aut}_{\overline{K}}(G))$ конечно, значит, конечно и число неизоморфных K-форм группы G.

Упражнение. Выяснить, остается ли справедливым утверждение следствия для произвольной связной группы G. (Отметим,

что приведенное доказательство не проходит уже для n-мерного алгебраического тора T при $n > 1$, ибо здесь $\mathrm{Aut}_{\overline{K}}(T) \simeq GL_n(\mathbb{Z})$ не является алгебраической группой.)

Следствие 2. *Пусть X — определенное над K однородное пространство линейной алгебраической K-группы G, причем поле K имеет тип (F). Тогда X_K является объединением конечного числа орбит группы G_K.*

Если $X_K = \varnothing$, то доказывать нечего. В противном случае пусть $x \in X_K$, $H = G(x)$ — стабилизатор точки x. Тогда, в силу совершенности K, группа H является K-определенной, и достаточно установить конечность числа орбит группы G_K на $(G/H)_K$. Однако известно, что последние находятся в биективном соответствии с элементами ядра отображения $H^1(K, H) \to H^1(K, G)$, поэтому требуемое вытекает из теоремы 16.

В частности, беря в качестве X многообразие торов $\mathcal{T}$ данной связной группы G, получаем

Следствие 3. *Пусть G — связная линейная группа над полем K типа (F). Тогда максимальные K-определенные торы группы G образуют конечное число классов сопряженности относительно группы G_K.*

Весьма частным случаем теоремы 16 является утверждение о конечности множества вещественных 1-когомологий $H^1(\mathbb{R}, G)$ для любой $\mathbb{R}$-определенной алгебраической группы G. Покажем, что этот факт на самом деле вытекает из теоремы Уитни (см. § 3.2, теорема 3.6). Действительно, в § 3.2, пользуясь теоремой Уитни, мы дали независимое от теоремы 16 доказательство следствия 2 для $K = \mathbb{R}$. Пусть теперь G — вещественная алгебраическая группа и $G \subset \boldsymbol{GL}_n$ — ее некоторая $\mathbb{R}$-определенная матричная реализация. Применяя утверждение следствия 2 к однородному пространству $X = \boldsymbol{GL}_n/G$, получаем конечность числа орбит группы $GL_n(\mathbb{R})$ на $X_{\mathbb{R}}$, а значит, и конечность ядра отображения $H^1(\mathbb{R}, G) \to H^1(\mathbb{R}, \boldsymbol{GL}_n)$ (см. доказательство следствия 2). Но $H^1(\mathbb{R}, \boldsymbol{GL}_n) = \{1\}$ (лемма 2.2), поэтому тем самым мы получаем конечность всего множества $H^1(\mathbb{R}, G)$. (Приведенное рассуждение показывает, что следствие 2 в действительности эквивалентно самой теореме 16. Адельный вариант этого наблюдения мы используем ниже при доказательстве теоремы 15.) На самом деле для вещественных когомологий имеются гораздо более точные результаты. Так, в случае $\mathbb{R}$-анизотропной группы G Серром (см. [1], гл. III, § 4.5) было доказано фактически следующее утверждение

Теорема 17. *Пусть G — связная $\mathbb{R}$-определенная алгебраическая группа с компактной группой $G_{\mathbb{R}}$. Тогда элементы множества $H^1(\mathbb{R}, G)$ находятся в биективном соответствии с элементами фактормножества S/W, где S — множество элементов фиксированного $\mathbb{R}$-определенного максимального тора $T \subset G$,*

удовлетворяющих соотношению $x^2 = 1$, W — *группа Вейля тора* T, *действующая на* T *сопряжениями.*

(В классических терминах утверждение теоремы означает, что элементы множества $H^1(\mathbb{R}, G)$ находятся в биективном соответствии с классами сопряженности инволюций в группе $G_{\mathbb{R}}$.)

Когомологии произвольной связной редуктивной вещественной группы G были недавно определены Боровым [2]. Для формулировки его результата нам понадобятся некоторые обозначения. Пусть T_0 — максимальный $\mathbb{R}$-анизотропный тор в G, $T = C_G(T_0)$ — его централизатор. Тогда T является максимальным $\mathbb{R}$-определенным тором в G, и можно рассмотреть соответствующую группу Вейля $W = W(T, G) = N/T$, где $N = N_G(T)$ — нормализатор тора T в G. Определим действие группы W на $H^1(\mathbb{R}, T)$ следующим образом. Пусть $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ — автоморфизм комплексного сопряжения. Любой коцикл $\xi \in Z^1(\mathbb{R}, T)$ может быть задан одним элементом $z = \xi_\sigma \in T_{\mathbb{C}}$, причем $z\sigma(z) = 1$. Если теперь $w \in W$ представляется элементом $n \in N_{\mathbb{C}}$, то определим $w\xi$ как коцикл, задаваемый элементом $n^{-1}z\sigma(n)$. Легко проверить, что это действие определено корректно. В этих обозначениях имеет место

Теорема 18. *Вложение* $T \subset G$ *индуцирует биекцию*

$$H^1(\mathbb{R}, T)/W \xrightarrow{\sim} H^1(\mathbb{R}, G).$$

Доказательство теоремы 18 и некоторые ее приложения читатель может найти в статье Борового [2].

Переходим к рассмотрению свойств конечности для когомологий групп, определенных над числовым полем K. Поле K не является полем типа (F) (почему ?), и в действительности множество $H^1(K, G)$ может здесь быть бесконечным. Поэтому результаты о конечности имеют в данной ситуации другой характер (см. теорему 15 и ниже теорему 19) и их получение основано на других соображениях.

Доказательство теоремы 15 начнем с рассмотрения конечной группы G.

Лемма 11. *Пусть* G — *конечная* K-*группа. Тогда ядро* $Ш(G)$ *канонического отображения* $H^1(K, G) \to \prod_v H^1(K_v, G)$ *конечно.*

Доказательство. Обозначим через $\mathscr{H}$ открытый нормальный делитель группы $\mathscr{G} = \mathrm{Gal}(\overline{K}/K)$, тривиально действующий на $G = G_{\overline{K}}$, и положим $L = \overline{K}^{\mathscr{H}}$. Мы покажем, что отображение $H^1(L, G) \xrightarrow{\theta} \prod_w H^1(L_w, G)$ имеет тривиальное ядро. Отсюда следует, что образ $Ш(G)$ при отображении ограничения $H^1(K, G) \to H^1(L, G)$ тривиален, так что из точной последовательности $1 \to H^1(L/K, G) \to H^1(K, G) \to H^1(L, G)$ заключаем,

что Ш(G) накрывается конечным множеством $H^1(L/K, G)$ и, следовательно, само конечно. Для исследования ядра отображения θ заметим, что 1-коциклами в данной ситуации являются непрерывные гомоморфизмы $\alpha\colon \mathscr{H} \to G$, причем существует лишь один тривиальный коцикл, который определяется единичным гомоморфизмом. Если теперь $\alpha \in \operatorname{Ker}\theta$, то $\alpha(\mathscr{H}_w) = \{1\}$ для любого нормирования $w \in V^L$, где $\mathscr{H}_w = \operatorname{Gal}(\bar{L}_w/L_w)$ отождествляется с подгруппой разложения в $\mathscr{H} = \operatorname{Gal}(\bar{L}/L)$ фиксированного продолжения $\bar{w}$ нормирования w на поле $\bar{L}$; отметим, что в силу сопряженности двух различных продолжений $\bar{w}'$ и $\bar{w}''$ относительно группы $\mathscr{H}$ соответствующие подгруппы $\mathscr{H}'_w$ и $\mathscr{H}''_w$ сопряжены в $\mathscr{H}$, и поэтому условия $\alpha(\mathscr{H}'_w) = \{1\}$ и $\alpha(\mathscr{H}''_w) = \{1\}$ эквивалентны. Поэтому достаточно показать, что замкнутая нормальная подгруппа $\mathscr{P} \subset \mathscr{H}$, порожденная всеми $\mathscr{H}_w$, совпадает с $\mathscr{H}$. Рассмотрим неподвижное поле $P = \bar{L}^{\mathscr{P}}$. Тогда P является нормальным расширением поля L, которое обладает тем свойством, что $P \subset L_w$ для всех $w \in V^L$. Если предположить, что $P \neq L$, то найдется нетривиальное конечное нормальное расширение F/L, также обладающее свойством: $F \subset L_w$ для всех $w \in V^L$. Но это, очевидно, противоречит теореме плотности Чеботарева. Лемма доказана.

Чтобы получить редукцию теоремы 15 к случаю связной группы, нам понадобится также следующее утверждение.

Лемма 12. *Пусть G — алгебраическая K-группа, G^0 ее связная компонента. Тогда $G_{K_v}/G^0_{K_v} = (G/G^0)_{K_v}$ для почти всех v. Следовательно, для почти всех v отображение $H^1(K_v, G^0) \to H^1(K_v, G)$ имеет тривиальное ядро.*

Доказательство. Рассмотрим точную последовательность $1 \to G_0 \to G \xrightarrow{\pi} G/G_0 \to 1$ и соответствующую ей точную когомологическую последовательность

$$G_{K_v} \xrightarrow{\pi} (G/G_0)_{K_v} \to H^1(K_v, G^0) \xrightarrow{\psi} H^1(K_v, G). \tag{2}$$

При доказательстве предложения 5.5 мы показали, что для почти всех $v \in V_f^K$ имеем $\pi(G_{\mathcal{O}_v}) = (G/G^0)_{K_v}$; в частности, $\pi(G_{K_v}) = (G/G^0)_{K_v}$. Поэтому из точной последовательности (2) получаем, что $\operatorname{Ker}\psi$ для этих v тривиально. Лемма доказана.

Предположим теперь, что мы умеем доказывать конечность Ш связных групп, и покажем, что тогда Ш(G) конечно для любой K-группы G. Рассмотрим коммутативную диаграмму

$$\begin{array}{ccc} H^1(K, G) & \xrightarrow{\rho} & \prod\limits_v H^1(K_v, G) \\ \sigma\downarrow & & \downarrow\tau \\ H^1(K, G/G^0) & \xrightarrow{\theta} & \prod\limits_v H^1(K_v, G/G^0) \end{array}$$

Согласно лемме 11 $\operatorname{Ker}\theta$ конечно, откуда следует конечность $\sigma(Ш(G))$, скажем, $\sigma(Ш(G)) = \sigma(\{\mu_1, \ldots, \mu_r\})$, $\mu_i \in Ш(G)$. Применяя процедуру скручивания, получаем, что $Ш(G)$ покрывается объединением образов множеств $Ш_i = \operatorname{Ker}(H^1(K, G_i^0) \to \to \prod_v H^1(K_v, G_i))$, где $G_i = {}_{\mu_i}G$, $G_i^0 = {}_{\mu_i}G_i^0$ — соответствующие скрученные группы. Но в силу леммы 12 ядро отображения $H^1(K_v, G_i^0) \to H^1(K_v, G_i)$ тривиально для почти всех v, и, как следует из теоремы 14, конечно в остальных случаях. Поэтому отображение $\prod_v H^1(K_v, G_i^0) \to \prod_v H^1(K_v, G_i)$ имеет конечное ядро, так что образ множества $Ш_i$ в $\prod_v H^1(K_v, G_i^0)$ конечен. Но по предположению ядро отображения $H^1(K, H) \to \prod_v H^1(K_v, H)$ конечно для любой связной группы H, поэтому опять применяя скручивание, получаем, что прообраз любого элемента при отображении $H^1(K, G_i^0) \to \prod_v H^1(K_v, G_i^0)$ конечен. Учитывая вышесказанное, отсюда получаем конечность каждого из множеств $Ш_i$, а значит, и множества $Ш(G)$.

Осталось рассмотреть основной случай связной K-группы G, которую в силу предложения 2.9 можно дополнительно предполагать редуктивной. Для этого зафиксируем матричную реализацию $G \subset \boldsymbol{GL}_n$ и построим однородное пространство $X = \boldsymbol{GL}_n/G$. Выше мы видели, что элементы множества $H^1(K, G)$ находятся в биективном соответствии с орбитами группы $GL_n(K)$ на X_K, причем, исходя из этой интерпретации, можно установить, скажем, конечность вещественных когомологий. Наше доказательство конечности $Ш(G)$ основано на аналогичной интерпретации.

Лемма 13. *Пусть* π: $\boldsymbol{GL}_n \to X$ — *каноническая проекция. Тогда элементы* $Ш(G)$ *находятся в биективном соответствии с орбитами группы* $GL_n(K)$ *на* $\pi_A(GL_n(A)) \cap X_K$, *где* A — *кольцо аделей поля* K.

Доказательство. Для всякого расширения P/K имеем отображение ψ_P: $X_P \to H^1(P, G)$, слои которого находятся в биективном соответствии с орбитами группы G_P на X_P. Тогда из коммутативной диаграммы

$$\begin{tikzcd} X_K \arrow[r, "\psi_K"] \arrow[d] & H^1(K, G) \arrow[d, "\rho"] \\ \prod_v X_{K_v} \arrow[r, "\prod_v \psi_{K_v}"] & \prod_v H^1(K_v, G) \end{tikzcd}$$

заключаем, что элементы $Ш(G)$ биективно соответствуют орбитам группы $GL_n(K)$ на множестве $B = \left(\prod_v \pi_{K_v}(GL_n(K_v))\right) \cap X_K$,

поэтому достаточно показать, что B совпадает с указанным в формулировке леммы пересечением $\pi_A(GL_n(A))\cap X_K$. Но это без труда следует из того факта, что для почти всех $v\in V_f^K$ имеем $\pi(GL_n(\mathcal{O}_v))=X_{\mathcal{O}_v}$. Доказательство этого утверждения полностью аналогично доказательству предложения 5 и оставляется читателю в качестве упражнения. Лемма доказана.

Сопоставляя лемму 13 с теоремой 5.3, мы и получаем доказательство теоремы 15.

Теореме 15 можно придать также следующую форму, которая иногда оказывается удобной.

Теорема 19. *Пусть G — линейная алгебраическая группа, определенная над числовым полем K, $S\subset V^K$ — конечное подмножество. Тогда естественное отображение $\rho_S\colon H^1(K,G)\to\prod_{v\notin S}H^1(K_v,G)$ собственно, т. е. прообраз любого конечного множества конечен.*

Действительно, используя конечность локальных когомологий (теорема 14), все легко свести к случаю $S=\varnothing$, причем достаточно установить конечность прообраза при $\rho=\rho_\varnothing$ любого элемента. При помощи процедуры скручивания легко получить, что для любого $\mu\in H^1(K,G)$ слой $\rho^{-1}(\rho(\mu))$ покрывается множеством $Ш({}_\mu G)$, которое конечно по теореме 15.

Множество $Ш(G)$ можно определить не только для линейной алгебраической группы, но и, скажем, для абелева многообразия, где оно является абелевой группой, называемой *группой Шафаревича — Тейта*. Однако здесь вопрос о конечности $Ш(G)$ является гораздо более сложным. Так, в течение долгого времени не было известно ни одной эллиптической кривой, для которой удалось доказать конечность Ш. Прогресс здесь был достигнут лишь совсем недавно в работах Рубина [1] и Колывагина [1], [2], которые установили конечность Ш для больших серий эллиптических кривых. (Отметим, что одна из причин, по которой приведенное доказательство теоремы 15 не проходит для абелевых многообразий, состоит в том, что абелево многообразие, вообще говоря, нельзя погрузить в алгебраическую группу с тривиальными когомологиями, в то время как для линейных групп такое погружение доставляет произвольная матричная реализация $G\subset \boldsymbol{GL}_n$.)

Завершим этот параграф примером полупростой K-определенной группы G с нетривиальным множеством $Ш(G)$. Начнем с расширения L/K, где $K=\mathbb{Q}$, $L=\mathbb{Q}(\sqrt{13},\sqrt{17})$, для которого нарушается принцип Хассе (см. пример 1 в § 6.3). Обозначим через μ_n алгебраическую группу, образованную корнями степени n из единицы и воспользуемся конструкцией, описанной при доказательстве предложения 7. А именно, рассмотрим норменное отображение $N\colon \boldsymbol{R}_{L/K}(\mu_n)\to\mu_n$ и обозначим через F его

ядро. (Ясно, что F совпадает со множеством элементов порядка, делящего n в норменном торе $S = \mathbf{R}^{(1)}_{L/K}(\boldsymbol{G}_m)$).

Когомологии группы F можно вычислить из точной последовательности

$$1 \to F \to \mathbf{R}_{L/K}(\mu_n) \to \mu_n \to 1, \tag{3}$$

которая индуцирует следующую коммутативную диаграмму с точными строками:

$$\begin{array}{ccccc} H^1(K, \mathbf{R}_{L/K}(\mu_n)) & \xrightarrow{\alpha_1} & H^1(K, \mu_n) & \xrightarrow{\alpha_2} & H^2(K, F) \\ \downarrow \gamma_1 & & \downarrow \gamma_2 & & \downarrow \gamma_3 \\ \prod\limits_v H^1(K_v, \mathbf{R}_{L/K}(\mu_n)) & \xrightarrow{\beta_1} & \prod\limits_v H^1(K_v, \mu_n) & \xrightarrow{\beta_2} & \prod\limits_v H^2(K_v, F) \end{array} \tag{4}$$

Имеем $H^1(K, \mu_n) = K^*/K^{*n}$, $H^1(K, \mathbf{R}_{L/K}(\mu_n)) = H^1(L, \mu_n) = L^*/L^{*n}$, причем α_1 индуцируется норменным отображением $N_{L/K}\colon L^* \to K^*$. Отсюда следует, что α_2 индуцирует вложение $K^*/K^{*n}N_{L/K}(L^*)$ в $H^2(K, F)$. Будем предполагать, что n имеет вид $n = 4l$, и тогда $K^{*n} \subset N_{L/K}(L^*)$, т. е. имеем вложение $K^*/N_{L/K}(L^*)$ в $H^2(K, F)$.

Пусть $x \in K^*/K^{*n}$ — такой элемент, что его образ в $K^*/N_{L/K}(L^*)$ определяет нетривиальный элемент группы Шафаревича — Тейта $Ш(S) \cong (K^* \cap N_{L/K}(J_L))/N_{L/K}(L^*)$, $y = \alpha_2(x)$. Тогда из коммутативности диаграммы (4) и определений вытекает

Лемма 14. *Элемент $y \in H^2(K, F)$ нетривиален и лежит в* $\operatorname{Im}\alpha_2 \cap \operatorname{Ker}\gamma_3$.

Теперь уже легко завершить построение соответствующего примера. Положим $\tilde{G} = \mathbf{R}_{L/K}(\mathbf{SL}_n)$. Тогда $Z(\tilde{G}) = \mathbf{R}_{L/K}(\mu_n)$, и можно рассмотреть вложение $F \subset Z(\tilde{G})$. Пусть, далее, $G = \tilde{G}/F$. Имеем коммутативную диаграмму с точными строками

$$\begin{array}{ccccc} H^1(K, \tilde{G}) & \xrightarrow{\delta_1} & H^1(K, G) & \xrightarrow{\delta_2} & H^2(K, F) \\ \downarrow \rho_1 & & \downarrow \rho_2 & & \downarrow \rho_3 \\ \prod\limits_v H^1(K_v, \tilde{G}) & \xrightarrow{\zeta_1} & \prod\limits_v H^1(K_v, G) & \xrightarrow{\zeta_2} & \prod\limits_v H^2(K_v, F). \end{array}$$

Так как $Z(G) = \mathbf{R}_{L/K}(\mu_n)/F \simeq \mu_n$, то $H^1(K, Z(G))$ можно отождествить с K^*/K^{*n}. Рассмотрим тогда x как элемент $H^1(K, Z(G))$, и пусть z — образ x в $H^1(K, G)$. Тогда $z \neq 1$, ибо $\delta_2(z) = y \neq 1$. С другой стороны, поскольку ρ_3 совпадает с γ_3, имеем $\zeta_2(\rho_2(z)) = 1$, и так как для любого v $H^1(K_v, \tilde{G}) = \prod\limits_{w|v} H^1(L_w, \boldsymbol{SL}_n) = 1$, то $\rho_2(z) = 1$. Таким образом, $z \in Ш(G)$ и $Ш(G) \neq 1$.

Как мы уже отмечали, в случае $Ш(G)=1$ говорят, что для группы G выполняется принцип Хассе. Таким образом, приведенный пример можно рассматривать как контрпример к принципу Хассе в классе полупростых групп. Цель последующих параграфов этой главы — показать, что в экстремальных случаях односвязных и присоединенных групп принцип Хассе выполняется всегда.

§ 6.5. Когомологии полупростых алгебраических групп над локальными и числовыми полями

Как мы уже отмечали в § 6.1, основные результаты о когомологиях полупростой односвязной K-группы G заключаются в следующем: $H^1(K, G)=1$, если K — неархимедово локальное поле (теорема 4), и $H^1(K, G)$ изоморфно $\prod_{v \in V_\infty^K} H^1(K_v, G)$, если K — числовое поле (теорема 6). Доказательству этих глубоких теорем будут посвящены § 6.7, 6.8. В настоящем параграфе мы, предполагая эти результаты известными, научимся вычислять когомологии произвольной полупростой группы и дадим некоторые приложения этих результатов (в частности, установим справедливость принципа Хассе для присоединенных групп и докажем тот факт, что группы типов B_n, C_n, E_7, E_8, F_4, G_2 над числовым полем K разложимы над некоторым квадратичным расширением L/K). В следующем параграфе мы с помощью этих результатов получим локально-глобальную классификацию различных типов полуторалинейных форм и докажем теорему 5 о том, что любая анизотропная группа над локальным полем K является группой типа $\boldsymbol{SL}_1(D)$ и аналогичное утверждение над чисто мнимым числовым полем K.

Вычисление когомологий полупростой неодносвязной K-группы G базируется на рассмотрении универсального K-определенного накрытия $1 \to F \to \tilde{G} \xrightarrow{\pi} G \to 1$ и соответствующей точной когомологической последовательности

$$H^1(K, \tilde{G}) \to H^1(K, G) \xrightarrow{\delta} H^2(K, F).$$

Основной результат, позволяющий с помощью теорем 4, 6 и 18 вычислять $H^1(K, G)$, выглядит следующим образом.

Теорема 20. *Если K — (неархимедово) локальное либо числовое поле, то отображение δ сюръективно.*

Следствие. *Если K — локальное поле, то отображение δ биективно.*

Действительно, из теоремы 4 вытекает, что $H^1(K, {}_\xi\tilde{G})=1$ для любого $\xi \in Z^1(K, G)$, откуда следует инъективность δ.

Доказательство теоремы 20 базируется на следующем результате, представляющем независимый интерес.

Теорема 21. *Пусть G — полупростая алгебраическая группа над локальным полем K. Тогда G обладает максимальным K-тором $S \subset G$, который анизотропен над K.*

Прежде чем доказывать теорему 21, отметим, что ее утверждение не выполняется над полем $K = \mathbb{R}$. Действительно, рассмотрим квадратичную форму $f(x_1, \ldots, x_6) = g(x_1, x_2, x_3) - g(x_4, x_5, x_6)$, где $g(x, y, z) = x^2 + y^2 + z^2$. Тогда максимальная компактная подгруппа группы $G_{\mathbb{R}} = \boldsymbol{SO}_6(f)$ имеет вид $\boldsymbol{SO}_3(g) \times \boldsymbol{SO}_3(g)$, т. е. является группой ранга 2. Следовательно, группа G, имеющая ранг 3, не обладает 3-мерным $\mathbb{R}$-анизотропным тором.

Доказательство теоремы 21 использует когомологическую характеризацию всевозможных K-торов группы G. Предполагая группу G присоединенной (это всегда можно сделать с точки зрения доказательства теоремы 21), зафиксируем максимальный K-тор $T \subset G$ и обозначим через $N = N_G(T)$ его нормализатор. Пусть T' — другой максимальный K-определенный тор в группе G. Тогда $T' = gTg^{-1}$ для подходящего $g \in G_{\overline{K}}$. Из K-определенности торов T и T' вытекает, что коцикл $\xi = \{\xi_\sigma\}$, где $\xi_\sigma = g^{-1}\sigma(g)$, $\sigma \in \mathrm{Gal}(\overline{K}/K)$, принимает значения в N и определяет элемент из $M = \mathrm{Ker}(H^1(K, N) \to H^1(K, G))$. При этом T' получается из T скручиванием с помощью ξ, если считать, что N действует на T сопряжениями. Обратно, для любого коцикла $\xi \in Z^1(K, N)$ скрученный тор ${}_\xi T$ является максимальным K-тором в группе ${}_\xi G$. Поэтому ${}_\xi T$ заведомо будет максимальным K-тором в G, если ${}_\xi G = G$, т. е. $\xi \in M$. Тем самым наша задача сводится к отысканию коцикла $\xi \in M$ такого, что скрученный тор ${}_\xi T$ является K-анизотропным.

Пусть $W = N/T$ — соответствующая группа Вейля. Рассматривая W как подгруппу группы $\mathrm{Aut}_{\overline{K}}(T)$ всех автоморфизмов T, можно для любого коцикла $\xi \in Z^1(K, W)$ определить скрученный тор ${}_\xi T$.

Лемма 15. *Существует такой коцикл $\xi \in Z^1(K, W)$, что тор ${}_\xi T$ анизотропен над K.*

Доказательство. Вначале получим сведение к квазиразложимому случаю. Пусть G_0 — квазиразложимая K-группа того же внутреннего типа, что и G, $T_0 \subset G_0$ — максимальный K-тор, содержащий максимальный K-разложимый тор и $f\colon G \to G_0$ — такой $\overline{K}$-определенный изоморфизм, что $f(T) = T_0$. Тогда коцикл $\alpha = \{\alpha_\sigma\}$, где $\alpha_\sigma = f^{-1} \circ \sigma(f)$ для $\sigma \in \mathrm{Gal}(\overline{K}/K)$ со значениями в группе $\mathrm{Int}\, G \simeq G$, на самом деле принимает значения в N. Ясно, что $G_0 = {}_\alpha G$, $T_0 = {}_\alpha T$ и $W_0 = {}_\beta W$, где β — образ α в $Z^1(K, W)$. При этом из свойств скручивания вытекает, что «умножение» на β индуцирует биекцию $Z^1(K, W_0) \simeq Z^1(K, W)$ и

множество торов, получаемых из T_0 скручиванием при помощи коциклов из $Z^1(K, W_0)$, совпадает с множеством торов, получаемых из T скручиванием при помощи коциклов из $Z^1(K, W)$, что и дает требуемую редукцию.

Разберем теперь случай, когда группа G разложима и T — максимальный K-разложимый тор. Тогда группа Галуа $\mathcal{G} = \mathrm{Gal}(\bar{K}/K)$ действует на $\mathbf{X}(T)$ и W тривиально; в частности, коциклы из $Z^1(K, W)$ — это просто (непрерывные) гомоморфизмы ξ: $\mathcal{G} \to W$. Мы будем интерпретировать группу характеров $\mathbf{X}({}_\xi T)$ как группу характеров $\mathbf{X}(T)$, на которой элемент $\sigma \in \mathcal{G}$ действует как автоморфизм ξ_σ^* группы $\mathbf{X}(T)$, отвечающий ξ_σ. Таким образом, нам достаточно построить такой коцикл $\xi = \{\xi_\sigma\}$, что все ξ_σ^* не имеют ненулевых общих неподвижных точек на $\mathbf{X}(T)$ (тогда $\mathbf{X}({}_\xi T)^{\mathcal{G}} = 0$, так что тор ${}_\xi T$ является K-анизотропным). Для этого в системе корней $R = R(T, G)$ рассмотрим некоторую подсистему $\Pi = \{\alpha_1, \ldots, \alpha_r\}$ простых корней и построим элемент Кокстера $w = w_{\alpha_1} \ldots w_{\alpha_r}$, где w_{α_i} — соответствующие отражения; известно (см. Бурбаки [4], гл. V, § 6, n° 2), что w не имеет ненулевых неподвижных точек на $\mathbf{X}(T)$. Пусть d — порядок элемента w (число Кокстера), L/K — неразветвленное расширение степени d, $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. Тогда искомым будет коцикл $\xi \in Z^1(L/K, W)$, задаваемый формулой $\xi_{\sigma^i} = w^i$.

При рассмотрении случая квазиразложимой, но не разложимой группы обозначим через L/K расширение Галуа, группа Галуа которого эффективно действует на диаграмме Дынкина системы R. Для типов ${}^2A_n$, ${}^2D_{2n+1}$, ${}^2E_6$ поле L является квадратичным расширением K. Пусть σ — образующая группы $\mathrm{Gal}(L/K)$. Пользуясь тем обстоятельством, что для групп этих типов $-1 \notin W$ и одновременно $\sigma^* \notin W$ (σ^* — действие σ на $\mathbf{X}(T)$), мы можем определить коцикл $\xi \in Z^1(L/K, W)$ равенством $\xi_\sigma^* = -\sigma^*$. Тогда σ действует на $\mathbf{X}({}_\xi T)$ как $\xi_\sigma^* \circ \sigma^* = -1$ и, следовательно, не имеет ненулевых неподвижных точек.

Для оставшегося типа D_{2n} (включая ${}^3D_4$, ${}^6D_4$) построим квадратичное расширение P/K такое, что $P \cap L = K$, $\mathrm{Gal}(P/K) = \langle\sigma\rangle$ (это всегда возможно, ибо K имеет по крайней мере два квадратичных расширения, а $\mathrm{Gal}(L/K)$ изоморфна подгруппе S_3). Легко видеть, что искомым будет коцикл $\xi \in Z^1(P/K, W)$ такой, что $\xi_\sigma = -1$ (здесь $-1 \in W$). Лемма 15 доказана.

С учетом леммы 15 доказательство теоремы 21 сводится к доказательству следующего утверждения: пусть ρ: $H^1(K, N) \to H^1(K, W)$ — каноническая проекция; тогда существует $\theta \in$

$\in \operatorname{Ker}\left(H^1(K, N) \xrightarrow{\tau} H^1(K, G)\right)$ со свойством $\rho(\theta) = \xi$. Для этого рассмотрим универсальное накрытие $1 \to F \to \tilde{G} \xrightarrow{\pi} G \to 1$, соответствующий кограничный морфизм δ: $H^1(K, G) \to H^2(K, F)$ и построим следующую коммутативную диаграмму:

$$\begin{array}{ccccc} H^1(K, \tilde{G}) & \to & H^1(K, G) & \xrightarrow{\delta} & H^2(K, F) \\ & & \uparrow \tau & & \| \\ & & H^1(K, N) & \xrightarrow{\delta} & H^2(K, F) \end{array}$$

Так как $H^1(K, \tilde{G}) = 1$ (теорема 4), то достаточно установить существование $\theta \in \rho^{-1}(\xi)$ такого, что $\delta(\theta) = 1$. Таким образом, завершает доказательство

Лемма 16. *Пусть коцикл $\xi \in Z^1(K, W)$ таков, что тор ${}_\xi T$ анизотропен. Тогда δ сюръективно отображает $\rho^{-1}(\xi)$ на $H^2(K, F)$.*

Доказательство. Поскольку тор ${}_\xi T$ анизотропен над K, то в силу теоремы 2 для любого конечного расширения L поля K, содержащего поле разложения ${}_\xi T$, имеем $H^2(L/K, {}_\xi T) = \hat{H}^0(L/K, \mathbf{X}({}_\xi T)) = 0$, откуда следует, что $H^2(K, {}_\xi T) = 1$. Поэтому, переходя в точной последовательности $1 \to T \to N \to W \to 1$ к когомологиям, получим, что ξ лежит в образе отображения ρ: $H^1(K, N) \to H^1(K, W)$, т. е. $\rho^{-1}(\xi) \neq \varnothing$.

Пусть $\theta \in \rho^{-1}(\xi)$. Рассмотрим скрученные группы ${}_\theta N$, ${}_\theta T = {}_\xi T$, ${}_\xi W$. Тогда из соображений скручивания вытекает, что утверждение леммы эквивалентно сюръективности отображения δ: $\operatorname{Ker}\left(H^1(K, {}_\theta N) \xrightarrow{\rho'} H^1(K, {}_\xi W)\right) \to H^2(K, F)$ (ясно, что ${}_\theta F = F$, и поэтому мы сохраняем ту же букву для обозначения кограничного морфизма). Имеем коммутативную диаграмму с точной верхней строкой:

$$\begin{array}{ccccc} H^1(K, {}_\theta T) & \to & H^1(K, {}_\theta N) & \xrightarrow{\rho'} & H^1(K, {}_\xi W) \\ \downarrow \delta & & \downarrow \delta & & \\ H^2(K, F) & = & H^2(K, F) & & \end{array}$$

Ясно, что достаточно установить сюръективность отображения $H^1(K, {}_\theta T) \xrightarrow{\delta} H^2(K, F)$. Но это следует из точной последовательности $H^1(K, {}_\theta T) \xrightarrow{\delta} H^2(K, F) \to H^2(K, {}_\theta \tilde{T})$, где $\tilde{T} = \pi^{-1}(T)$, ибо ${}_\theta \tilde{T}$ вместе с ${}_\theta T$ является K-анизотропным, и, следовательно, $H^2(K, {}_\theta \tilde{T}) = 1$. Доказательство завершено.

Доказательство теоремы 20 (случай локального поля). Пусть $S \subset G$ — максимальный тор, анизотропный над K, существова-

ние которого дает теорема 21, $\tilde{S} = \pi^{-1}(S)$. Коммутативная диаграмма

$$\begin{array}{ccccccccc} 1 & \to & F & \to & \tilde{G} & \to & G & \to & 1 \\ & & \| & & \uparrow & & \uparrow & & \\ 1 & \to & F & \to & \tilde{S} & \to & S & \to & 1 \end{array}$$

индуцирует коммутативную когомологическую диаграмму

$$\begin{array}{ccccc} H^1(K, S) & \xrightarrow{\delta} & H^2(K, F) & \to & H^2(K, \tilde{S}) \\ \downarrow & & \| & & \\ H^1(K, G) & \xrightarrow{\delta} & H^2(K, F) & & \end{array}$$

Поскольку тор $\tilde{S}$, вместе с S, анизотропен над K, то $H^2(K, \tilde{S}) = 1$, и, следовательно, отображение δ: $H^1(K, S) \to H^2(K, F)$ сюръективно. Тем более отображение δ: $H^1(K, G) \to H^2(K, F)$ сюръективно.

Для рассмотрения числового случая нам понадобится еще ряд вспомогательных утверждений.

Лемма 17. *Пусть G — полупростая алгебраическая группа, определенная над произвольным полем K характеристики нуль и обладающая подгруппой Бореля над его квадратичным расширением L/K, σ — образующая группы Галуа $\mathrm{Gal}(L/K)$. Тогда существует такая L-определенная подгруппа Бореля $B \subset G$, что пересечение $B \cap B^\sigma$ является максимальным K-определенным тором группы G.*

Доказательство. Рассмотрим K-многообразие $\mathscr{B}$ подгрупп Бореля группы G (см. § 2.4, п. 6) и положим $H = \mathbf{R}_{L/K}(G)$, $X = \mathbf{R}_{L/K}(\mathscr{B})$. Тогда над полем L многообразие X может быть отождествлено с прямым произведением $\mathscr{B} \times \mathscr{B}$; при этом элементам из X_K отвечают пары вида (B, B^σ), где $B \in \mathscr{B}_L$. Так как по условию $\mathscr{B}_L \neq \varnothing$, то $X_K \neq \varnothing$. С другой стороны, X является многообразием подгрупп Бореля группы H, в частности, однородным пространством H. В силу плотности H_K в H (теорема 2.2) отсюда следует плотность X_K в X. Покажем теперь, что подмножество $U \subset X$, состоящее из таких пар (B_1, B_2), что пересечение $B_1 \cap B_2$ является максимальным тором в G, содержит открытое в X подмножество. Тогда пересечение $U \cap X_K$ непусто, и любой его элемент, имеющий вид (B, B^σ), очевидно, доставляет нам искомую подгруппу Бореля B. Для доказательства того, что U содержит открытое подмножество, рассмотрим подмногообразие $Y \subset G \times \mathscr{B} \times \mathscr{B}$, состоящее из точек (g, b_1, b_2), удовлетворяющих условиям $gb_1 = b_1$, $gb_2 = b_2$, и покажем, что множество U может быть охарактеризовано как совокупность таких $y \in \mathscr{B} \times \mathscr{B}$, что размерность слоя $\pi^{-1}(y)$ естественной проекции π: $Y \to \mathscr{B} \times \mathscr{B}$ минимальна; тогда требуемый факт будет вытекать из теоремы о размерности слоев морфизма. Если $y = (b_1, b_2) \in \mathscr{B} \times \mathscr{B}$, то $\pi^{-1}(y) = (B_1 \cap B_2, b_1, b_2)$, где B_i — отве-

чающая точке b_i подгруппа Бореля в G. Известно (см. следствие из теоремы 2.5), что $B_1 \cap B_2$ всегда содержит некоторый максимальный тор T группы G. Поэтому, учитывая тот факт, что пересечение противоположных подгрупп Бореля в точности является тором, получаем, что если $\dim \pi^{-1}(y)$ минимальна, то связная компонента $(B_1 \cap B_2)^0$ является тором. С другой стороны, из разложения $B_1 = TU_1$ в полупрямое произведение получается разложение $B_1 \cap B_2 = T(U_1 \cap B_2)$. Здесь группа $U_1 \cap B_2$ унипотентна, и, следовательно, связна, поэтому пересечение $B_1 \cap B_2$ также связно. Лемма 17 доказана.

Лемма 18. *Пусть G — полупростая односвязная алгебраическая группа над полем $\mathbb{R}$. Тогда существует такой максимальный $\mathbb{R}$-определенный тор $T \subset G$, что $H^2(\mathbb{R}, T) = 1$.*

Доказательство. Пользуясь леммой 17, выберем такую $\mathbb{C}$-определенную подгруппу Бореля $B \subset G$, что $T = B \cap B^\sigma$ — максимальный $\mathbb{R}$-определенный тор в группе G, где σ обозначает комплексное сопряжение. Наша цель — показать, что $H^2(\mathbb{R}, T) = 1$. Для этого рассмотрим систему корней $R = R(T, G)$ и зафиксируем систему простых корней $\Pi \subset R$, ассоциированную с подгруппой Бореля B (см. § 2.1, п. 10). Так как группа G односвязна, то группа $\mathbf{X}_*(T)$ кохарактеров тора T имеет базис, состоящий из двойственных корней $\alpha^\vee$ для $\alpha \in \Pi$, множество которых мы обозначим через $\Pi^\vee$. Поскольку пересечение $B \cap B^\sigma$ совпадает с T, то подгруппа B^σ является противоположной к B, и, следовательно, $\sigma^*(\Pi) = -\Pi$, $\sigma^*(\Pi^\vee) = -\Pi^\vee$ (σ^* означает индуцированное действие σ на характерах и кохарактерах). Таким образом, для $\alpha^\vee \in \Pi^\vee$ имеем либо $\sigma^*(\alpha^\vee) = -\alpha^\vee$, либо $\sigma^*(\alpha^\vee) = -\beta^\vee$ для некоторого $\beta^\vee \in \Pi^\vee$, $\beta^\vee \neq \alpha^\vee$. Пользуясь этим свойством базиса группы $\mathbf{X}_*(T)$, легко получить, что $\hat{H}^0(\mathbb{R}, \mathbf{X}_*(T)) = 0$. А тогда из локальной теоремы Накаямы — Тейта вытекает, что $H^2(\mathbb{R}, T) = 1$. Лемма 18 доказана.

Доказательство теоремы 20 (случай числового поля). Установим вначале, что образ $\rho_v(x)$ фиксированного элемента $x \in H^2(K, F)$ при отображении ограничения ρ_v: $H^2(K, F) \to H^2(K_v, F)$ тривиален для почти всех $v \in V_f^K$. Действительно, x лежит в образе отображения инфляции $H^2(L/K, F) \to H^2(K, F)$, где L/K — подходящее конечное расширение поля K. Для почти всех $v \in V_f^K$ расширение L_w/K_v неразветвлено, и тогда $\rho_v(x)$ попадает в образ отображения инфляции $H^2(K_v^{\text{нр}}/K_v, F) \to H^2(K_v, F)$. Но $H^2(K_v^{\text{нр}}/K_v, F) = 1$, ибо $\mathrm{Gal}(K_v^{\text{нр}}/K_v) \simeq \hat{\mathbb{Z}}$ — группа когомологической размерности 1, поэтому $\rho_v(x) = 1$, что и требовалось. Обозначим через S конечное подмножество в V^K, содержащее по крайней мере одно неархимедово нормирование и все те v, для которых $\rho_v(x) \neq 1$. Для каждого $v \in S$ можно выбрать такой максимальный K_v-определенный тор $\tilde{T}_v \subset \tilde{G}$, что

$H^2(K_v, \tilde{T}_v) = 1$. Действительно, если v неархимедово, то достаточно взять максимальный K_v-анизотропный тор $\tilde{T}_v \subset \tilde{G}$ (см. теорему 21), а для архимедова v следует воспользоваться леммой 18. Используя свойство слабой аппроксимации для многообразия торов (см. следствие 3 в § 7.1), найдем K-определенный тор $\tilde{T} \subset \tilde{G}$, который над K_v изоморфен $\tilde{T}_v$ (отметим, что доказательство существования такого тора в гл. VII не использует никаких результатов гл. VI). Положим $T = \pi(\tilde{T})$. Очевидно, нам достаточно показать, что x лежит в образе когранничного морфизма δ: $H^1(K, T) \to H^2(K, F)$, отвечающего точной последовательности $1 \to F \to \tilde{T} \to T \to 1$. Имеем коммутативную диаграмму с точными строками

$$\begin{array}{ccccc}
H^1(K, T) & \xrightarrow{\delta} & H^2(K, F) & \xrightarrow{\tau} & H^2(K, \tilde{T}) \\
\downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\rho} & & \downarrow{\scriptstyle\gamma} \\
\prod\limits_v H^1(K_v, T) & \xrightarrow{\mu} & \prod\limits_v H^2(K_v, F) & \xrightarrow{\eta} & \prod\limits_v H^2(K_v, \tilde{T})
\end{array}$$

Так как условия $x \in \operatorname{Im}\delta$ и $x \in \operatorname{Ker}\tau$ равносильны, то проверим второе из них. Имеем $\gamma(\tau(x)) = \eta(\rho(x)) = 1$, ибо для тех v, что $\rho_v(x) \neq 1$, по построению $H^2(K_v, \tilde{T}) = 1$. Но поскольку S содержит неархимедово нормирование v_0 и тор $\tilde{T}$ является K_{v_0}-анизотропным, то из предложения 12 вытекает, что $\operatorname{Ker}\gamma$ тривиально, и поэтому $\tau(x) = 1$. Теорема 20 доказана.

Отметим, что теорема 20 заключает в себе существенную арифметическую информацию. Так, для группы $G = \boldsymbol{PSL}_n$ фундаментальная группа F совпадает с группой μ_n корней степени n из единицы. Тогда в силу леммы 2.6 $H^2(K, F) = \operatorname{Br}(K)_n$ — подгруппа элементов группы Брауэра $\operatorname{Br}(K)$, аннулируемых умножением на n. При этом легко видеть, что образ отображения $H^1(K, G) \xrightarrow{\delta} H^2(K, F)$ состоит из элементов $\operatorname{Br}(K)_n$, представляемых простой алгеброй размерности n^2. Поэтому утверждение о сюръективности δ для локальных и числовых полей в действительности эквивалентно глубокому утверждению о том, что над этими полями экспонента простой алгебры совпадает с ее индексом (см. § 1.4, п. 1).

Для дальнейшего нам понадобится явное вычисление когомологий центров односвязных групп. Ясно, что структура центра как модуля над группой Галуа одинакова для групп одного и того же внутреннего типа, причем для простых групп мы имеем следующую таблицу, в которой L/K означает расширение Галуа поля K, группа Галуа которого эффективно действует на соответствующей диаграмме Дынкина:

Тип G	$Z(G)$	Тип G	$Z(G)$
${}^1A_{n-1}$	μ_n	${}^3D_4$	$\mathbf{R}^{(1)}_{L/K}(\mu_2)$
${}^2A_{n-1}$	$\mathbf{R}^{(1)}_{L/K}(\mu_n)$	${}^6D_4$	$\mathbf{R}^{(1)}_{P/K}(\mu_2)$
B_n, C_n, E_7	μ_2	${}^1E_6$	μ_3
${}^1D_n$	μ_4, $n=2k+1$, $\mu_2\times\mu_2$, $n=2k$	${}^2E_6$	$\mathbf{R}^{(1)}_{L/K}(\mu_3)$
${}^2D_n$	$\mathbf{R}^{(1)}_{L/K}(\mu_4)$, $n=2k+1$ $\mathbf{R}_{L/K}(\mu_2)$, $n=2k$	E_8, F_4, G_2	1

(здесь для типа ${}^6D_4$ через P обозначено подполе в L, имеющее степень три над K).

Когомологии группы μ_n нам хорошо известны (лемма 2.6):

$$H^1(K,\ \mu_n)=K^*/K^{*n},\quad H^2(K,\ \mu_n)=\mathrm{Br}\,(K)_n.$$

Когомологии группы $\mathbf{R}^{(1)}_{L/K}(\mu_n)$ вычисляются исходя из точной последовательности $1\to\mathbf{R}^{(1)}_{L/K}(\mu_n)\to\mathbf{R}_{L/K}(\mu_n)\xrightarrow{N}\mu_n\to 1$. Переходя к когомологиям, получим точную последовательность

$$\mathbf{R}_{L/K}(\mu_n)_K\xrightarrow{N}(\mu_n)_K\to H^1(K,\ \mathbf{R}^{(1)}_{L/K}(\mu_n))\to H^1(K,\ \mathbf{R}_{L/K}(\mu_n))\to$$
$$\to H^1(K,\ \mu_n)\to H^2(K,\ \mathbf{R}^{(1)}_{L/K}(\mu_n))\to H^2(K,\ \mathbf{R}_{L/K}(\mu_n))\to H^2(K,\ \mu_n).$$

Таким образом, группы $H^i(K,\ \mathbf{R}^{(1)}_{L/K}(\mu_n))$ $(i=1,2)$ входят в точные последовательности

$$1\to(\mu_n)_K/N_{L/K}((\mu_n)_L)\to$$
$$\to H^1(K,\ \mathbf{R}^{(1)}_{L/K}(\mu_n))\to\mathrm{Ker}\,(L^*/L^{*n}\xrightarrow{N}K^*/K^{*n})\to 1,\qquad(1)$$

$$1\to K^*/K^{*n}N_{L/K}(L^*)\to$$
$$\to H^2(K,\ \mathbf{R}^{(1)}_{L/K}(\mu_n))\to\mathrm{Ker}\,(\mathrm{Br}\,(L)_n\xrightarrow{N}\mathrm{Br}\,(K)_n)\to 1.\qquad(2)$$

Используя (2), вычислим в явном виде группы $H^2(K,\ Z)$, где Z — центр односвязной группы одного из типов ${}^{3,6}D_4$, ${}^2E_6$, т. е. когда $Z=\mathbf{R}^{(1)}_{L/K}(\mu_2)$, $\mathbf{R}^{(1)}_{P/K}(\mu_2)$ или $\mathbf{R}^{(1)}_{L/K}(\mu_3)$ в обозначениях приведенной выше таблицы. Для этого заметим, что если n взаимно просто со степенью расширения L/K, то $K^*=K^{*n}N_{L/K}(L^*)$, и поэтому соответствующий член в (2) тривиален (именно так обстоит дело в разбираемых нами случаях). Покажем теперь,

что для локального поля K группа $B = \mathrm{Ker}\,(\mathrm{Br}\,(L)_n \xrightarrow{N} \mathrm{Br}\,(K)_n)$ тривиальна. Разберем сперва случай типа ${}^{3,6}D_4$, т. е. когда $Z = \mathbf{R}^{(1)}_{L/K}(\mu_2)$, где L/K — любое расширение степени 3, и покажем, что в этом случае отображение $\mathrm{Br}\,(L)_2 \xrightarrow{N} \mathrm{Br}\,(K)_2$ является изоморфизмом. Сквозное отображение $\mathrm{Br}\,(K)_2 \xrightarrow{i} \mathrm{Br}\,(L)_2 \xrightarrow{N} \mathrm{Br}\,(K)_2$, где i индуцировано расширением основного поля, является умножением на 3 и поэтому совпадает с тождественным. Так как $[\mathrm{Br}\,(K)_2] = [\mathrm{Br}\,(L)_2] = 2$, то i — изоморфизм, следовательно, N — тоже изоморфизм, что и требовалось. Пусть теперь $Z = \mathbf{R}^{(1)}_{L/K}(\mu_3)$, где L/K — квадратичное расширение (случай группы типа ${}^2E_6$). Тогда элементы из B отвечают классам простых алгебр над L экспоненты 3, которые обладают такой инволюцией τ второго рода, что поле неподвижных элементов L^τ совпадает с K. Известно (см. Алберт [1], гл. X), что над локальным полем нетривиальных простых алгебр с инволюцией второго рода не существует, и поэтому в рассматриваемом случае опять $B = 1$. Итак, над локальным полем для указанных типов $H^2(K, Z) = 1$.

Пусть теперь K — числовое поле. Покажем, что здесь для любого элемента $x \in H^2(K, Z)$ найдется расширение E/K, имеющее степень 2 для типов ${}^{3,6}D_4$ и степень 3 для ${}^2E_6$ такое, что образ x при отображении ограничения $H^2(K, Z) \to H^2(E, Z)$ тривиален. Рассмотрим отвечающий x элемент $y \in B$ и представляющую его алгебру с делением $D \in \mathrm{Br}\,(L)$. Обозначим через $\bar{S}$ конечное подмножество в V^L, состоящее из тех w, для которых алгебра $D_w = D \otimes_L L_w$ нетривиальна, и пусть S состоит из ограничений нормирований из $\bar{S}$ на K. Предположим теперь, что мы имеем дело со случаем групп типов ${}^{3,6}D_4$. Тогда $[L : K] = 3$, и поэтому $[L_w : K_v] \leqslant 3$ для любого $v \in V^K$. Отсюда легко вытекает существование такого квадратичного расширения E/K, что $[EL_w : L_w] = 2$ для всех $w \in \bar{S}$. Тогда из п. 1 § 1.5 вытекает, что EL является полем разложения для D, и поэтому расширение E искомое. В случае типа ${}^2E_6$ ясно, что D является алгеброй над L с инволюцией второго рода, поэтому из отсутствия таких алгебр над локальными полями вытекает, что $L \subset K_v$ для $v \in S$. Легко видеть, что существует кубическое расширение $E = K(\sqrt[3]{d})$, обладающее свойством: $[E_w : K_v] = 3$ для всех $v \in S$. Тогда, как и выше, заключаем, что E искомое. Более того, используя теорему Грюнвальда — Ванга из теории полей классов (см. Артин, Тейт [1]), можно показать, что всегда существует циклическое расширение K степени 3 с описанным свойством. Соберем полученные результаты.

Предложение 14. *Пусть Z — центр простой односвязной K-группы одного из типов ${}^{3,6}D_4$, ${}^2E_6$. Тогда*

1) *если K — локальное поле, то $H^2(K, Z) = 1$;*

2) *если K — числовое поле, то для любого $x \in H^2(K, Z)$ найдется такое расширение E/K, имеющее степень 2 для типов ${}^{3,6}D_4$ и степень 3 для типа ${}^2E_6$, что образ x при отображении ограничения $H^2(K, Z) \to H^2(E, Z)$ тривиален (более того, для типа ${}^2E_6$ можно выбрать циклическое расширение E/K степени 3 с таким свойством).*

Покажем теперь, как предложение 14 применяется для выяснения структуры групп указанных типов. Пусть G_0 — соответствующая односвязная квазиразложимая группа, $Z = Z(G_0)$ — ее центр и $\bar{G}_0 = G_0/Z$ — присоединенная группа. Тогда элементы множества $H^1(K, \bar{G}_0)$ классифицируют с точностью до K-изоморфизма простые односвязные группы, относящиеся к тому же внутреннему типу, что и G_0. В частности, группа $G = {}_\xi G_0$, отвечающая коциклу $\xi \in H^1(K, \bar{G}_0)$, квазиразложима над K в том и только том случае, если коцикл ξ тривиален, и становится квазиразложимой над расширением E поля K, если тривиален образ ξ при отображении ограничения $H^1(K, \bar{G}_0) \to H^1(E, \bar{G}_0)$. Множество $H^1(K, \bar{G}_0)$ входит в точную последовательность

$$H^1(K, G_0) \to H^1(K, \bar{G}_0) \xrightarrow{\delta} H^2(K, Z).$$

Предположим теперь, что K — локальное поле и множество $H^1(K, G_0)$ тривиально (мы намеренно не пользуемся теоремой 4 в полном объеме). Тогда отображение δ имеет тривиальное ядро. С другой стороны, согласно утверждению 1) предложения 14 $H^2(K, Z) = 1$. Поэтому $H^1(K, \bar{G}_0) = 1$, и, значит, любая группа, относящаяся к типам ${}^{3,6}D_4$, ${}^2E_6$, квазиразложима над K.

Пусть теперь K — числовое поле. Предположим, что уже известна тривиальность $H^1(P, G_0)$ для любого вполне мнимого расширения P/K (мы опять не пользуемся теоремой 6 в полном объеме). Тогда, замечая, что расширение E в утверждении 2) предложения 14 можно для типов ${}^{3,6}D_4$ выбрать вполне мнимым, мы окончательно приходим к следующему утверждению.

Предложение 15. *Пусть G_0 — односвязная квазиразложимая группа одного из типов: ${}^{3,6}D_4$, ${}^2E_6$ над неархимедовым локальным либо числовым полем K. Предположим, что известна тривиальность $H^1(K, G_0)$ для локального поля K и тривиальность $H^1(P, G_0)$ для любого вполне мнимого расширения числового поля K. Тогда*

1) *если поле K локально, то любая K-группа одного из указанных типов квазиразложима;*

2) *если K — числовое поле, то любая K-группа одного из типов ${}^{3,6}D_4$ становится квазиразложимой над некоторым квадратичным расширением K;*

3) *если K — вполне мнимое числовое поле, то любая K-группа типа ${}^2E_6$ становится квазиразложимой над некоторым (циклическим) расширением K степени три.*

Установим теперь следующий важный в структурном плане факт, который будет играть ключевую роль в § 9.4 при изучении нормального строения групп рациональных точек.

Предложение 16. *Пусть G_0 — односвязная разложимая группа одного из типов: B_n, C_n, E_7, E_8, F_4, G_2 над неархимедовым локальным либо числовым полем K. Предположим, что известна тривиальность $H^1(P, G_0)$ для локального поля K и тривиальность $H^1(P, G_0)$ для любого вполне мнимого расширения P числового поля K. Тогда*

1) *любая K-группа одного из типов E_8, F_4, G_2 является K-разложимой, если поле K локальное, и разложимой над любым вполне мнимым расширением K, если поле K числовое;*

2) *любая K-группа одного из типов B_n, C_n, E_7 становится разложимой над подходящим квадратичным расширением L/K, которое в числовой ситуации является вполне мнимым.*

В частности, любая группа одного из указанных типов разложима над подходящим квадратичным расширением L/K.

Доказательство. Диаграммы Дынкина групп указанных типов не имеют нетривиальных симметрий, поэтому их K-формы классифицируются элементами множества $H^1(K, \overline{G}_0)$, где $\overline{G}_0$ — соответствующая присоединенная группа. Так как для типов, указанных в п. 1), $G_0 = \overline{G}_0$, то отсюда без труда следует требуемое утверждение. Для групп оставшихся типов $Z(G_0) = \mu_2$, и, значит, $H^2(K, Z) = \mathrm{Br}(K)_2$, так что любой элемент $x \in H^2(K, Z)$ становится тривиальным над некоторым квадратичным расширением L/K, которое в числовом случае можно считать вполне мнимым. Тогда из точной последовательности

$$H^1(L, G_0) \to H^1(L, \overline{G}_0) \to H^2(L, Z)$$

мы и получаем требуемое утверждение.

Ознакомившись с формулировками предложений 15 и 16, читатель, по-видимому, испытал чувство некоторого недоумения по поводу содержащейся в них «непоследовательности»: а именно, предполагая всюду в этом параграфе выполненными теоремы 4 и 6, мы в этих двух предложениях почему-то ограничиваемся более слабым требованием о тривиальности $H^1(K, G_0)$ для квазиразложимой группы G над локальным или вполне мнимым числовым полем K. Причина этого заключается в том, что сами предложения 15 и 16 оказываются вплетенными в сложную схему доказательства теорем 4 и 6, причем их приходится использовать именно в той ситуации, которая описана в их формулировках. Нет нужды отмечать, что после доказательства теорем 4 и 6 предложения 15 и 16 превращаются из условных утверждений в безусловные.

Вернемся теперь к обсуждению принципа Хассе для полупростых групп. В предыдущем параграфе мы видели, что он

выполняется не всегда, однако теорема 6 утверждает его выполнимость для односвязных групп. Покажем, что он также справедлив для другого «крайнего» случая — присоединенных групп.

Теорема 22. *Пусть G — полупростая присоединенная группа над числовым полем K. Тогда* $Ш(G) = 1$.

Доказательство. Ясно, что достаточно рассмотреть случай простой группы G. Обозначим через $\pi\colon \tilde{G} \to G$ универсальное накрытие, и пусть $Z = \operatorname{Ker} \pi$ — его ядро. Имеем следующую коммутативную диаграмму с точными строками:

$$\begin{array}{ccccccc}
H^1(K, Z) & \xrightarrow{\alpha_1} & H^1(K, \tilde{G}) & \xrightarrow{\alpha_2} & H^1(K, G) & \xrightarrow{\alpha_3} & H^2(K, Z) \\
\downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle \gamma_2} & & \downarrow{\scriptstyle \gamma_3} & & \downarrow{\scriptstyle \gamma_4} \\
\prod\limits_v H^1(K_v, Z) & \xrightarrow{\beta_1} & \prod\limits_v H^1(K_v, \tilde{G}) & \xrightarrow{\beta_2} & \prod\limits_v H^1(K_v, G) & \xrightarrow{\beta_3} & \prod\limits_v H^2(K_v, Z)
\end{array} \tag{3}$$

Лемма 19. $\operatorname{Ker} \gamma_4 = 1$.

Доказательство. Если $Z = \mu_n$, то γ_4 превращается в каноническое отображение $\operatorname{Br}(K)_n \to \prod\limits_v \operatorname{Br}(K_v)_n$, которое инъективно по теореме Хассе — Брауэра — Нётер (см. теорему 1.12 в § 1.5). Пусть теперь $Z = R^{(1)}_{L/K}(\mu_n)$. Тогда из последовательности (2) получаем следующую коммутативную диаграмму с точными строками:

$$\begin{array}{l}
1 \longrightarrow K^*/K^{*n} N_{L/K}(L^*) \xrightarrow{\varepsilon_1} \\
\qquad\qquad\qquad\qquad \downarrow{\scriptstyle \eta_1} \\
1 \to \prod\limits_v K_v^*/K_v^{*n} N_{L/K}\left(\left(L \bigotimes\limits_K K_v\right)^*\right) \xrightarrow{\theta_1} \\
\qquad \xrightarrow{\varepsilon_1} H^2(K, Z) \xrightarrow{\varepsilon_2} \operatorname{Ker}\left(\operatorname{Br}(L) \xrightarrow{N_{L/K}} \operatorname{Br}(K)\right) \to 1 \\
\qquad\qquad \downarrow{\scriptstyle \eta_2 = \gamma_4} \qquad\qquad\qquad \downarrow{\scriptstyle \eta_3} \\
\qquad \xrightarrow{\theta_1} \prod\limits_v H^2(K_v, Z) \xrightarrow{\theta_2} \prod\limits_v \operatorname{Ker}\left(\sum\limits_{w \mid v} \operatorname{Br}(L_w) \xrightarrow{N_{L/K}} \operatorname{Br}(K_v)\right) \to 1
\end{array}$$

Опять по теореме Хассе — Брауэра — Нётер $\operatorname{Ker} \eta_3 = 1$. Отсюда следует, что если $x \in \operatorname{Ker} \eta_2$, то $x = \varepsilon_1(y)$, где $y \in \operatorname{Ker} \eta_1$. Поэтому остается показать, что в нашей ситуации $\operatorname{Ker} \eta_1 = 1$. Пусть вначале L/K — квадратичное расширение. Тогда при нечетном n группа $K^*/K^{*n} N_{L/K}(L^*)$ тривиальна, и доказывать нечего. Наоборот, $K^{*n} \subset N_{L/K}(L^*)$ при четном n, так что η_1 сводится к отображению $K^*/N_{L/K}(L^*) \to \prod\limits_v K_v^*/N_{L/K}\left(\left(L \bigotimes\limits_K K_v\right)^*\right)$, которое инъективно в силу того, что для L/K выполняется норменный принцип Хассе (см. следствие из теоремы 11). Из приведенной выше

таблицы вытекает, что остается рассмотреть случай $n=2$, L/K — расширение третьей степени. Тогда опять $K^*/K^{*n}N_{L/K}(L^*)=1$, и доказательство леммы 19 завершено.

Пусть теперь $x\in \operatorname{Ker}\gamma_3$ в обозначениях диаграммы (3). Тогда $\alpha_3(x)\in \operatorname{Ker}\gamma_4$, так что в силу леммы 19 $\alpha_3(x)$ тривиально. Из точности верхней строки в (3) вытекает, что $x\in \operatorname{Im}\alpha_2$, т. е. $x=\alpha_2(y)$, $y\in H^1(K,\tilde{G})$. Рассмотрим $\gamma_2(y)$. Из точности нижней строки в диаграмме (3), ее коммутативности и условия $x\in \operatorname{Ker}\gamma_3$ легко получить, что $\gamma_2(y)\in \operatorname{Im}\beta_1$, т. е. $\gamma_2(y)=\beta_1(z)$, $z=(z_v)\in\prod_v H^1(K_v, Z)$. Воспользуемся теперь тем фактом, что отображение $H^1(K, Z)\xrightarrow{\varphi}\prod_{v\in V_\infty^K} H^1(K_v, Z)$ сюръективно (см. следствие 2 из предложения 7.7; естественно, что приводимое в гл. VII доказательство этого утверждения не зависит от теоремы 22). Тогда можно выбрать $a\in H^1(K,Z)$ со свойством $\varphi(a)=(z_v)_{v\in V_\infty^K}$. Из тривиальности $H^1(K_v, \tilde{G})$ для $v\in V_f^K$ (теорема 4) и наших построений вытекает, что $\gamma_2(\alpha_1(a))=\gamma_2(y)$. Но, используя теорему 6 (принцип Хассе для $\tilde{G}$), отсюда получаем, что $y=\alpha_1(a)$, и тогда $x=\alpha_2(y)=\alpha_2(\alpha_1(a))=1$. Теорема 22 доказана.

Замечание. На самом деле мы показали, что принцип Хассе выполняется для полупростой группы G, если для ее фундаментальной группы F отображение $H^2(K, F)\to\prod_v H^2(K_v, F)$ инъективно. В частности, это всегда имеет место, если $F=\mu_2$. Мы воспользуемся этим замечанием в следующем параграфе применительно к ортогональным и унитарным группам.

Чтобы не перегружать последующие параграфы, посвященные доказательству принципа Хассе, приведем здесь редукцию теоремы 6 к доказательству равенства $Ш(G)=1$ для полупростой односвязной группы G над числовым полем K. Эту редукцию дает следующее

Предложение 17. *Пусть G — связная группа над числовым полем K. Тогда отображение $H^1(K, G)\to\prod_{v\in V_\infty^K} H^1(K_v, G)$ сюръективно.*

Доказательство. Для торов мы установим этот факт в гл. VII (см. следствие 2 в § 7.3), не используя, естественно, результатов настоящего параграфа. Поэтому сейчас покажем, как общий случай сводится к торам. С этой целью прежде всего убедимся, что для любой связной вещественной алгебраической группы G наперед заданный элемент $\xi\in H^1(\mathbb{R}, G)$ лежит в образе отображения $H^1(\mathbb{R},T)\to H^1(\mathbb{R}, G)$ для подходящего $\mathbb{R}$-определенного максимального тора $T\subset G$. Действительно, коцикл $\xi=$

$=\{\xi_\tau\}$ определяется заданием элемента $z=\xi_\sigma\in G_{\mathbb{C}}$, где σ означает комплексное сопряжение, причем $z\sigma(z)=1$. Рассмотрим разложение Жордана $z=z_s z_u$. Тогда легко видеть, что имеют место соотношения $z_s\sigma(z_s)=1$, $z_u\sigma(z_u)=1$, т. е. полупростая и унипотентная части z также определяют коциклы. Хорошо известно, что минимальная алгебраическая группа U, порожденная z_u, изоморфна аддитивной группе $\boldsymbol{G}_a$, причем из соотношения $z_u\sigma(z_u)=1$, очевидно, вытекает, что эта группа $\mathbb{R}$-определена. Так как $H^1(\mathbb{R}, U)=1$ (лемма 2.7), то, используя перестановочность z_s с любым элементом из U, легко показать, что ξ эквивалентен коциклу θ, определяемому элементом $t=z_s$. Далее, рассмотрим связную компоненту H^0 централизатора $H=Z_G(t)$. Поскольку $\sigma(t)=t^{-1}$, то группы H и H^0 определены над $\mathbb{R}$. Известно (см. Борель [8], § 11), что $t\in H^0$. С другой стороны, H^0 обладает максимальным $\mathbb{R}$-определенным тором T, который будет максимальным и в G. Но поскольку t централен в H^0, то $t\in T$, и, значит, θ лежит в образе отображения $H^1(\mathbb{R}, T)\to H^1(\mathbb{R}, G)$.

Пусть теперь $\xi=(\xi_v)\in\prod\limits_{v\in V_\infty^K} H^1(K_v, G)$. Согласно уже доказанному, для каждого $v\in V_\infty^K$ можно выбрать K_v-определенный максимальный тор $T_v\subset G$ такой, что $\xi_v\in \operatorname{Im}(H^1(K_v, T_v)\to H^1(K_v, G))$. Как уже отмечалось, мы вправе использовать здесь следствие 3 из предложения 7.3, в результате чего найдем такой максимальный K-определенный тор $T\subset G$, который G_{K_v}-сопряжен тору T_v над каждым K_v $(v\in V_\infty^K)$. Легко видеть, что если коцикл $\theta\in H^1(\mathbb{R}, G)$ определяется элементом $z\in G_{\mathbb{C}}$, то для любого $g\in G_{\mathbb{R}}$ элемент gzg^{-1} определяет коцикл, эквивалентный исходному. Отсюда следует, что образы отображений $H^1(K_v, T)\to H^1(K_v, G)$ и $H^1(K_v, T_v)\to H^1(K_v, G)$ совпадают для любого $v\in V_\infty^K$. А тогда ξ лежит в образе сквозного отображения $H^1(K, T)\xrightarrow{\alpha}\prod\limits_{v\in V_\infty^K} H^1(K_v, T)\to\prod\limits_{v\in V_\infty^K} H^1(K_v, G)$, ибо мы считаем уже установленным, что α сюръективно. Предложение 17 доказано.

В § 6.7—6.8 мы приведем доказательство теорем 4 и 6. Рассуждения в этих параграфах являются многоэтапными и используют самую разнообразную технику, начиная с арифметических свойств полуторалинейных форм и кончая весьма тонкими результатами из теории алгебраических групп и алгебраической теории чисел. Свойствам форм мы посвятим специальный § 6.6, а здесь укажем на необходимые нам для дальнейшего когомологические следствия одной теоремы Стейнберга.

Теорема 23 (Стейнберг [1]). *Пусть G_0 — полупростая односвязная группа, определенная и квазиразложимая над* (*совер-*

шенным) полем K. Тогда любой K-определенный класс сопряженности полупростых элементов в G_0 обладает K-рациональной точкой.

Мы будем использовать не саму теорему Стейнберга, а вытекающие из нее когомологические следствия.

Предложение 18. *Пусть G_0 — полупростая K-определенная квазиразложимая группа (не обязательно односвязная), $\xi \in Z^1(K, G_0)$ и $G = {}_\xi G_0$ — соответствующая скрученная группа. Тогда для любого максимального K-определенного тора $T \subset G$ найдется такой коцикл $\mu \in Z^1(K, T)$, что $G_0 = {}_\mu G$.*

Доказательство. В силу теоремы Ленга наше утверждение тривиальным образом выполняется для конечного поля K, поэтому в дальнейшем мы будем считать K бесконечным. Пусть π_0: $\tilde{G}_0 \to G_0$ — универсальное K-определенное накрытие. Применяя скручивание при помощи ξ, мы получим универсальное K-определенное накрытие π: $\tilde{G} \to G$. Будем интерпретировать группу $\tilde{G}_{\bar{K}}$ как группу $(\tilde{G}_0)_{\bar{K}}$, на которой группа Галуа $\mathrm{Gal}(\bar{K}/K)$ действует скрученным образом: $\sigma^*(x) = \tilde{a}_\sigma \sigma(x) \tilde{a}_\sigma^{-1}$ для любых $\sigma \in \mathrm{Gal}(\bar{K}/K)$, $x \in (\tilde{G}_0)_{\bar{K}} = \tilde{G}_{\bar{K}}$, где $\xi = \{a_\sigma\}$ и $\tilde{a}_\sigma$ — произвольный прообраз a_σ. Положим $\tilde{T} = \pi^{-1}(T)$ и зафиксируем произвольный регулярный элемент $x \in \tilde{T}_K$. Тогда $\sigma^*(x) = x$ для всех $\sigma \in \mathrm{Gal}(\bar{K}/K)$, т. е. $\sigma(x) = \tilde{a}_\sigma^{-1} x \tilde{a}_\sigma$. Отсюда следует, что класс сопряженности $C = \{gxg^{-1} \mid g \in \tilde{G}_0\}$ определен над K. Поэтому согласно теореме Стейнберга $C_K \neq \varnothing$, т. е. найдется такой $y \in (\tilde{G}_0)_{\bar{K}}$, что $\sigma(yxy^{-1}) = yxy^{-1}$. Тогда имеем $yxy^{-1} = \sigma(y) \tilde{a}_\sigma^{-1} x \tilde{a}_\sigma \sigma(y)^{-1}$, откуда в силу регулярности x получаем, что $y^{-1}\sigma(y)\tilde{a}_\sigma^{-1} \in \tilde{T}_{\bar{K}}$, и, значит, $z^{-1}\sigma(z) a_\sigma^{-1} \in T_{\bar{K}}$ для $z = \pi_0(y)$. Ясно, что G_0 получается из G скручиванием при помощи коцикла $\{a_\sigma^{-1}\} \in Z^1(K, G)$. Рассмотрим эквивалентный ему коцикл $\mu = \{b_\sigma\}$, где $b_\sigma = z^{-1} a_\sigma^{-1} \sigma^*(z)$, и покажем, что $b_\sigma \in T_{\bar{K}}$ для всех $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Действительно,

$$b_\sigma = z^{-1} a_\sigma^{-1} \sigma^*(z) = z^{-1} a_\sigma^{-1} (a_\sigma \sigma(z) a_\sigma^{-1}) = z^{-1} \sigma(z) a_\sigma^{-1} \in T_{\bar{K}},$$

и предложение доказано.

Бывает полезной также следующая (фактически эквивалентная) переформулировка предложения 18.

Предложение 19. *Пусть G_0, ξ и G как в предложении 18. Тогда любой максимальный K-определенный тор $T \subset G$ допускает K-определенное вложение в G_0, и при этом ξ лежит в образе отображения $H^1(K, T) \to H^1(K, G_0)$.*

Для доказательства сохраним обозначения, введенные при доказательстве предложения 18. Мы установили существование

такого $y \in (\tilde{G}_0)_{\bar{K}}$, что $yxy^{-1} = \sigma(y)\,\tilde{a}_\sigma^{-1} x \tilde{a}_\sigma \sigma(y)^{-1}$. Тогда для $z = \pi_0(y)$ получаем $a'_\sigma = z a_\sigma \sigma(z)^{-1} \in T' = Z_{G_0}(\pi_0(yxy^{-1}))$. Так как T', будучи централизатором регулярного полупростого элемента $\pi_0(yxy^{-1}) \in (G_0)_K$, является K-определенным максимальным тором в G_0 и коцикл $\xi' = \{a'_\sigma\}$ эквивалентен исходному, то остается показать, что изоморфизм $T \xrightarrow{\sim} T'$, задаваемый отображением φ: $t \mapsto ztz^{-1}$, определен над K. Для этого достаточно установить, что φ коммутирует с любым $\sigma \in \mathrm{Gal}(\bar{K}/K)$, который действует как σ на T' и как σ^* на T. Имеем:

$$\varphi(\sigma^*(t)) = z a_\sigma \sigma(t)\, a_\sigma^{-1} z^{-1} =$$
$$= z a_\sigma \sigma(z)^{-1}\, \sigma(ztz^{-1})\, \sigma(z)\, a_\sigma^{-1} z^{-1} = \sigma(ztz^{-1}) = \sigma(\varphi(t))$$

для любого $t \in T_{\bar{K}}$, ибо $a'_\sigma = z a_\sigma \sigma(z)^{-1} \in T'$, что и требовалось.

Из предложений 18 и 19 вытекает следующее любопытное наблюдение: если G — полупростая K-определенная группа, G_0 — квазиразложимая K-группа того же внутреннего типа, то любой K-определенный максимальный тор $T \subset G$ допускает K-определенное вложение в G_0. (Тем самым квазиразложимая группа является универсальным вместилищем всех K-определенных торов, встречающихся в K-группах данного внутреннего типа.) Действительно, пусть ρ: $G \to \bar{G}$ — изогения на соответствующую присоединенную группу. Так как G получается из G_0 скручиванием при помощи коцикла $\xi \in H^1(K, \bar{G}_0)$, то в силу предложения 18 найдется такой коцикл $\mu \in H^1(K, \rho(T))$, что $G_0 = {}_\mu G$. Но компоненты μ действуют на T тривиально, и поэтому $T = {}_\mu T$ является максимальным K-тором в $G_0 = {}_\mu G$.

Вот один необходимый для дальнейшего пример использования этого утверждения. Пусть L — либо квадратичное расширение поля K, либо алгебра $K \oplus K$. Обозначим через $*$ инволюцию L, которая совпадает с нетривиальным автоморфизмом расширения L/K в первом случае и переставляет слагаемые во втором. Далее, рассмотрим алгебру $A = M_n(L)$ и обозначим через τ инволюцию алгебры A, определяемую формулой

$$\tau((x_{ij})) = f\,(x^*_{ji})\,f^{-1},$$

где

$$f = \begin{pmatrix} 0 & E_{n/2} \\ E_{n/2} & 0 \end{pmatrix}$$

в случае четного n, и

$$f = \begin{pmatrix} 0 & E_{(n-1)/2} & 0 \\ E_{(n-1)/2} & 0 & \vdots \\ 0 & \dots & 1 \end{pmatrix}$$

в случае нечетного n,

$$E_l = \begin{pmatrix} 1 & \dots & 0 \\ \cdot & \ddots & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ 0 & \dots & 1 \end{pmatrix}$$

— единичная матрица соответствующего размера, причем 1 в случае $L = K \oplus K$ понимается как $(1, 1)$. Тогда соответствующая специальная унитарная группа $G_0 = \boldsymbol{SU}(A, \tau)$ является квазиразложимой группой типа ${}^2A_{n-1}$ в случае $[L : K] = 2$ и изоморфна $\boldsymbol{SL}_n$ в случае $L = K \oplus K$ (см. § 2.3). Покажем, что любая коммутативная полупростая алгебра B над L степени n, снабженная инволюцией σ, ограничение которой на L совпадает с $*$, вкладывается в (A, τ) как алгебра с инволюцией. Действительно, используя регулярное представление, вложим B в A как алгебру без инволюции. Далее, продолжим σ до инволюции всей алгебры A (см. Алберт [1], гл. X) и будем обозначать продолжение той же буквой. Пусть $G = \boldsymbol{SU}(A, \sigma)$ — соответствующая унитарная группа. Тогда пересечение $T = (B \otimes_K \bar{K}) \cap G$ является максимальным K-определенным тором в G. Из предыдущего вытекает, что $G_0 = {}_\mu G$ для подходящего коцикла $\mu \in Z^1(K, \bar{G})$, тривиально действующего на T. Ясно, что элементы из $\bar{G} = \operatorname{Int} G$ действуют как автоморфизмы алгебры (A, σ), и $(A, \tau) = {}_\mu(A, \sigma)$. При этом μ действует тривиально на B, так что $(B, \sigma) = {}_\mu(B, \sigma) \hookrightarrow (A, \tau)$.

Предложение 19 будет использоваться нами в сочетании с некоторыми фактами о когомологической размерности. Мы напоминаем лишь основные относящиеся к этому результаты, отсылая за доказательствами и сопутствующими деталями к книге Серра [1]. Пусть p — простое число. Говорят, что *когомологическая размерность* $\operatorname{cd}_p(\mathcal{G})$ проконечной группы $\mathcal{G}$ относительно p не превосходит единицы ($\operatorname{cd}_p(\mathcal{G}) \leqslant 1$), если для любого конечного $\mathcal{G}$-модуля A группа $H^2(\mathcal{G}, A)$ не имеет p-кручения. При этом $\operatorname{cd}(\mathcal{G}) \leqslant 1$, если $\operatorname{cd}_p(\mathcal{G}) \leqslant 1$ для любого p. Соответственно $\operatorname{cd}_p(K) \leqslant 1$ для совершенного поля K, если $\operatorname{cd}_p(\mathcal{G}) \leqslant 1$ для абсолютной группы Галуа $\mathcal{G} = \operatorname{Gal}(\bar{K}/K)$, и $\operatorname{cd}(K) \leqslant 1$, если $\operatorname{cd}_p(K) \leqslant 1$ для любого p. В случае когда $p \neq \operatorname{char} K$ (у нас, как правило, $\operatorname{char} K = 0$), можно дать переформулировку условия $\operatorname{cd}_p(K) \leqslant 1$ в терминах теорий полей: оно оказывается эквивалентным тривиальности p-компоненты $\operatorname{Br}(L)_p$ группы Брауэра любого конечного расширения L/K. Отсюда получаются важные для нас примеры полей с условием $\operatorname{cd}_p(K) \leqslant 1$.

Предложение 20. *Пусть K — локальное либо числовое поле, Π — некоторое множество простых чисел. Обозначим через K_Π поле, получаемое присоединением к K всех корней из единицы,*

степени которых делятся лишь на простые числа из Π. *Тогда* $\mathrm{cd}_p(K_\Pi) \leqslant 1$ *для любого* $p \in \Pi$.

Доказательство вытекает из того факта, что любая алгебра с делением индекса n над конечным расширением L поля K имеет поле разложения вида $L(\zeta_{n^a})$, где ζ_m — корень степени m из единицы. (Ср. доказательство предложения 9 на с. 101 в книге Серра [1].)

Лемма 20. *Пусть* $\mathrm{cd}_p(K) \leqslant 1$. *Тогда для любого* K*-определенного тора* T *группа* $H^1(K, T)$ *не имеет* p*-кручения. В частности, если* $\mathrm{cd}(K) \leqslant 1$, *то* $H^1(K, T) = 1$.

Доказательство. Покажем вначале, что для произвольного K-тора S группа $H^2(K, S)$ не имеет p-кручения. Для этого рассмотрим точную последовательность $1 \to S_p \to S \xrightarrow{[p]} S \to 1$, где $[p]$ означает возведение в p-ю степень, $S_p = \mathrm{Ker}\,[p]$. Ей отвечает точная когомологическая последовательность

$$\ldots \to H^2(K,\ S_p) \to H^2(K,\ S) \xrightarrow{[p]} H^2(K,\ S),$$

откуда следует, что $H^2(K, S_p)$ накрывает все элементы порядка p в $H^2(K, S)$. Но $H^2(K, S_p) = 1$, ибо группа $H^2(K, S_p)$ одновременно должна аннулироваться умножением на p и не иметь p-кручения в силу условия $\mathrm{cd}_p(K) \leqslant 1$, откуда $H^2(K, S)_p = 1$. Вложим теперь исходный тор T в точную последовательность $1 \to S \to F \to T \to 1$, где S и F — K-торы, причем тор F квазиразложим (см. предложение 2.2). Тогда из точной последовательности

$$1 = H^1(K,\ F) \to H^1(K,\ T) \to H^2(K,\ S)$$

и предыдущего замечания вытекает, что $H^1(K, T)_p = 1$. Лемма доказана.

Изложенные результаты позволяют распространить на поля, когомологическая размерность которых не превосходит единицы, теорему Ленга о тривиальности когомологий связных групп над конечными полями (такие поля K, очевидно, удовлетворяют условию $\mathrm{cd}_p(K) \leqslant 1$).

Теорема 24 (Стейнберг [1]). *Если* $\mathrm{cd}(K) \leqslant 1$, *то* $H^1(K, G) = 1$ *для любой связной* K*-определенной алгебраической группы* G.

Действительно, можно ограничиться случаем редуктивной группы G. Пусть $H = [G, G]$ — ее полупростая часть. Тогда $T = G/H$ — тор, и из точной последовательности $H^1(K, H) \to H^1(K, G) \to H^1(K, T)$, используя лемму 20, получаем, что тривиальность $H^1(K, G)$ вытекает из тривиальности $H^1(K, H)$. Тем самым, имеется редукция доказательства теоремы 24 к полупростому случаю. Обозначим через G_0 квазиразложимую K-группу того же внутреннего типа. Из предложения 19 и леммы 20 вытекает тривиальность $H^1(K, B)$ для любой полупростой квазиразложимой над K группы B. Применяя это утверждение к со-

ответствующей присоединенной группе $\bar{G}_0$, получаем, что существует лишь одна K-форма данного внутреннего типа, т. е. $G = \bar{G}_0$ — квазиразложимая группа. Но тогда, как мы уже выяснили, $H^1(K, G) = 1$. Теорема 24 доказана.

§ 6.6. Когомологии Галуа и квадратичные, эрмитовы и другие формы

В этом параграфе мы изложим необходимые нам для дальнейшего арифметические свойства полуторалинейных форм и дадим их интерпретацию на языке когомологий Галуа. С другой стороны, мы покажем, что с помощью принципа Хассе можно дать локально-глобальную классификацию форм. К основным результатам этого параграфа следует также отнести доказательство теоремы 5 и аналогичного результата для чисто мнимых числовых полей.

Вначале разберем наиболее популярный и наглядный случай квадратичных форм. Пусть f — невырожденная K-определенная квадратичная форма на n-мерном векторном пространстве W. Тогда f представляет нуль над K, т. е. уравнение $f(x) = 0$ имеет ненулевое решение $x \in W_K$ в том и только том случае, если это имеет место над всеми пополнениями K_v, $v \in V^K$ (теорема Минковского — Хассе, см. п. 3 § 2.2). При этом если $n \geqslant 5$, то f автоматически представляет нуль над всеми неархимедовыми пополнениями K_v, $v \in V_f^K$ (теорема Мейера). Таким образом, здесь, в частности, выполняется следующее

Утверждение 1. *Пусть f — невырожденная n-мерная квадратичная форма над локальным либо числовым полем K, причем $n \geqslant 5$. Тогда f представляет нуль, если поле K локально или если K — числовое поле и f представляет нуль над всеми K_v, $v \in V_\infty^K$.*

Иногда бывает удобна также следующая эквивалентная переформулировка.

Утверждение 1′. *Пусть f — такая же как в утверждении 1, $n \geqslant 4$ и $a \in K^*$. Тогда f представляет a над K, т. е. уравнение $f(x) = a$ имеет решение $x \in W_K$, в том и только том случае, если это имеет место над всеми K_v, $v \in V_\infty^K$.*

Для удобства ссылок сформулируем также соответствующее утверждение для случая эрмитовых форм, связанных либо с квадратичным расширением L/K, либо с телом кватернионов D/K, непосредственно сводящееся к случаю квадратичных форм. А именно, пусть W — n-мерное векторное пространство соответственно над L или D, f — невырожденная σ-эрмитова форма на W, где σ соответственно — нетривиальный автоморфизм L/K либо каноническая инволюция D. Будем говорить, что f представляет нуль над K, если уравнение $f(x) = 0$ имеет ненулевое решение в W, и над K_v — если решение существует в простран-

стве $W \otimes_K K_v$. Аналогично определяется представимость формой f эрмитова элемента $a \in L^*, D^*$ (отметим, что в нашей ситуации множество эрмитовых элементов совпадает с K^*). Тогда имеет место

Утверждение 2. *В описанной ситуации предположим дополнительно, что $n \geqslant 3$ в случае квадратичного расширения L/K и $n \geqslant 2$ в случае тела кватернионов D. Тогда f представляет нуль, если либо поле K локально, либо K — числовое поле и f представляет нуль над всеми K_v для $v \in V_\infty^K$.*

Действительно, в ортогональном базисе пространства W форма f имеет соответственно вид $f(x_1, \ldots, x_n) = a_1 N_{L/K}(x_1) + \ldots + a_n N_{L/K}(x_n)$ или $f(x_1, \ldots, x_n) = a_1 \operatorname{Nrd}_{D/K}(x_1) + \ldots + a_n \operatorname{Nrd}_{D/K}(x_n)$, где $a_i \in K$, т. е. значения f совпадают со значениями квадратичной формы размерности $2n$ (соответственно $4n$), поэтому все следует из утверждения 1. Отметим также, что в данной ситуации имеется очевидный аналог утверждения 1′ для представимости формой f элемента $a \in K^*$, в котором нижние границы для размерностей уменьшаются по сравнению с утверждением 2 на единицу.

Осталось рассмотреть случай косоэрмитовой формы f, заданной на n-мерном векторном пространстве W над телом кватернионов D. Как обычно, будем говорить, что косоэрмитов элемент $a \in D^*$ представляется формой f над K (соответственно, над K_v), если уравнение $f(x) = a$ имеет решение $x \in W$ (соответственно, $x \in W \otimes_K K_v$). Отметим, что понятие представимости нуля над формами такого типа имеет свои тонкости: если $D \otimes_K K_v \simeq M_2(K_v)$, то следует требовать не просто существования ненулевого решения уравнения $f(x) = 0$, а такого решения $x \in W \otimes_K K_v$, которое может быть включено в базис $W \otimes_K K_v$ как модуля над $D \otimes_K K_v$; это условие в действительности эквивалентно тому, что ранг над K_v квадратичной формы $\tilde{f}$, отвечающей f, не меньше 2. Мы не будем здесь обсуждать подробности, которые заинтересованный читатель может найти в книге Шарлау [1], гл. 10.

Утверждение 3. *Пусть f — невырожденная косоэрмитова форма над телом кватернионов D с центром K размерности $n \geqslant 3$. Тогда f представляет косоэрмитов элемент $a \in D^*$, если либо поле K локально, либо K — числовое поле и f представляет a над всеми пополнениями K_v, $v \in V_\infty^K$.*

Обычное доказательство этого утверждения см. в книге Шарлау [1], гл. 10. Мы же сейчас покажем, что оно на самом деле вытекает из справедливости теорем 4 и 6 для групп типов $A_1 \times A_1$ и A_3. Так как в следующем параграфе эти теоремы для групп типа A_n будут доказаны без использования утверждения 3, то это даст полное его доказательство, независимое от других источников.

Рассмотрим вначале случай локального поля K; при этом без ограничения общности можно считать, что $n=3$. Построим вначале 3-мерную косоэрмитову форму g над D, которая заведомо представляет a и имеет тот же дискриминант, что и форма f. Будем искать матрицу g в виде $\operatorname{diag}(a, b, c)$. Из утверждения 1 (см. также § 1.4, п. 3) вытекает, что $\operatorname{Nrd}_{D/K}(D^*)=K^*$, в частности, можно найти такой элемент $d\in D^*$, что $\operatorname{Nrd}_{D/K}(d)=d(f)\operatorname{Nrd}_{D/K}(a)$, где $d(f)$ — дискриминант формы f. Рассмотрим, далее, пространство $P=\{x\in D\mid \sigma(x)=-x\}$ «чистых» кватернионов. Легко видеть, что $\dim_K P=3$, откуда следует, что $dP\cap P\neq(0)$. Тогда найдутся элементы $b, c\in P$ со свойством $db^{-1}=c$, которые и будут искомыми.

В силу предложения 2.16 форма f получается из формы g скручиванием при помощи коцикла $\xi\in H^1(K, G)$, где $G=\mathbf{SU}_3(g)$. Обозначим через H стабилизатор в G вектора $t=(1, 0, 0)$ пространства D^3, на котором определена форма g. Тогда из теоремы Витта (см. § 2.4, п. 5) вытекает, что фактор-пространство G/H может быть отождествлено со «сферой» $S_g=\{x\in D^3\otimes_K \bar{K}\mid g(x)=a\}$. Из определений также легко следует, что «скрученное» пространство ${}_\xi(G/H)$ относительно действия G на G/H левыми сдвигами совпадает со сферой $S_f=\{x\in W\otimes_K \otimes_K \bar{K}\mid f(x)=a\}$. Поэтому, как следует из леммы 1.6, $(S_f)_K\neq\varnothing$ в том и только том случае, если ξ лежит в образе отображения ε: $H^1(K, H)\to H^1(K, G)$, и нам достаточно показать, что в нашей ситуации отображение ε сюръективно. Для этого заметим, что группы G и H являются полупростыми группами типов $D_3=A_3$ и $D_2=A_1\times A_1$ соответственно (см. § 2.3), причем их универсальные накрывающие $\tilde{G}$ и $\tilde{H}$ согласованы в том смысле, что имеет место коммутативная диаграмма

$$\begin{array}{ccccccccc} 1 & \to & F & \to & \tilde{G} & \to & G & \to & 1 \\ & & \| & & \uparrow & & \uparrow & & \\ 1 & \to & F & \to & \tilde{H} & \to & H & \to & 1 \end{array} \qquad (1)$$

где $F=\{\pm 1\}$. Из (1) получается коммутативная когомологическая диаграмма

$$\begin{array}{ccc} H^1(K, G) & \xrightarrow{\delta_G} & H^2(K, F) \\ \uparrow{\scriptstyle\varepsilon} & & \| \\ H^1(K, H) & \xrightarrow{\delta_H} & H^2(K, F) \end{array}$$

Так как мы предполагаем теорему 4 доказанной для групп типов D_3 и D_2, то в сочетании с теоремой 20 этот факт позволяет утверждать, что отображения δ_G и δ_H являются биекциями. Поэтому отображение ε также биективно, что и требовалось.

Рассуждения для числового поля аналогичны, однако отличаются некоторыми деталями, связанными с наличием веще-

ственных нормирований (для вполне мнимых полей приведенные рассуждения проходят без всяких изменений). Прежде всего получим редукцию к случаю $n=3$. По условию для каждого $v \in V_\infty^K$ можно найти такой $x_v \in W \otimes_K K_v$, что $f(x_v)=a$. Из слабой аппроксимационной теоремы для поля K вытекает наличие слабой аппроксимации и в пространстве W, так что по соображениям непрерывности существует такой $x \in W$, что $f(x) \in \{ya\sigma(y) \mid y \in D_v^*\}$ для всех $v \in V_\infty^K$. Обозначим через W' трехмерное подпространство в W, содержащее x и такое, что ограничение f' формы f на W' невырождено. Тогда, очевидно, из существования решения уравнения $f'(x)=a$ вытекает существование решения уравнения $f(x)=a$. Итак, в дальнейшем $\dim f=3$. Далее, при построении формы g, представляющей a и имеющей тот же дискриминант, что и f, следует заметить, что, с одной стороны,

$$\mathrm{Nrd}_{D/K}(D^*)=K^* \cap \left(\bigcap_{v \in V_\infty^K} \mathrm{Nrd}_{D_v/K_v}(D_v^*)\right)$$

(следует из утверждения 1 или теоремы 1.13), с другой — что $d(f)/\mathrm{Nrd}_{D/K}(a) \in \mathrm{Nrd}_{D_v/K_v}(D_v^*)$ для $v \in V_\infty^K$, ибо a представимо над всеми K_v, $v \in V_\infty^K$. Найдя $d \in D^*$ со свойством $\mathrm{Nrd}_{D/K}(d)=d(f)/\mathrm{Nrd}_{D/K}(a)$ и рассуждая как и выше, мы осуществим выбор матрицы искомой формы g в виде $\mathrm{diag}(a, b, c)$. Пусть опять $G=SU_3(g)$, $\xi \in H^1(K, G)$ — коцикл, скручивание при помощи которого переводит форму g в f. Из рассуждений в локальном случае вытекает, что наша задача переформулируется на языке когомологий Галуа следующим образом: пусть $\xi \in H^1(K, G)$, причем известно, что для всех $v \in V_\infty^K$ образ ξ_v коцикла ξ в $H^1(K_v, G)$ лежит в $\mathrm{Im}\left(H^1(K_v, H) \xrightarrow{\varepsilon_v} H^1(K_v, G)\right)$; требуется показать, что $\xi \in \mathrm{Im}(H^1(K, H) \xrightarrow{\varepsilon} H^1(K, G))$. Для этого снова рассмотрим получающуюся из (1) коммутативную когомологическую диаграмму с точными строками

$$\begin{array}{ccccc} H^1(K, \tilde{G}) & \xrightarrow{\gamma} & H^1(K, G) & \xrightarrow{\delta_G} & H^2(K, F) \\ \uparrow{\scriptstyle\beta} & & \uparrow{\scriptstyle\varepsilon} & & \| \\ H^1(K, \tilde{H}) & \xrightarrow{\alpha} & H^1(K, H) & \xrightarrow{\delta_H} & H^2(K, F) \end{array} \qquad (2)$$

Так как отображение δ_H сюръективно (теорема 20), то найдется такой коцикл $\eta \in H^1(K, H)$, что $\delta_H(\eta)=\delta_G(\xi)$. Скручивая диаграмму (2) при помощи коцикла η, мы сведем нашу задачу к случаю $\delta_G(\xi)=1$, что мы и будем в дальнейшем предполагать, не изменяя обозначений (т. е. не переходя от H к ${}_\eta H$ и т. д.). Тогда $\xi=\gamma(\theta)$ для подходящего $\theta \in H^1(K, \tilde{G})$. Далее, по условию для каждого $v \in V_\infty^K$ можно найти такой коцикл

$\mu_v \in H^1(K_v, H)$, что $\xi_v = \varepsilon_v(\mu_v)$. Выписав диаграмму, аналогичную (2), но построенную для поля K_v и воспользовавшись условием $\delta_G(\xi) = 1$, получим, что $\mu_v = \alpha_v(\omega_v)$, $\omega_v \in H^1(K_v, \tilde{H})$. Так как $\gamma_v(\theta_v) = \gamma_v(\beta_v(\omega_v))$, то $\beta_v(\omega_v) = f_v\theta_v$ для подходящего $f_v \in H^1(K_v, F)$. Используя сюръективность отображения $K^*/K^{*2} = H^1(K, F) \to \prod_{v \in V_\infty^K} H^1(K_v, F) = \prod_{v \in V_\infty^K} K_v^*/K_v^{*2}$, найдем элемент $f \in H^1(K, F)$ отображающийся в $(f_v)_{v \in V_\infty^K}$. «Подправляя» θ на элемент f, можно без ограничения общности предполагать, что $\beta_v(\omega_v) = \theta_v$ для всех $v \in V_\infty^K$. Рассмотрим теперь коммутативную диаграмму

$$\begin{array}{ccc} H^1(K, \tilde{G}) & \xrightarrow{\rho_{\tilde{G}}} & \prod\limits_{v \in V_\infty^K} H^1(K_v, \tilde{G}) \\ \uparrow \beta & & \uparrow \Pi\beta_v \\ H^1(K, \tilde{H}) & \xrightarrow{\rho_{\tilde{H}}} & \prod\limits_{v \in V_\infty^K} H^1(K_v, \tilde{H}) \end{array}$$

Применяя к группам $\tilde{G}$ и $\tilde{H}$, которые относятся к типам A_3 и $A_1 \times A_1$ соответственно, теорему 6, получим, что отображения $\rho_{\tilde{G}}$ и $\rho_{\tilde{H}}$ являются биекциями. В частности, можно найти (единственный) элемент $\omega \in H^1(K, \tilde{H})$ такой, что $\rho_{\tilde{H}}(\omega) = (\omega_v)_{v \in V_\infty^K}$. Тогда $\rho_{\tilde{G}}(\beta(\omega)) = \rho_{\tilde{G}}(\theta)$, и поэтому $\beta(\omega) = \theta$. Возвращаясь к диаграмме (2), будем иметь $\xi = \gamma(\theta) = \gamma(\beta(\omega)) = \varepsilon(\alpha(\omega))$, т. е. $\xi \in \operatorname{Im} \varepsilon$. Утверждение 3 полностью доказано.

Рассуждения, использованные при доказательстве утверждения 3, допускают обращение. Более точно, предполагая известными определенные свойства полуторалинейных форм, можно получить доказательство теорем 4 и 6 для ассоциированных с ними односвязных алгебраических групп. Именно на этом принципе будет основано доказательство этих теорем для групп классических типов, отличных от A_n, которое мы проведем в следующем параграфе. Отметим, что тип A_n рассматривается отдельно, и поэтому, доказывая теоремы 4 и 6 для групп типа D_n, мы вправе использовать утверждение 3, ибо его доказательство опиралось только на справедливость этих теорем для групп типов A_3 и $A_1 \times A_1$.

Обсудим теперь еще один аспект связи между арифметикой полуторалинейных форм и когомологиями Галуа алгебраических групп над локальными и числовыми полями. Речь идет о проблеме эквивалентности форм одного и того же типа. Эта проблема естественно распадается на две проблемы: (1) классификация форм над локальными полями (включая поля $\mathbb{R}$ и

$\mathbb{C}$); (2) обоснование возможности локально-глобального перехода, т. е. вывода из эквивалентности двух K-форм f и g над всеми пополнениями K_v их эквивалентности над полем K. В случае когда утверждение (2) имеет место, говорят, что для форм данного типа выполняется *слабый принцип Хассе*, в отличие от *сильного принципа Хассе*, заключающегося в локально-глобальной трактовке вопроса о представимости нуля (или другого элемента). Отметим, что сильный принцип Хассе, вообще говоря, не имеет прямой и универсальной когомологической интерпретации, о чем свидетельствует, в частности, когомологическое доказательство утверждения 3. С точки зрения теории алгебраических групп задача заключается в исследовании когомологическими методами принципа Хассе для однородных пространств алгебраических групп. К сожалению, на сегодняшний день эта задача еще не получила своего полного решения, хотя потребность в нем ощущается уже давно. Укажем только, что принцип Хассе для так называемых «симметрических пространств» исследован в работе Рапинчука [5].

В отличие от сильного принципа Хассе, слабый принцип имеет вполне четкую и практически очевидную трактовку: так как K-формы того же типа, что и f, классифицируются элементами множества $H^1(K, G)$, где G — соответствующая ортогональная (унитарная) группа (предложение 2.16), то вопрос о справедливости в данной ситуации локально-глобального принципа равносилен вопросу об инъективности отображения

$$H^1(K, G) \to \prod_v H^1(K_v, G).$$

В качестве примера конкретных вычислений (и результатов) рассмотрим случаи квадратичных форм и косоэрмитовых форм над телами кватернионов.

Пусть f — невырожденная n-мерная квадратичная форма над числовым полем K. Тогда множество классов K-эквивалентности невырожденных n-мерных квадратичных форм над K находится в биективном соответствии с элементами множества $H^1(K, \boldsymbol{O}_n(f))$, где $\boldsymbol{O}_n(f)$ — соответствующая ортогональная группа. Так как группа $\boldsymbol{O}_n(f)$ не является связной, то к ней непосредственно не применимы полученные нами результаты. Для перехода к связной группе $\boldsymbol{SO}_n(f)$ рассмотрим точную последовательность

$$1 \to \boldsymbol{SO}_n(f) \to \boldsymbol{O}_n(f) \xrightarrow{\det} \mu_2 \to 1, \tag{3}$$

где det обозначает гомоморфизм взятия определителя, $\mu_2 = \{\pm 1\}$. Последовательности (3) отвечает точная когомологическая последовательность

$$\boldsymbol{O}_n(f) \xrightarrow{\det} \mu_2 \to H^1(K, \boldsymbol{SO}_n(f)) \xrightarrow{\varphi} H^1(K, \boldsymbol{O}_n(f)) \xrightarrow{\psi} H^1(K, \mu_2).$$

Отображение det: $\boldsymbol{O}_n(f) \to \mu_2$, очевидно, сюръективно, и поэтому отображение φ имеет тривиальное ядро. Так как это верно для всех квадратичных форм, то, применяя стандартные соображения скручивания, получим, что φ инъективно. Далее, если отождествить $H^1(K, \mu_2)$ с K^*/K^{*2}, то читатель легко получит следующее описание ψ: если $\xi \in H^1(K, \boldsymbol{O}_n(f))$ — некоторый класс когомологий и $[g]$ — отвечающий ему класс эквивалентности невырожденных n-мерных квадратичных форм, то $\psi(\xi)$ совпадает с образом в группе K^*/K^{*2} элемента $d(g)/d(f)$, где d означает дискриминант. Таким образом, слой отображения ψ состоит из классов форм с фиксированным дискриминантом. В частности, мы еще раз получаем, что элементы $H^1(K, \boldsymbol{SO}_n(f))$ классифицируют классы эквивалентности n-мерных невырожденных форм, имеющих тот же дискриминант, что и f. Ясно, что если формы f и g эквивалентны над всеми K_v, то элемент $d = d(g)/d(f)$ всюду локально является квадратом, а поэтому является квадратом и в K. Тем самым локально эквивалентные формы имеют одинаковый дискриминант. Когомологическая интерпретация этого факта получается из диаграммы

$$\begin{array}{ccc} H^1(K, \boldsymbol{O}_n(f)) & \xrightarrow{\psi} & H^1(K, \mu_2) \\ \downarrow \rho & & \downarrow \theta \\ \prod_v H^1(K_v, \boldsymbol{O}_n(f)) & \to & \prod_v H^1(K_v, \mu_2) \end{array}$$

Тогда θ инъективно, так что из $\rho(\xi_1) = \rho(\xi_2)$ вытекает $\psi(\xi_1) = \psi(\xi_2)$, что и требовалось. Эти рассуждения показывают, что для обоснования слабого принципа Хассе нам достаточно исследовать на инъективность отображение μ: $H^1(K, G) \to \prod_v H^1(K_v, G)$, где $G = \boldsymbol{SO}_n(f)$. В случае $n = 2$ группа G является одномерным тором, причем $G \simeq \boldsymbol{G}_m$, если форма f изотропна над K (т. е. $-d(f) \in K^{*2}$), и $G \cong \mathbf{R}^{(1)}_{L/K}(\boldsymbol{G}_m)$, если форма f анизотропна над K (т. е. $-d(f) \notin K^{*2}$), где $L = K(\sqrt{-d(f)})$. Поэтому из теоремы Хассе о нормах вытекает инъективность μ.

Пусть теперь $n \geqslant 3$. Тогда группа G является полупростой, и ее фундаментальная группа F изоморфна μ_2. Поэтому из замечания, сделанного после доказательства теоремы 22, вытекает, что отображение μ здесь также инъективно. Таким образом, для квадратичных форм выполняется слабый принцип Хассе. Поэтому чтобы завершить их классификацию, остается решить соответствующую локальную задачу. Будем рассматривать формы одного и того же дискриминанта d над полем K_v, классы эквивалентности которых отвечают элементам множества

$H^1(K_v, G)$. Рассмотрим вначале случай $n=2$. Тогда если $-d \in K_v^{*2}$, то $G = \boldsymbol{G}_m$ и $H^1(K_v, G) = 1$, т. е. в данном случае все формы эквивалентны, скажем, форме $f(x, y) = xy$. Если же $-d \notin K_v^{*2}$, то $G = \mathbf{R}_{L/K}^{(1)}(\boldsymbol{G}_m)$, $L = K(\sqrt{-d})$, так что $H^1(K_v, G) = K_v^*/N_{L/K_v}(L^*)$ имеет порядок 2. Представителями двух классов эквивалентности являются формы $f_1 = x^2 + dy^2$, $f_2 = ax^2 + \frac{d}{a}y^2$, где $a \in K_v^*$ и символ Гильберта $(a, -d)_v$ равен -1. Таким образом, здесь полную систему инвариантов квадратичной формы f образуют ее дискриминант $d(f)$ и так называемый *инвариант Хассе—Витта* $\varepsilon_v(f)$, который по определению равен символу Гильберта $(a, b)_v$, если $f = ax^2 + by^2$ $\left(\text{заметим, что } \varepsilon(f_1) = (1, d)_v = 1,\ \varepsilon(f_2) = \left(a, \frac{d}{a}\right)_v = (a, -d)_v = -1\right)$. Пусть теперь $n \geqslant 3$ и $v \in V_f^K$. Тогда из теоремы 20 вытекает, что имеет место биекция $H^1(K_v, G) \xrightarrow{\delta_v} H^2(K_v, \mu_2)$. Если отождествить группу $H^2(K_v, \mu_2) = \mathrm{Br}(K_v)_2$ с $\{\pm 1\}$, то можно показать, что отображение δ_v задается формулой $\delta_v([g]) = \varepsilon_v(g)/\varepsilon_v(f)$, где $\varepsilon_v(f)$, $\varepsilon_v(g)$ — *инварианты Хассе — Витта* форм f и g соответственно (напомним, что для $h = a_1x_1^2 + \ldots + a_nx_n^2$ по определению полагают $\varepsilon_v(h) = \prod_{i<j}(a_i, a_j)_v$). При этом доказательство формулы для δ_v читатель может найти у Спрингера [1]. Получается, что и в случае $n \geqslant 3$ класс эквивалентности квадратичной формы f вполне характеризуется заданием дискриминанта $d(f)$ и инварианта $\varepsilon_v(f)$. Обратно, для любых значений $d \in K_v^*/K_v^{*2}$ и $\varepsilon = \pm 1$, подчиняющихся единственному ограничению: $\varepsilon = 1$, если $-d \in K_v^{*2}$ при $n = 2$, найдется n-мерная квадратичная форма f над K_v, имеющая такие инварианты.

Остается дать интерпретацию для элементов множества $H^1(\mathbb{R}, G)$. Ограничимся для простоты формами положительного дискриминанта, и тогда можно считать, что $f = x_1^2 + \ldots + x_n^2$. В этом случае описание $H^1(\mathbb{R}, G)$ нетрудно извлечь из теоремы 17. А именно, предположим для определенности, что $n = 2l$ — четное число и возьмем в качестве максимального $\mathbb{R}$-определенного тора $T \subset G$ тор $T = \boldsymbol{SO}_2(g_1) \times \ldots \times \boldsymbol{SO}_2(g_l)$, где $g_i = x_{2i-1}^2 + x_{2i}^2$. Тогда множество T_2 элементов порядка 2 в T можно отождествить с множеством $D = \{\mathrm{diag}(\varepsilon_1, \ldots, \varepsilon_l) \mid \varepsilon_i = \pm 1\}$. При этом орбиты действия группы Вейля $W = W(T, G)$ на T_2 совпадают с орбитами естественного действия симметрической группы S_l на D. Тем самым класс эквива-

лентности в D/S_l определяется числами r и s тех ε_i, которые соответственно равны $+1$ и -1 (ясно, что $r+s=l$). С другой стороны, легко видеть, что форма, отвечающая классу с представителем $\operatorname{diag}(\varepsilon_1, \ldots, \varepsilon_l)$, где $\varepsilon_1 = \ldots = \varepsilon_r = -1$, $\varepsilon_{r+1} = \ldots = \varepsilon_l = 1$, имеет вид $f_r = -x_1^2 - \ldots - x_{2r}^2 + x_{2r+1}^2 + \ldots + x_n^2$, и мы приходим к хорошо известной классификации вещественных форм при помощи сигнатуры.

Упражнение. Используя теорему 18, получить аналогичную интерпретацию для элементов множества $H^1(\mathbb{R}, \boldsymbol{SO}_n(f))$, где $d(f) = -1$.

Подводя итоги нашего обсуждения, можно констатировать, что класс эквивалентности n-мерной квадратичной формы над числовым полем K характеризуется

1) дискриминантом $d(f)$,

2) инвариантами Хассе — Витта $\varepsilon_v(f)$ для $v \in V_f^K$,

3) сигнатурами (r_v, s_v) для вещественных $v \in V_\infty^K$.

Отметим, что не все эти инварианты являются независимыми; в частности, из теоремы 1.12 вытекает, что $\varepsilon_v(f) = 1$ для почти всех $v \in V_f^K$ и $\prod\limits_v \varepsilon_v(f) = 1$ (произведение берется по всем v, включая архимедовы). Обратно, для любого набора инвариантов, подчиняющихся этим и некоторым другим простым условиям, найдется квадратичная форма с заданными инвариантами. Подробное изложение этой теории читатель сможет найти в книгах О'Миры [1] и Шарлау [1]; блестящим введением является глава 4 в книге Серра [8].

Перейдем к рассмотрению косоэрмитовых форм над телом кватернионов D. Пусть f — невырожденная косоэрмитова форма размерности n, $G = \boldsymbol{SU}_n(f)$ — соответствующая специальная унитарная группа. Тогда G при $n=1$ является одномерным тором вида $\mathbf{R}_{L/K}^{(1)}(\boldsymbol{G}_m)$, где $L \subset D$ — некоторое максимальное подполе, а при $n \geqslant 2$ G — полупростая группа, фундаментальная группа которой изоморфна μ_2. В обоих случаях для G выполняется принцип Хассе. Отсюда следует, что в данной ситуации справедлив слабый принцип Хассе для собственной эквивалентности: две косоэрмитовы формы f и g собственно эквивалентны (т. е. переводятся друг в друга матрицей из $SL_n(D)$) в том и только том случае, если это имеет место над всеми пополнениями K_v. Однако нас интересует обычная эквивалентность форм, и поэтому от когомологий группы $\boldsymbol{SU}_n(f)$ надо перейти к когомологиям всей унитарной группы $\boldsymbol{U}_n(f)$. Нам понадобится следующее известное утверждение (см. Кнезер [12]).

Лемма 21. $U_n(f) = SU_n(f)$.

Рассмотрим точную последовательность $1 \to \boldsymbol{SU}_n(f) \to \boldsymbol{U}_n(f) \xrightarrow{\mathrm{Nrd}} \mu_2 \to 1$ и соответствующую ей точную когомологи-

ческую последовательность

$$U_n(f) \xrightarrow{\mathrm{Nrd}} \mu_2 \xrightarrow{\varepsilon} H^1(K,\ \boldsymbol{SU}_n(f)) \xrightarrow{\varphi} H^1(K,\ \boldsymbol{U}_n(f)) \xrightarrow{\psi} H^1(K,\ \mu_2). \tag{4}$$

Из леммы 21 вытекает, что $\varepsilon(\mu_2) = \operatorname{Ker}\varphi$ состоит из двух элементов, в частности, φ никогда не бывает инъективным. Тем не менее, используя последовательность (4), можно получить полную классификацию косоэрмитовых форм над локальным полем K. А именно, поскольку G при $n \geqslant 2$ является полупростой группой с фундаментальной группой μ_2, а при $n = 1$ — одномерным тором $\mathbf{R}^{(1)}_{L/K}(\boldsymbol{G}_m)$, где L/K — квадратичное расширение, то здесь $H^1(K, \boldsymbol{SU}_n(f))$ состоит из двух элементов, а следовательно, совпадает с $\operatorname{Ker}\varphi$. Отсюда, применяя скручивание, получаем, что ψ инъективно. Таким образом, над локальным полем класс эквивалентности косоэрмитовой формы однозначно определяется своим дискриминантом, причем дискриминант может принимать произвольные значения, если $n \geqslant 2$, и значения, не принадлежащие $-K^{*2}$, если $n = 1$.

Покажем теперь, что слабый принцип Хассе для эквивалентности косоэрмитовых форм, вообще говоря, не выполняется, причем причина с когомологической точки зрения кроется в неинъективности отображения $H^1(K, \boldsymbol{SU}_n(f)) \to H^1(K, \boldsymbol{U}_n(f))$. Рассмотрим коммутативную диаграмму с точными строками

$$\begin{tikzcd}
1 \arrow[r] & \mu_2 \arrow[r, "\alpha_1"] \arrow[d, "\gamma_1"] & H^1(K,\ \boldsymbol{SU}_n(f)) \arrow[r, "\alpha_2"] \arrow[d, "\gamma_2"] & H^1(K,\ \boldsymbol{U}_n(f)) \arrow[d, "\gamma_1"] \\
1 \arrow[r] & \prod\limits_{v \in S} \mu_2 \times \prod\limits_{v \notin S} \{1\} \arrow[r, "\beta_1"] & \prod\limits_{v} H^1(K_v,\ \boldsymbol{SU}_n(f)) \arrow[r, "\beta_2"] & \prod\limits_{v} H^1(K_v,\ \boldsymbol{U}_n(f))
\end{tikzcd}$$

где $S = \{v \in V^K \mid D_v = D \otimes_K K_v - \text{тело}\}$. Из этой диаграммы вытекает, что $\alpha_2(\gamma_2^{-1}(\operatorname{Im}\beta_1)) \subset \operatorname{Ker}\gamma_3$, причем, очевидно, $[\alpha_2(\gamma_2^{-1}(\operatorname{Im}\beta_1))] = \frac{1}{2}[\gamma_2^{-1}(\operatorname{Im}\beta_1)]$.

Лемма 22. $[\gamma_2^{-1}(\operatorname{Im}\beta_1)] \geqslant 2^{t-1}$, *где* $t = [S \cap V_f^K]$.

Доказательство. Рассмотрим коммутативную диаграмму, индуцированную универсальным накрытием $\tilde{G} \to G$ группы $G = \boldsymbol{SU}_n(f)$,

$$\begin{tikzcd}
H^1(K,\ \tilde{G}) \arrow[r] \arrow[d] & H^1(K,\ G) \arrow[r, "\delta"] \arrow[d, "\gamma_2"] & H^2(K,\ \mu_2) \arrow[d, "\tau"] \\
\prod\limits_{v \in V^K} H^1(K_v,\ \tilde{G}) \arrow[r] & \prod\limits_{v} H^1(K_v,\ G) \arrow[r, "\theta"] & \prod H^2(K_v,\ \mu_2)
\end{tikzcd} \tag{5}$$

Так как отображение ε в последовательности (4), написанной для поля K_v, $v \in S \cap V_f^K$, является биекцией, мы видим, что достаточно установить равенство $\left[\gamma_2^{-1}\left(\prod_{v \in S \cap V_f^K} H^1(K_v, G) \times \times \prod_{v \notin S \cap V_f^K} \{1\}\right)\right] = 2^{t-1}$. Но ограничение θ на множество $H^1(K_v, G)$ для $v \in V_f^K$ биективно отображает его на $H^2(K_v, \mu_2)$, поэтому учитывая сюръективность δ (теорема 20) и теорему 6, при помощи скручивания получаем, что наша задача сводится к доказательству равенства

$$\left[\tau^{-1}\left(\prod_{v \in S \cap V_f^K} H^2(K_v, \mu_2) \times \prod_{v \notin S \cap V_f^K} \{1\}\right)\right] = 2^{t-1}$$

(детали рассуждений мы оставляем читателю). Но с учетом отождествлений $H^2(K, \mu_2) = \mathrm{Br}(K)_2$, $H^2(K_v, \mu_2) = \mathrm{Br}(K_v)_2$ последнее равенство вытекает из теоремы 1.12. Лемма доказана.

Таким образом, $[\mathrm{Ker}\,\gamma_3] \geqslant 2^{t-2}$, и поэтому γ_3 инъективным, вообще говоря, не является. Несколько более точный подсчет (см. Кнезер [12], Бартельс [2]) показывает, что $[\mathrm{Ker}\,\gamma_3] = 2^{s-2}$, где $s = [S]$. Отметим, что несмотря на нарушение слабого принципа Хассе, локально-глобальная классификация косоэрмитовых форм возможна (см. Бартельс [2], Шарлау [1]). Заинтересованного читателя мы отсылаем к статьям Бартельса [1, 2], содержащим подробное изложение когомологического подхода к классификации косоэрмитовых форм.

Основываясь на результатах по арифметике полуторалинейных форм, мы получим доказательство теоремы 5 о том, что простая односвязная анизотропная группа над локальным полем является группой типа $\boldsymbol{SL}_1(D)$, и следующего ее аналога для вполне мнимых полей.

Теорема 25. *Пусть G — простая анизотропная группа над вполне мнимым числовым полем K. Тогда G является группой типа A_n.*

(Разница между теоремами 5 и 25 заключается в том, что в локальной ситуации анизотропными могут быть лишь внутренние формы типа A_n, в то время как над вполне мнимым полем появляются и внешние анизотропные формы.)

Изотропность групп типов B_n $(n \geqslant 2)$, C_n $(n \geqslant 2)$, ${}^{1,2}D_n$ $(n \geqslant 4)$ вытекает из описания этих групп как связных компонент групп автоморфизмов квадратичных, эрмитовых либо косоэрмитовых форм (см. § 2.3), того факта, что изотропность группы равносильна изотропности соответствующей формы (см. предложение 2.15) и утверждений 1)—3). Отметим также, что в случае локального поля некоммутативные тела с инволюцией

второго рода отсутствуют, так что внешние формы типа ${}^2A_n$ ($n \geqslant 2$) отвечают эрмитовым формам степени $\geqslant 3$ над квадратичным расширением L/K, которые в силу утверждения 2) являются изотропными.

Для исключительных групп доказательство теорем 5, 25 использует предложения 15 и 16, т. е. в конечном счете зависит от теорем 4, 6. С другой стороны, утверждение теорем 5, 25 будет использоваться при доказательстве теорем 4, 6. Поэтому мы, чтобы не пойти по порочному кругу, будем доказывать следующее условное утверждение, которое автоматически завершит доказательство теорем 5, 25 после доказательства теорем 4, 6.

Теорема 26. *Пусть G — простая односвязная группа одного из исключительных типов, определенная над локальным либо вполне мнимым числовым полем K, G_0 — квазиразложимая группа того же внутреннего типа. Тогда если $H^1(K, G_0) = 1$, то группа G является K-изотропной.*

Доказательство. Если G относится к одному из типов E_8, F_4, G_2, то из условия $H^1(K, G_0) = 1$ вытекает K-разложимость G (утверждение 1) предложения 16), и доказывать нечего.

Из оставшихся типов ${}^{3,6}D_4$, ${}^{1,2}E_6$, E_7 группы типов ${}^{3,5}D_4$ и ${}^2E_6$ квазиразложимы над K, если поле K локально (предложение 15), поэтому здесь остается рассмотреть только типы ${}^1E_6$ и E_7; над вполне мнимым числовым полем приходится рассматривать все типы.

Наиболее просто разбирается случай групп G типа E_7. Из предложения 16 вытекает, что группа G разложима над некоторым квадратичным расширением L/K. Далее применяется

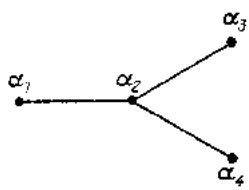
Лемма 23. *Пусть G — связная K-определенная группа, разложимая над квадратичным расширением L/K. Тогда существует максимальный K-определенный тор $T \subset G$, разложимый над L.*

Действительно, G обладает подгруппой Бореля, определенной над L, и поэтому согласно лемме 17 существует такая L-определенная подгруппа Бореля $B \subset G$, что $T = B \cap \sigma(B)$ является максимальным K-определенным тором в G, где σ — образующая группы Галуа $\mathrm{Gal}(L/K)$. Остается заметить, что в силу разложимости G над полем L любой L-определенный тор в B является L-разложимым.

Предположим теперь, что группа G анизотропна над K и рассмотрим систему корней $R = R(T, G)$, где T — тор из леммы 23. В силу K-анизотропности T имеем $\mathbf{X}(T)^{\sigma^*} = \{0\}$, где σ^* обозначает действие σ на группе характеров. Так как $(\sigma^*)^2 = \mathrm{id}$, то отсюда следует, что $\sigma^*\chi = -\chi$ для любого $\chi \in \mathbf{X}(T)$. В частности, $\sigma^*\alpha = -\alpha$ для любого $\alpha \in R$, и поэтому корневая подгруппа G_α, порожденная одномерными унипотентными подгруппами U_α и $U_{-\alpha}$ (см. § 2.1, п. 10), определена над K. Более того,

для любого подмножества Σ системы простых корней $\Pi \subset R$ группа G_Σ, порожденная G_α для $\alpha \in \Sigma$, определена над K. (Предыдущие рассуждения годятся для любой анизотропной группы, разложимой над квадратичным расширением, и не раз нам встретятся в дальнейшем.) Возьмем в качестве Σ подмножество, состоящее из двух соседних корней в диаграмме Дынкина. Тогда $H = G_\Sigma$ является K-определенной подгруппой в G типа A_2, разложимой над квадратичным расширением L/K. Поэтому из описания групп такого типа (см. § 2.3) вытекает, что H не может быть не чем иным, как группой, изогенной специальной унитарной группе $SU_3(f)$, где f — эрмитова форма над L/K. Но из утверждения 2 вытекает, что в случае локального или вполне мнимого числового поля такая форма является изотропной. Поэтому группа H, и тем более группа G, изотропны над K.

Группы типов ${}^{3,6}\boldsymbol{D}_4$. Согласно утверждению 2) предложения 15 группа G, относящаяся к одному из этих типов, обладает подгруппой Бореля $B \subset G$, определенной над некоторым квадратичным расширением L/K. Предположим, что G является K-анизотропной. Тогда пересечение $T = B \cap \sigma(B)$, где σ — образующая группы $\mathrm{Gal}(L/K)$, является K-определенным максимальным тором в G, содержащимся в B. Рассмотрим систему корней $R = R(T, G)$ и занумеруем простые корни следующим образом:

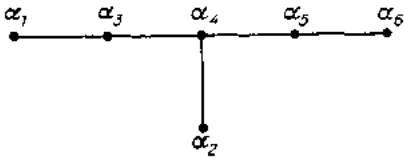


(6)

Из явного описания корней (см. табл. IV в книге Бурбаки [4]) вытекает, что $\beta = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4$ является корнем. При этом корни $\alpha = \alpha_2$ и β инвариантны относительно всех симметрий диаграммы (6), и поэтому определены над L. Тогда из K-анизотропности G, как и выше, получаем, что $\sigma^*\alpha = -\alpha$, $\sigma^*\beta = -\beta$, так что группа H, порожденная G_α и G_β, определена над K. Из описания корней вытекает, что H является группой типа A_2, разложимой над расширением L/K. Поэтому рассуждения завершаются как и в предыдущем случае.

Группы типа ${}^1\boldsymbol{E}_6$. Мы знаем, что $Z(G) = \mu_3$, поэтому, рассуждая как и при доказательстве предложения 16, получим, что G разложима над некоторым циклическим расширением L/K степени три. Пусть σ — образующая группы $\mathrm{Gal}(L/K)$. Здесь использованный выше прием, состоящий в рассмотрении L-определенной борелевской подгруппы $B \subset G$ и пересечения $B \cap \sigma(B) \cap \sigma^2(B)$ всех ее сдвигов, уже не приводит к цели, ибо

последнее пересечение может оказаться тривиальным. Однако можно воспользоваться некоторой его модификацией, суть которой заключается в том, что вместо борелевских подгрупп используются параболические. А именно, рассмотрим систему корней $R = R(T, G)$ относительно максимального L-разложимого тора $T \subset G$ и занумеруем простые корни следующим образом:

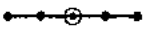


(7)

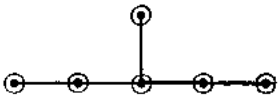
Положим $P = P_\Delta$ в обозначениях п. 12 § 2.1, где $\Delta = \{\alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$. Тогда P является максимальной L-определенной параболической подгруппой в G коразмерности 16 ($\dim G = 78$, $\dim P = 62$), центральный тор редуктивной части P одномерен, а полупростая часть является группой типа D_5. Положим $H = P \cap \sigma(P) \cap \sigma^2(P)$. Тогда из теорем о размерности вытекает, что $\operatorname{codim} H \leqslant 3 \cdot 16 = 48$, т. е. $\dim H \geqslant 78 - 48 = 30$. Если предположить K-анизотропной группу G, то H является K-определенной редуктивной подгруппой в G. Покажем, что ее полупростая часть D содержит простую компоненту не типа A_n. Тогда изотропность D будет следовать из того факта, что изотропность групп всех типов, отличных от A_n и E_6, уже установлена. Предположим противное, т. е. пусть D имеет тип $A_{d_1} \times \ldots \times A_{d_n}$. Тогда $d_1 + \ldots + d_n \leqslant 5$ и $d_1 + \ldots + d_n + m \leqslant 6$, где m — размерность центрального тора в H. Кроме того, невозможен случай $d_i = 5$, ибо D должно содержаться в группе типа D_5 (полупростой части P), а группа типа A_5 вложением в D_5 не обладает (скажем, потому, что порядок группы Вейля $W(A_5)$, равный 6!, не делит порядок $W(D_5)$, равный $2^4 5!$). При помощи элементарных оценок тогда получается, что $\dim H = d_1^2 + \ldots + d_n^2 + 2(d_1 + \ldots + d_n) + m \leqslant 28$, что невозможно, ибо у нас $\dim H \geqslant 30$.

Группы типа ${}^2E_6$. Пусть L/K — то квадратичное расширение, над которым G становится внутренней формой. Тогда согласно уже доказанному, G является L-изотропной. Утверждается, что на L-индексе группы G хотя бы одна из концевых вершин α_i ($i = 1, 2, 6$) в диаграмме (7) *является отмеченной*. Действительно, в противном случае L-анизотропное ядро G имеет простую компоненту типа A_1. С другой стороны, анизотропное ядро должно разлагаться над расширением L степени 3 — противоречие. Тогда соответствующая параболическая подгруппа $P = P_\Delta$, где $\Delta = \{\alpha_j \mid j \neq i\}$ определена над L и имеет коразмерность 16 для $i = 1, 6$ и 21 для $i = 2$. Если предположить K-анизотропной

группу G, то $H = P \cap \sigma(P)$, где σ — образующая группы $\mathrm{Gal}(L/K)$, является редуктивной K-определенной подгруппой. В случае $\operatorname{codim} P = 16$ имеем $\operatorname{codim} H \leqslant 32$, т. е. $\dim H \geqslant 78 - 32 = 46$, и, как и выше, легко убедиться, что все простые компоненты не могут иметь тип A_n, что и дает требуемое. Поэтому единственный случай, когда G априори может быть K-анизотропной, — это случай, когда отмеченной является вершина α_2 и полупростая часть D группы H является группой типа A_5. (Ясно, что при этом D совпадает с полупростой частью P.) Далее, группа D должна разлагаться над расширением L третьей степени, откуда следует, что для L-индекса D имеется две возможности

и 

Тогда L-индекс G имеет соответственно вид

 и

В первом случае G разложима над L, и доказательство ее K-изотропности проводится, как и в случае групп типа E_7. Рассмотрим второй случай. Положим $P' = P_{\Delta'}$, где $\Delta' = \{\alpha_j \mid j \neq 2,4\}$. Тогда $\dim P' = 48$, откуда для $F = P' \cap \sigma(P')$ получаем оценку $\dim F \geqslant 18$. Так как F является редуктивной K-группой, полупростая часть S которой должна вкладываться в группу типа $A_2 \times A_2$, то анализ размерностей показывает, что S имеет тип $A_2 \times A_2$, и, значит, совпадает с полупростой частью P. Централизатор $C = Z_G(S)$ является полупростой K-группой типа A_2, которая становится изотропной над L, ибо даже централизатор D L-изотропен. Отсюда следует, что C не может быть не чем иным, как группой типа $SU_3(f)$, где f — связанная с расширением L/K эрмитова форма. Так как группы такого вида K-изотропны, то доказательство теоремы 26 завершено.

§ 6.7. Доказательство теорем 4 и 6: группы классических типов

Используя представимость полупростой односвязной K-группы G в виде $G = \prod_{i=1}^{r} \mathbf{R}_{L_i/K}(G_i)$, где G_i — простая односвязная группа над конечным расширением L_i поля K, мы с помощью леммы Шапиро без труда получаем редукцию доказательства теорем 4, 6 к случаю простых групп.

В этом параграфе мы рассмотрим группы типов ${}^{1,2}A_l$, B_l, C_l, ${}^{1,2}D_l$. Структура параграфа следующая. Вначале рассматриваются группы типа ${}^1A_l$. Оказывается, что здесь теорема 4 эквивалентна утверждению о сюръективности приведенной нормы в простой алгебре над локальным полем (см. п. 3 § 1.4), а теорема 6 — теореме Эйхлера о нормах. Далее, при помощи утверждений 1)—3) предыдущего параграфа доказательство теорем 4 и 6 для групп типов B_l, C_l, ${}^{1,2}D_l$, а также специальных унитарных групп $\boldsymbol{SU}_n(f)$ эрмитовых форм над квадратичным расширением L/K, редуцируется к группам типов $B_1 = C_1 = A_1$ и $D_2 = A_1 \times A_1$, которые уже рассмотрены. Таким образом, остается рассмотреть случай форм типа ${}^2A_l$, связанных с некоммутативными телами с инволюцией второго рода (отметим, что над локальными полями, т. е. при доказательстве теоремы 4, этот случай встретиться не может). Рассуждения здесь опираются на сравнительно малоизвестную теорему Ландера, которая у нас приводится с доказательством. Отметим также, что при доказательстве теоремы 6 для групп всех типов мы проверяем лишь отсутствие ядра отображения

$$H^1(K, G) \to \prod_{v \in V_\infty^K} H^1(K_v, G),$$

ибо его сюръективность уже доказана (предложение 17).

Группы типа ${}^1\boldsymbol{A}_l$. Здесь $G = \boldsymbol{SL}_n(D)$, где D — конечномерная алгебра с делением над K. Тогда в силу леммы 2.9

$$H^1(K, G) \simeq K^*/\mathrm{Nrd}_{A/K}(A^*) = K^*/\mathrm{Nrd}_{D/K}(D^*),$$

где $A = M_n(D)$. Если K — локальное поле, то $\mathrm{Nrd}_{D/K}(D^*) = K^*$ (см. § 1.4, п. 3), и поэтому $H^1(K, G) = 1$, т. е. теорема 4 в этой ситуации доказана. Пусть теперь K — числовое поле. Тогда отображение

$$H^1(K, G) \xrightarrow{\delta} \prod_{v \in V_\infty^K} H^1(K_v, G)$$

эквивалентно отображению

$$K^*/\mathrm{Nrd}_{A/K}(A^*) \to \prod_{v \in V_\infty^K} K_v^* \big/ \mathrm{Nrd}_{A_v/K_v}(A_v^*),$$

где $A_v = A \otimes_K K_v$, поэтому тривиальность $\mathrm{Ker}\,\delta$ равносильна равенству

$$\mathrm{Nrd}_{A/K}(A^*) = \bigcap_{v \in V_\infty^K} \left(K^* \cap \mathrm{Nrd}_{A_v/K_v}(A_v^*)\right). \tag{1}$$

Легко видеть, что при $v \in V_\infty^K$ группа $\mathrm{Nrd}_{A_v/K_v}(A_v^*)$ совпадает с K_v^*, если A_v является полной матричной алгеброй над K_v (в частности, если $K_v = \mathbb{C}$), и совпадает с множеством положительных элементов K_v^* в противном случае, т. е. если $K_v = \mathbb{R}$

и A_v является полной матричной алгеброй над телом вещественных кватернионов. Поэтому равенство (1) следует из теоремы Эйхлера о нормах (см. теорему 1.13).

Группы типов B_l, C_l, ${}^{1,2}D_l$. Так как для симплектической группы Sp_{2n} над любым полем K имеем $H^1(K, Sp_{2n}) = 1$ (см. предложение 2.7), то мы можем исключить симплектические группы из дальнейшего рассмотрения. Тогда оставшиеся группы, относящиеся к одному из указанных типов, являются универсальными накрывающими G_n специальных ортогональных групп $SO_n(f)$ (специальных унитарных групп $SU_n(f)$), где f — невырожденная n-мерная квадратичная форма (соответственно эрмитова либо косоэрмитова форма над телом кватернионов D). Одновременно будем рассматривать также специальные унитарные группы $SU_n(f)$, отвечающие эрмитовым формам, связанным с квадратичным расширением L/K, которые относятся к типу ${}^2A_{n-1}$. Обозначим через W n-мерное векторное пространство над K (соответственно D или L), на котором определена форма f. Кроме того, будем обозначать через m_0 целое число, которое было указано в списке классических групп (см. § 2.3, п. 4) для каждого типа. Его арифметический смысл вытекает из утверждений 1′, 2, 3 предыдущего параграфа и состоит в том, что при $n \geqslant m_0$ форма f автоматически представляет элемент $a \in K^*$ (соответственно, эрмитов либо косоэрмитов элемент $a \in D^*$ или L^*), если K — локальное поле, либо K — числовое поле, и представимость имеет место над всеми K_v, $v \in V_\infty^K$. Отметим, что $m_0 = 1$ для кватернионных групп типа C_n, и в этом случае для соблюдения единообразия удобно считать группу типа C_0 единичной группой. Для остальных типов группы G_{m_0-1} относятся к типам $B_1 = A_1$ и $D_2 = A_1 \times A_1$, которые уже были разобраны.

Рассуждение будем вести индукцией по степени n формы f. Рассмотрим вначале случай локального поля K. Предположим, что $n \geqslant m_0$, и покажем, что тривиальность $H^1(K, G_n)$ вытекает из тривиальности $H^1(K, G_{n-1})$. Зафиксируем анизотропный вектор $x \in W$. Тогда его стабилизатор в G_n является группой типа G_{n-1} (см. предложение 2.21). Покажем, что отображение $H^1(K, G_{n-1}) \xrightarrow{\varphi} H^1(K, G_n)$ сюръективно. Для этого заметим, что в силу теоремы Витта однородное пространство G_n/G_{n-1} можно отождествить со «сферой» $X = \{y \in W \otimes_K \bar{K} \mid f(y) = f(x)\}$. Пусть теперь $\xi \in H^1(K, G)$. Тогда скрученное пространство ${}_\xi(G_n/G_{n-1})$ изоморфно «сфере» $Y = \{y \in W \otimes_K \otimes_K \bar{K} \mid g(y) = f(x)\}$, где $g = {}_\xi f$ — соответствующая скрученная форма. Так как $n \geqslant m_0$, то $Y_K \neq \varnothing$, и поэтому $\xi \in \operatorname{Im} \varphi$ (см. лемму 2.6), что и требовалось.

Перейдем к случаю числового поля K. Если K является чисто мнимым, то предыдущее рассуждение проходит без всяких

изменений и позволяет установить тривиальность $H^1(K, G_n)$. В общем случае приходится дополнительно использовать один результат о слабой аппроксимации, который мы докажем в § 7.1. А именно, пусть $x \in W$ — анизотропный вектор и $X = \{y \in W \otimes_K R \mid f(y) = f(x)\}$ — соответствующая «сфера»; тогда X обладает слабой аппроксимацией относительно любого конечного множества $S \subset V^K$, т. е. вложение $X_K \to X_S = \prod_{v \in S} X_{K_v}$ является плотным. Мы используем этот факт в следующем контексте. Так как X является однородным пространством группы G_n, то для любого $v \in V^K$ и любого $x_v \in X_{K_v}$ орбита $(G_n)_{K_v} x_v$ открыта в X_{K_v} (следствие 2 из предложения 3.3), и поэтому найдется $x \in X_K$ со свойством $x \in (G_n)_{K_v} x_v$ для всех $v \in S$. Другими словами, отображение $(G_n)_K \backslash X_K \to \prod_{v \in S} \left((G_n)_{K_v} \backslash X_{K_v}\right)$ соответствующих пространств орбит сюръективно. Рассмотрим теперь «точную последовательность» $1 \to G_{n-1} \to G_n \xrightarrow{\alpha} X \to 1$, где $\alpha(g) = gx$, из которой получается следующая коммутативная диаграмма:

$$\begin{array}{ccccc} (G_n)_K \backslash X_K & \xrightarrow{\beta_1} & H^1(K, G_{n-1}) & \xrightarrow{\beta_2} & H^1(K, G_n) \\ \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} \\ \prod_{v \in V_\infty^K} (G_n)_{K_v} \backslash X_{K_v} & \xrightarrow{\gamma_1} & \prod_{v \in V_\infty^K} H^1(K_v, G_{n-1}) & \xrightarrow{\gamma_2} & \prod_{v \in V_\infty^K} H^1(K_v, G_n) \end{array} \qquad (2)$$

Пусть теперь $\xi \in \operatorname{Ker} \alpha_3$. Как и в локальном случае, скрученное пространство ${}_\xi(G_n/G_{n-1})$ может быть отождествлено со «сферой» $Y = \{y \in W \otimes_K \overline{K} \mid g(y) = f(x)\}$, где $g = {}_\xi f$ — скрученная форма. Поскольку $\xi \in \operatorname{Ker} \alpha_3$, то над каждым полем K_v, $v \in V_\infty^K$ формы f и g эквивалентны, в частности, уравнение $g(y) = f(x)$ имеет решение, т. е. $Y_{K_v} \neq \varnothing$. Но по условию $n \geqslant m_0$, и поэтому $Y_K \neq \varnothing$. Это означает, что $\xi = \beta_2(\zeta)$ для подходящего $\zeta \in H^1(K, G_{n-1})$. По условию коцикл $\gamma_2(\alpha_2(\zeta)) = \alpha_3(\beta_2(\zeta)) = \alpha_3(\xi)$ тривиален, так что из точности нижней строки в (2) получаем $\alpha_2(\zeta) = \gamma_1(z)$, $z \in \prod_{v \in V_\infty^K} (G_n)_{K_v} \backslash X_{K_v}$. Но выше мы установили, что α_1 сюръективно, и, значит, $z = \alpha_1(a)$, $a \in (G_n)_K \backslash X_K$. Тогда из коммутативности (2) вытекает, что $\alpha_2(\zeta) = \alpha_2(\beta_1(a))$, и поэтому $\zeta = \beta_1(a)$, ибо по предположению индукции α_2 инъективно. (Индуктивное предположение состоит в том, что α_2 имеет тривиальное ядро для всех групп фиксированного типа данной степени $n-1$, что в силу соображений

скручивания эквивалентно инъективности α_2 для того же класса групп.) Окончательно получаем, что коцикл $\xi = \beta_2(\zeta) = \beta_2(\beta_1(a))$ тривиален.

Группы типа ^2A_l. Случай специальных унитарных групп, связанных с квадратичным расширением L/K, был рассмотрен вместе с группами типов B_l, D_l, поэтому теперь обратимся к специальным унитарным группам $G = \boldsymbol{SU}_n(f)$ эрмитовых форм f над (некоммутативным) телом D с инволюцией σ второго рода, центр L которого является квадратичным расширением основного поля K (в частности, всюду ниже K — числовое поле). Рассуждения здесь являются весьма длинными и сложными, причем их можно разбить на два основных этапа: 1) доказательство принципа Хассе для соответствующей унитарной группы $H = \boldsymbol{U}_n(f)$; 2) вывод принципа Хассе для G из принципа Хассе для H. В предварительной части доказательства мы проведем редукцию этих утверждений к некоторым свойствам алгебр с инволюциями, а затем докажем эти свойства.

Рассмотрим алгебру $A = M_n(D)$ и определим ее инволюцию τ, полагая $\tau((x_{ij})) = F(\sigma(x_{ji}))F^{-1}$, где F — матрица формы f. Обозначим через B группу $\boldsymbol{GL}_n(D)$ и через Σ — множество симметрических относительно τ элементов B. Тогда отображение $\varphi\colon B \to \sum$, $\varphi(x) = x\tau(x)$ сюръективно, имеет своим ядром группу H и поэтому позволяет отождествить Σ с однородным пространством B/H. Точная последовательность $1 \to H \to B \xrightarrow{\varphi} \Sigma \to 1$ порождает следующую диаграмму:

$$\begin{tikzcd}
A^* \arrow[r, "\beta_1"] \arrow[d, "\alpha_1"] & \Sigma_K \arrow[r, "\beta_2"] \arrow[d, "\alpha_2"] & H^1(K, H) \arrow[r, "\beta_3"] \arrow[d, "\alpha_3"] & H^1(K, B) = 1 \arrow[d, "\alpha_4"] \\
\prod\limits_{v \in V^K} (A \otimes_K K_v)^* \arrow[r, "\gamma_1"] & \prod\limits_{v \in V^K} \Sigma_{K_v} \arrow[r, "\gamma_2"] & \prod\limits_{v \in V^K} H^1(K_v, H) \arrow[r, "\gamma_3"] & \prod\limits_{v \in V^K} H^1(K_v, B) = 1
\end{tikzcd} \tag{3}$$

Пусть $\xi \in \operatorname{Ker} \alpha_3$. Так как $H^1(K, B) = 1$, то $\xi = \beta_2(x)$, $x \in \Sigma_K$. По условию коцикл $\gamma_2(\alpha_2(x)) = \alpha_3(\xi)$ тривиален, что в силу точности нижней строки в (3) означает, что $\alpha_2(x) \in \operatorname{Im} \gamma_1$. С другой стороны, утверждение о тривиальности ξ равносильно тому, что $x \in \operatorname{Im} \beta_1$. Таким образом, принцип Хассе для унитарной группы H эквивалентен следующей теореме.

Теорема 27 (Ландер [1]). *Пусть $y \in A^*$ — симметрический элемент. Предположим, что уравнение $y = x\tau(x)$ имеет решение $x_v \in A \otimes_K K_v$ для всех $v \in V^K$. Тогда оно имеет решение $x \in A^*$.*

Далее, предположим, что принцип Хассе для H уже доказан. Положим $S = \mathbf{R}^{(1)}_{L/K}(\boldsymbol{G}_m)$. Приведенная норма $\operatorname{Nrd}_{A/L}$ индуцирует точную последовательность $1 \to G \to H \to S \to 1$, из которой

получается диаграмма:

$$\begin{tikzcd} H_K \arrow[r, "\theta_1"] \arrow[d, "\delta_1"] & S_K \arrow[r, "\theta_2"] \arrow[d, "\delta_2"] & H^1(K, G) \arrow[r, "\theta_3"] \arrow[d, "\delta_3"] & H^1(K, H) \arrow[d, "\delta_4"] \\ \prod\limits_{v \in V^K} H_{K_v} \arrow[r, "\rho_1"] & \prod\limits_{v \in V^K} S_{K_v} \arrow[r, "\rho_2"] & \prod\limits_{v \in V^K} H^1(K_v, G) \arrow[r, "\rho_3"] & \prod\limits_{v \in V^K} H^1(K_v, H) \end{tikzcd} \qquad (4)$$

Опять, если $\xi \in \operatorname{Ker} \delta_3$, то из инъективности δ_4 вытекает, что $\xi = \theta_2(x)$, $x \in S_K$, причем из коммутативности (4) получаем, что $\delta_2(x) \in \operatorname{Im} \rho_1$. Для доказательства тривиальности ξ нам надо показать, что $x \in \operatorname{Im} \theta_1$. Таким образом, доказательство завершает следующий унитарный вариант теоремы Эйхлера.

Теорема 28. *Пусть $y \in L^*$ и $N_{L/K}(y) = 1$. Предположим, что уравнение $\operatorname{Nrd}_{A/L}(x) = y$ для всех $v \in V^K$ имеет решение $x_v \in A \otimes_K K_v$ такое, что $x_v \tau(x_v) = 1$. Тогда оно имеет решение $x \in A^*$ такое, что $x\tau(x) = 1$.*

Оставшаяся часть параграфа посвящена доказательству теорем 27 и 28. Доказательство теоремы 27 начнем с редукции к случаю $\operatorname{Nrd}_{A/L}(y) = 1$. Имеем $a = \operatorname{Nrd}_{A/L}(y) \in L^\tau = K$, причем для любого $v \in V^K$, полагая $t_v = \operatorname{Nrd}_{A \otimes_K K_v / L \otimes_K K_v}(x_v)$, получим, что $a = t_v \tau(t_v) \in N_{L \otimes_K K_v / K_v}((L \otimes_K K_v)^*)$. Так как для L/K выполняется принцип Хассе, то $a \in N_{L/K}(L^*)$, т. е. $a = t\tau(t)$ для подходящего $t \in L^*$. Покажем, что выбор t можно осуществить таким образом, чтобы $t \in \operatorname{Nrd}_{A/L}(A^*)$. Для этого в силу теоремы Эйхлера надо добиться, чтобы $t \in \operatorname{Nrd}_{A \otimes_L L_w / L_w}((A \otimes_L L_w)^*)$ для $w \in V_\infty^L$. Эквивалентная формулировка: $t \in U_v = \operatorname{Nrd}_{A \otimes_K K_v / L \otimes_K K_v}((A \otimes_K K_v)^*)$ для $v \in V_\infty^K$. Имеем $a = t\tau(t) = t_v \tau(t_v)$, где $t_v \in \operatorname{Nrd}_{A \otimes_K K_v / L \otimes_K K_v}(x_v) \in U_v$. Тогда $z_v = t t_v^{-1} \in S_{K_v}$, где $S = \mathbf{R}_{L/K}^{(1)}(\boldsymbol{G}_m)$, и поэтому по слабой аппроксимационной теореме для тора S найдется $z \in S_K \cap \prod\limits_{v \in V_\infty^K} z_v(S_{K_v} \cap U_v)$. Полагая $t' = tz^{-1}$, получим $a = t\tau(t) = t'\tau(t')$ и $t' \in U_v$ для всех $v \in V_\infty^K$, что и требовалось. Итак, пусть $t = \operatorname{Nrd}_{A/L}(b)$, $b \in A^*$. Тогда для $y' = b^{-1} y \tau(b^{-1})$ будем иметь $\operatorname{Nrd}_{A/L}(y') = \operatorname{Nrd}_{A/L}(b^{-1} y \tau(b^{-1})) = t^{-1} a \tau(t^{-1}) = 1$. Если предположить, что $y' = x\tau(x)$ для $x \in A^*$, то $y = tx\tau(x)\tau(t) = (tx)\tau(tx)$, и требуемая редукция получена.

Идея дальнейших рассуждений заключается в том, чтобы искать решение уравнения $y = x\tau(x)$ не в A, а в поле $L(y)$. Тогда задача сводится к тому, чтобы установить принадлежность y норменной группе $N_{L(y)/K(y)}(L(y)^*)$. Но $L(y)/K(y)$ имеет степень 2, и поэтому удовлетворяет норменному принципу Хассе, так что достаточно установить, что y является нормой по-

всем пополнениям $w \in V^{K(y)}$. Последнее, как легко видеть, эквивалентно тому, что $y \in N_{L(y)\otimes_K K_v/K(y)\otimes_K K_v}(L(y)\otimes_K K_v)$ для всех $v \in V_f^K$. Чтобы реализовать эту схему, нам придется перейти от элемента y к элементу y' вида $y' = ty\tau(t)$, $t \in SL_1(\Lambda)$, что допустимо, ибо элементы y и y' одновременно представимы или не представимы в виде $x\tau(x)$, $x \in A^*$.

Лемма 24. *Пусть $y \in SL_1(A)$ — симметрический элемент. Тогда если уравнение $y = x\tau(x)$ имеет решение $x_v \in A \otimes_K K_v$, где $v \in V_f^K$, то оно имеет также решение $z_v \in SL_1(A \otimes_K K_v)$.*

Доказательство. Достаточно найти такой элемент $t_v \in A \otimes_K K_v$ что $t_v\tau(t_v) = 1$ и $\mathrm{Nrd}_{A\otimes_K K_v/L\otimes_K K_v}(t_v) = \mathrm{Nrd}_{A\otimes_K K_v/L\otimes_K K_v}(x_v^{-1})$. Для этого рассмотрим отдельно два случая, когда соответственно $L \otimes_K K_v \simeq K_v \oplus K_v$ и $L \otimes_K K_v$ — поле. В первом случае $A \otimes_K K_v \simeq A_1 \oplus A_2$ — прямая сумма двух простых алгебр, между которыми существует антиизоморфизм φ: $A_1 \to A_2$, причем можно считать, что K_v-линейное продолжение τ задается формулой $\tau((a, b)) = (\varphi^{-1}(b), \varphi(a))$. Отсюда следует, что элементы $t_v \in A \otimes_K K_v$, удовлетворяющие соотношению $t_v\tau(t_v) = 1$, имеют вид $t_v = (a, \varphi(a)^{-1})$, $a \in A_1^*$, а значения приведенной нормы на таких элементах в силу п. 3 § 1.4 заполняют все множество $X = \{(s, s^{-1}) \mid s \in K_v^*\}$. Остается заметить, что в силу условий $y \in SL_1(A)$, $y = x_v\tau(x_v)$ приведенная норма $\mathrm{Nrd}_{A\otimes_K K_v/L\otimes_K K_v}(x_v)$ попадает в X. Во втором случае $A_w = A \otimes_K K_v$ является полной матричной алгеброй над полем $L_w = L \otimes_K K_v$, и можно выбрать изоморфизм $A_w \xrightarrow{\sim} M_n(L_w)$ таким образом, что инволюция τ запишется в виде $\tau((x_{ij})) = a\tau((x_{ji}))a^{-1}$, где $a = \mathrm{diag}(a_1, \ldots, a_n)$, $a_i \in K_v^*$. Тогда в качестве t_v можно взять матрицу вида $\mathrm{diag}(d, 1, \ldots, 1)$, где $d = \mathrm{Nrd}_{A_w/L_w}(x_v)^{-1}$. Заметим, что в силу $y \in SL_1(A)$ и $y = x_v\tau(x_v)$ имеем $d\tau(d) = 1$, откуда $t_v\tau(t_v) = 1$. Лемма 24 доказана.

Завершим доказательство теоремы 27. Зафиксируем в алгебре A некоторый τ-инвариантный порядок с тем, чтобы можно было корректно говорить о целых точках. Обозначим через S_0 конечное подмножество V^K, содержащее все архимедовы нормирования, а также те неархимедовы, относительно которых либо элемент y не является единицей, либо расширение L/K разветвлено. Для каждого $v \in S_0$ зафиксируем решение $z_v \in SL_1(A \otimes_K K_v)$ уравнения $y = x\tau(x)$. Утверждается, что существуют такие открытые подмножества $W_v \subset SL_1(A \otimes_K K_v)$, что для $t_v \in W_v$ элемент $t_v y\tau(t_v)$ является квадратом в $K_v[t_v y\tau(t_v)]$. Действительно, рассмотрим алгебраическую группу $F = SL_1(A \otimes_K R)$ (отметим, что в действительности $F = \mathbf{R}_{L/K}(\mathbf{SL}_1(A))$) и обозначим через Φ множество τ-симметрических элементов в F. Ясно, что Φ содержит полупростые регулярные в F элементы, и поэтому множество Φ_0 последних

является непустым открытым подмножеством. Так как отображение $F \xrightarrow{\varphi} \Phi$, $\varphi(t) = t\sigma(t)$, очевидно, сюрективно, то отсюда следует, что $F_0 = \{t \in F \mid ty\tau(t) \in \Phi_0\}$ является непустым открытым по Зарисскому подмножеством в F. С другой стороны, из предложения 3.3 вытекает, что отображение $\Phi_{K_v} \to \Phi_{K_v}$, $p \mapsto p^2$ является открытым, в частности, существует окрестность единицы $U_v \subset \Phi_{K_v}$, содержащаяся в $\Phi_{K_v}^2$. Покажем, что множества $W_v = F_0 \cap (\varphi^{-1}(U_v) z_v^{-1})$ являются искомыми (непустота W_v вытекает из леммы 3.2). По построению для $t_v \in W_v$ имеем $y' = t_v y \tau(t_v) \in U_v \cap \Phi_0$. Таким образом, $y' = s^2$ для некоторого $s \in \Phi_{K_v}$ и алгебра $(L \otimes_K K_v)[y']$ является максимальной полупростой коммутативной подалгеброй в $A \otimes_K K_v$. Отсюда следует, что $s \in (L \otimes_K K_v)[y']$, и так как $\tau(s) = s$, то в действительности $s \in K_v[y']$, что и требовалось.

Пользуясь теоремой плотности Чеботарева, выберем такое нормирование $v_0 \notin S_0$, чтобы $L \otimes_K K_{v_0} \simeq K_{v_0} \oplus K_{v_0}$ и, сверх того, алгебра $A \otimes_K K_{v_0}$ являлась бы прямой суммой двух матричных алгебр над K_{v_0}. Тогда группа $F_{K_{v_0}}$ некомпактна, и поэтому к группе F и множеству $\{v_0\}$ применима сильная аппроксимационная теорема 7.13. (Отметим, что доказательство теоремы 7.13, данное Платоновым [4] и приводимое нами в § 7.4, не использует никаких результатов о когомологиях над числовыми полями.) Из нее вытекает существование такого элемента $t \in F$, что $t \in W_v$ для $v \in S_0$ и $t \in F_{\mathcal{O}_v}$ для $v \notin S_0 \cup \{v_0\}$. Покажем, что элемент t является искомым, т. е. для $y' = ty\tau(t)$ и всех $v \in V^K$ выполняется условие

$$y' \in N_{L(y') \otimes_K K_v / K(y') \otimes_K K_v}(L(y') \otimes_K K_v), \tag{5}$$

что, как мы видели выше, позволяет завершить доказательство теоремы 27. Если $v \in S_0$, то по построению y' является квадратом в $K(y') \otimes_K K_v$, и условие (5) очевидно. Для разбора остальных случаев заметим, что $L(y') \otimes_K K_v$ является «композитом» L и $K(y') \otimes_K K_v$. Отсюда следует, что условие (5) заведомо выполняется, если $L \otimes_K K_v \simeq K_v \oplus K_v$, в частности, для $v = v_0$. Пусть теперь $v \notin S_0 \cup \{v_0\}$. Тогда, с одной стороны, «расширение» $L(y') \otimes_K K_v / K(y') \otimes_K K_v$ является неразветвленным в очевидном смысле, с другой — элемент y' является v-адической единицей, и условие (5) снова выполняется. Теорема 27 доказана.

Замечание. Проверка условий теоремы Ландера заметно упрощается, если воспользоваться следующим наблюдением: при $v \in V_f^K$ симметрический элемент y представим в виде $y = x_v \tau(x_v)$, где $x_v \in A \otimes_K K_v$, в том и только том случае, если $\mathrm{Nrd}_{A/L}(y) \in N_{L \otimes_K K_v / K_v}((L \otimes_K K_v)^*)$. Для доказательства достаточности пред-

положим, что $\mathrm{Nrd}_{A/L}(y) = N_{L\otimes_K K_v/K_v}(z)$, $z \in L \otimes_K K_v$. Найдем элемент $t \in A \otimes_K K_v$ такой, что $\mathrm{Nrd}_{A\otimes_K K_v/L\otimes_K K_v}(t) = z$ и рассмотрим элемент $y' = t^{-1}y\tau(t)$. Достаточно показать, что y' представим в виде $y' = x_v\tau(x_v)$, $x_v \in A \otimes_K K_v$. Но это вытекает из уже доказанного результата о том, что $H^1(K_v, G) = 1$, где $G = \boldsymbol{SU}_n(f)$ — специальная унитарная группа. В самом деле, введенное выше отображение φ: $F \to \Phi$ индуцирует точную последовательность $1 \to G \to F \xrightarrow{\varphi} \Phi \to 1$ и соответствующую когомологическую последовательность

$$F_{K_v} \xrightarrow{\varphi} \Phi_{K_v} \to H^1(K_v, G).$$

Так как $H^1(K_v, G) = 1$, то $\varphi(F_{K_v}) = \Phi_{K_v}$, что и требовалось.

Доказательство теоремы 28 представляет собой унитарный вариант доказательства теоремы Эйхлера, приведенного в книге Вейля [7]. А именно, строится неприводимый над L полином $f(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0$, степень которого равна степени алгебры A (корню квадратному из $\dim_L A$), $a_0 = (-1)^n y$, со следующим свойством: расширение $P = L(x)$, где x — корень f, вкладывается в A таким образом, что $x\tau(x) = 1$. В этом случае $\mathrm{Nrd}_{A/L}(x) = y$, и элемент x — искомый. Читатель легко покажет самостоятельно, что без ограничения общности можно считать локальные решения x_v уравнения $\mathrm{Nrd}_{A/L}(x) = y$ полупростыми регулярными элементами в группе $\mathbf{R}_{L/K}(\boldsymbol{GL}_1(A))$. Искомый полином $f(t)$ мы построим, беря достаточно близкую аппроксимацию характеристических полиномов $f_v(t)$ элементов x_v относительно некоторого конечного множества нормирований S. Чтобы придать словам «достаточно близкий» точный смысл, нам понадобятся некоторые предварительные рассуждения.

Пусть χ: $\mathbb{A}^n \to \mathbb{A}^n$ — регулярное отображение, которое $x = (x_1, \ldots, x_n)$ ставит в соответствие упорядоченную совокупность коэффициентов полинома $f(x, t) = \prod_{i=1}^{n}(t - x_i)$ (которые с точностью до знака совпадают с элементарными симметрическими функциями от $x_1, \ldots, x_n$).

Лемма 25. *Если все координаты точки $x = (x_1, \ldots, x_n)$ различны, то дифференциал $d_x\chi$ является линейным изоморфизмом.*

Доказательство. Достаточно показать, что $d_x\chi$ инъективно. Пусть $d_x\chi(X_1, \ldots, X_n) = 0$. На языке двойных чисел это означает, что

$$\prod_{i=1}^{n}(t - (x_i + \delta X_i)) = \prod_{i=1}^{n}(t - x_i), \text{ где } \delta^2 = 0.$$

Полагая в этом равенстве $t = x_i$, получим $\delta X_i \prod_{j \neq i}((x_i - x_j) -$

$-\delta X_j)=0$, откуда в силу условия $x_j \neq x_i$ при $i \neq j$ вытекает, что $X_i=0$. Лемма доказана.

Зафиксируем теперь $v \in V^K$ и рассмотрим K_v-многообразие $W=((L \otimes_K K_v)[x_v]) \otimes_{K_v} \bar{K}_v$ вместе с регулярным отображением χ: $W \to B=(L \otimes_K \bar{K}_v)^n$, которое сопоставляет элементу коэффициенты соответствующего характеристического полинома. Из леммы 25 вытекает, что в регулярной точке $z \in W$ дифференциал $d_z\chi$ является линейным изоморфизмом, что в силу предложения 3.3 влечет открытость отображения χ_v: $(L \otimes_K K_v)[x_v] \to (L \otimes_K K_v)^n$ в любой регулярной точке. На этом пути легко получить другое доказательство леммы Краснера (см. § 6.4). Для наших целей понадобится ее унитарный вариант. Обозначим через X подмногообразие в W, состоящее из унитарных относительно τ элементов, а через Y — подмногообразие в B, состоящее из наборов $(a_0, \ldots, a_{n-1})$, удовлетворяющих условиям

$$\tau(a_0)\, a_0=1, \quad a_0\tau(a_i)=a_{n-i}, \quad i=1, \ldots, n-1. \tag{6}$$

Если характеристический полином элемента x имеет вид $f(t)=t^n+a_{n-1}t^{n-1}+\ldots+a_0$, то характеристические полиномы элементов x^{-1} и $\tau(x)$ имеют соответственно вид $t^n+a_1a_0^{-1}t^{n-1}+\ldots+a_0^{-1}$ и $t^n+\tau(a_{n-1})\,t^{n-1}+\ldots+\tau(a_0)$. Отсюда следует, что χ индуцирует морфизм χ^*: $X \to Y$, причем легко подсчитать, что размерности многообразий X и Y равны n. Ясно, что X является (мультипликативной) алгебраической группой, в частности, гладким многообразием. Непосредственная проверка позволяет также установить гладкость Y. Далее, для $z \in X$ дифференциал $d_z\chi^*$ является ограничением $d_z\chi$ на касательное пространство T_zX, поэтому является линейным изоморфизмом на $T_{\chi^*(z)}Y$. Применяя предложение 3.3, получим, что отображение χ_v^*: $X_{K_v} \to Y_{K_v}$ является открытым в любой регулярной точке. В частности, найдется такая окрестность $U_v \subset Y_{K_v}$ точки $a_v=\chi_v^*(x_v)$, что для любого $a \in U_v$ найдется регулярный элемент $x \in X_{K_v}$, для которого $\chi_v^*(x)=a$. Это утверждение можно переформулировать на языке характеристических полиномов в духе классической леммы Краснера. Пусть характеристический полином элемента x_v имеет вид $f_v(t)=t^n+a_{n-1}^v t^{n-1}+\ldots+a_0^v$. Тогда если полином $f(t)=t^n+a_{n-1}t^{n-1}+\ldots+a_0$ достаточно близок к полиному f_v в том смысле, что отвечающая ему точка $a=(a_0, \ldots, a_{n-1})$ лежит в построенной окрестности U_v точки $a_v=(a_0^v, \ldots, a_{n-1}^v)$, причем удовлетворяются условия (6), то существует такой корень $x \in (L \otimes_K K_v)[x_v]$ полинома f, что $(L \otimes_K K_v)[x]=(L \otimes_K K_v)[x_v]$ и $x\tau(x)=1$.

Осуществим теперь выбор конечного множества S, относительно которого будет вестись аппроксимация полиномов f_v.

Лемма 26. *Существует такое конечное подмножество $S_0 \subset V^K$, содержащее V_∞^K, что для $v \notin S_0$ любая коммутативная полупростая алгебра B_v размерности n над $L \otimes_K K_v$, снабженная инволюцией, ограничение которой на L совпадает с τ, допускает вложение в $A \otimes_K K_v$ как алгебра с инволюцией.*

Доказательство. Известно (теорема 7), что для почти всех $v \in V_f^K$ группа $G = \boldsymbol{SU}_n(f) = \boldsymbol{SU}(A, \tau)$ является K_v-квазиразложимой. А тогда, как следует из предложения 19 и последующих рассуждений, любая алгебра с инволюцией степени n над $L \otimes_K K_v$ вкладывается в $(A \otimes_K K_v, \tau)$. Поэтому в качестве S_0 можно взять объединение V_∞^K со множеством тех неархимедовых v, для которых группа G не является K_v-квазиразложимой. Лемма доказана.

Выберем еще два нормирования v_1, $v_2 \in V^K \setminus S_0$, обладающие следующими свойствами: $L \otimes_K K_{v_i}$ является полем для $i = 1, 2$, причем расширение $L \otimes_K K_{v_1}/K_{v_1}$ неразветвлено. Обозначим через B_{v_1} алгебру $L \otimes_K E$, где E — неразветвленное расширение K_{v_1} степени n, снабженную инволюцией σ_1, которая определяется условиями: $\sigma_1|_L = \tau|_L$, $\sigma_1|_E = \mathrm{id}$. Рассмотрим, далее, алгебру $B_{v_2} = (L \otimes_K K_{v_2})^n$, снабдив ее инволюцией σ_2, которая на каждом слагаемом индуцируется τ. Покажем, что существуют элементы $x_i \in B_{v_i}$ $(i = 1, 2)$ со следующими свойствами: $N_{B_{v_i}/L \otimes_K K_{v_i}}(x_i) = y$, $B_{v_i} = (L \otimes_K K_{v_i})[x_i]$ и $\sigma_i(x_i) x_i = 1$. Это очевидно для $i = 2$, поэтому разберем случай $i = 1$. Пользуясь теоремой 90 Гильберта, представим y в виде $y = \tau(z) z^{-1}$, где в силу неразветвленности $L \otimes_K K_{v_1}$ над K_{v_1} элемент $z \in (L \otimes_K K_{v_1})^*$ можно без ограничения общности считать v_1-адической единицей. Так как расширение E/K_{v_1} неразветвлено, то можно найти элемент $t \in B_{v_1}$ такой, что $N_{B_{v_1}/L \otimes_K K_{v_1}}(t) = z$. Тогда элемент $s = \sigma_1(t) t^{-1}$ будет удовлетворять свойствам $N_{B_{v_1}/L \otimes_K K_{v_1}}(s) = y$ и $\sigma_1(s) s = 1$. Для получения x_{v_1} остается «подправить» s на унитарный элемент с нормой 1 с тем, чтобы получился регулярный элемент. Поскольку $v_i \notin S_0$, то существуют вложения алгебр B_{v_i} в $A \otimes_K K_{v_i}$ как алгебр с инволюциями, так что в дальнейшем мы можем считать B_{v_i} подалгебрами в $A \otimes_K K_{v_i}$.

Теперь уже легко завершить построение искомого полинома f. Положим $S = S_0 \cup \{v_1, v_2\}$ и для каждого $v \in S$ рассмотрим соответствующий элемент x_v, причем считаем, что для $v = v_i$ элемент x_v совпадает с построенным выше элементом x_i, и пусть $f^v(t) = t^n + a_{n-1}^v t^{n-1} + \ldots + a_0^v$ — его характеристический полином. Тогда для его коэффициентов выполняются условия (6), и,

сверх того, $a_0^v = (-1)^n y$. Полагая $a_0 = (-1)^n y$ в (6), мы получим для остальных коэффициентов систему линейных уравнений с коэффициентами из K. Поэтому, используя слабую аппроксимацию для поля K, можно найти набор $(a_0, \ldots, a_{n-1}) \in L^n$, удовлетворяющий (6), такой, что $a_0 = (-1)^n y$, и достаточно близкий к $(a_0^v, \ldots, a_{n-1}^v)$ по всем $v \in S$ в указанном смысле. Рассмотрим L-алгебру $P = L[t]/(f(t))$, где $f(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0$, обозначим через x образ t в P и определим инволюцию σ алгебры P условиями: ограничение $\sigma|_L$ совпадает с τ и $\sigma(x) = x^{-1}$ (в силу условий (6) такая инволюция существует). Нам остается установить существование L-вложения θ: $P \to A$ как алгебр с инволюциями, ибо тогда элемент $\theta(x)$ является искомым.

Для этого заметим, что из наших построений вытекает, во-первых, существование вложений θ_v: $P \otimes_K K_v \to A \otimes_K K_v$ как алгебр с инволюциями для всех $v \in V^K$, и, во-вторых, существование вложения ε: $P \to A$ как алгебр без инволюций. Действительно, существование θ_v для $v \notin S_0$ вытекает из леммы 26. Чтобы установить существование θ_v для $v \in S_0$, достаточно найти такой элемент $x_v' \in A \otimes_K K_v$, что $f(x_v') = 0$, алгебра $(L \otimes_K K_v)[x_v']$ имеет размерность n над $L \otimes_K K_v$ и $\tau(x_v')x_v' = 1$. Но по построению такой элемент можно указать уже в $(L \otimes_K K_v)[x_v]$. Используя критерий вложимости поля в простую алгебру в качестве максимального подполя (см. § 1.5, п. 1), легко показать, что существование ε вытекает из существования θ_v, если установить, что P является полем. Рассмотрим K-алгебру неподвижных точек $F = P^\sigma$. Тогда по построению $P \otimes_K K_{v_1} \xrightarrow{\theta_{v_1}} (L \otimes_K K_{v_1})[x_1] \simeq L \otimes_K E$, откуда следует, что $F \otimes_K K_{v_1} \simeq E$ является неразветвленным расширением поля K_{v_1} степени n; в частности, F — поле. Вложим поле F в алгебраическое замыкание $\bar{K}$ поля K и покажем, что для его нормального замыкания M имеем $M \cap L = K$. Для этого используем нормирование v_2. По построению $P \otimes_K K_{v_2} = (F \otimes_K L) \otimes_K K_{v_2} = (F \otimes_K K_{v_2}) \otimes_{K_{v_2}} (L \otimes_K K_{v_2}) \simeq (L \otimes K_{v_2})^n$, откуда $F \otimes_K K_{v_2} \simeq K_{v_2}^n$, и, значит, $M \subset K_{v_2}$, в то время как $[L \otimes_K K_{v_2} : K_{v_2}] = 2$. В частности, $P = F \otimes_K L = FL$ является полем.

Посредством ε отождествим P с подалгеброй в A и продолжим инволюцию σ до инволюции всей алгебры A, причем продолжение будем обозначать той же буквой. Тогда существует такой симметрический элемент $t \in A^*$, что $\sigma(z) = t\tau(z)t^{-1}$ для всех $z \in A$ (см. лемму 2.10). По теореме Сколема — Нётер любое другое вложение P в A имеет вид $x \mapsto s^{-1}xs$, $s \in A^*$, и наша задача сводится к осуществлению выбора элемента s таким образом, чтобы получающееся вложение было согласовано с инволюциями, т. е. $s\sigma(z)s^{-1} = \tau(szs^{-1})$ для всех $z \in P$. Простое

вычисление показывает, что последнее условие эквивалентно включению $s\tau(s)t^{-1} \in Z_A(P) = P$. Таким образом, нам надо найти элемент $b \in P^*$, для которого уравнение $s\tau(s) = bt$ имеет решение $s \in A^*$. Для этого, согласно теореме Ландера, достаточно выбрать $b \in P^*$ таким образом, чтобы существовали локальные решения $s_v \in (A \otimes_K K_v)^*$. При этом, как мы отметили после доказательства теоремы Ландера, для $v \in V_f^K$ условие разрешимости уравнения $s\tau(s) = bt$ в $A \otimes_K K_v$ (в предположении, что $\tau(bt) = bt$) можно записать в виде $\mathrm{Nrd}_{A/L}(bt) \in N_{L \otimes_K K_v/K_v}((L \otimes_K K_v)^*)$. Итак, осталось найти такой $b \in P$, чтобы выполнялись условия

$$\mathrm{Nrd}_{A/L}(bt) \in N_{L/K}(L^*), \tag{7}$$

$$\tau(bt) = bt, \tag{8}$$

и, сверх того, уравнение $s\tau(s) = bt$ было разрешимо в $A \otimes_K K_v$ для $v \in V_\infty^K$. Условие (8) эквивалентно тому, что $\sigma(b) = b$, т. е. $b \in F$. Тогда (7) перепишется в виде

$$r = \mathrm{Nrd}_{A/L}(t) \in N_{F/K}(b)^{-1} N_{L/K}(L^*). \tag{9}$$

При этом из существования θ_v вытекает, что соответствующая задача разрешима всюду локально, т. е. для любого $v \in V^K$ существует $b_v \in (F \otimes_K K_v)^*$, для которого уравнение $s\tau(s) = b_v t$ имеет решение $s_v \in (A \otimes_K K_v)$. В частности,

$$r \in N_{F \otimes_K K_v/K_v}((F \otimes_K K_v)^*) N_{L \otimes_K K_v/K_v}((L \otimes_K K_v)^*). \tag{10}$$

Воспользуемся теперь тем обстоятельством, что для пары полей F, L имеет место мультинорменный принцип Хассе, ибо выполняются условия предложения 11 (тот факт, что нормальное замыкание F пересекается с L по K, был установлен выше; а справедливость норменного принципа для L/K вытекает из теоремы Хассе). Поэтому из (10) вытекает, что

$$r = N_{F/K}(b_0)^{-1} N_{L/K}(l_0) \tag{11}$$

для подходящих $b_0 \in F^*$, $l_0 \in L^*$. Для завершения рассуждений остается построить такие элементы $b \in F^*$, $l \in L^*$, что опять $r = N_{F/K}(b) N_{L/K}(l)$ и уравнение $s\tau(s) = bt$ разрешимо в $(A \otimes_K K_v)^*$ для $v \in V_\infty^K$. Для каждого $v \in V^K$ множество Φ_v элементов вида $s\tau(s)$, $s \in (A \otimes_K K_v)^*$ открыто во множестве Σ_v симметрических элементов. Поэтому если уравнение $s\tau(s) = b_v t$ разрешимо, то разрешимо и любое уравнение $s\tau(s) = bt$, где $b \in F \otimes_K K_v$ достаточно близко к b. Ясно также, что $r = N_{F \otimes_K K_v/K_v}(b_v) N_{L \otimes_K K_v/K_v}(l_v)$ для подходящего $l_v \in L \otimes_K K_v$. Таким образом, достаточно доказать следующее утверждение:

Лемма 27. *Множество* $X=\{(b, l)\in F^*\times L^*\mid r\in N_{F/K}(b)^{-1}N_{L/K}(l)\}$ *плотно в* $\prod_{v\in V_\infty^K} X_v$, *где* $X_v=\{(b_v, l_v)\in(F\otimes_K K_v)^*\times(L\otimes_K K_v)^*\mid r=$ $=N_{F\otimes_K K_v/K_v}(b_v)^{-1}\cdot N_{L\otimes_K K_v/K_v}(l_v)\}$.

Доказательство. Утверждение леммы означает, что для многообразия $C=\{b, l)\in\mathbf{R}_{F/K}(\boldsymbol{G}_m)\times\mathbf{R}_{L/K}(\boldsymbol{G}_m)\mid r=N_{F/K}(b^{-1})N_{L/K}(l)\}$ выполняется слабая аппроксимация относительно множества $S=V_\infty^K$. Имеем $c=(b_0, l_0)\in C_K$ (см. (11)) и $C=cT$, где T — подтор в $\mathbf{R}_{F/K}(\boldsymbol{G}_m)\times\mathbf{R}_{L/K}(\boldsymbol{G}_m)$, задаваемый уравнением $N_{F/K}(b)=N_{L/K}(l)$. При этом плотность C_K в C_S эквивалентна плотности T_K в T_S, т. е. слабой аппроксимации для T. Однако в случае $S=V_\infty^K$ последнее свойство имеет место для любого тора (см. предложение 7.8). Доказательство леммы 27, а вместе с тем и теоремы 28 завершено.

Упражнения. 1) Отбрасывая в приведенном доказательстве рассуждения, связанные со спецификой унитарной ситуации, получить доказательство теоремы Эйхлера о нормах.

2) Получить эрмитов аналог теоремы 28. Более точно, показать, что для $y\in K^*$ уравнение $\mathrm{Nrd}_{A/L}(x)=y$ имеет решение $x\in A^*$ такое, что $\tau(x)=x$, если для любого $v\in V^K$ оно имеет решение $x_v\in A\otimes_K K_v$ такое, что $\tau(x_v)=x_v$.

§ 6.8. Доказательство теорем 4 и 6: группы исключительных типов

В настоящем параграфе мы завершим доказательство теорем 4 и 6, рассмотрев группы типов ${}^{3,6}D_4$, ${}^{1,2}E_6$, E_7, E_8, F_4 и G_2. Всюду через G обозначается простая односвязная K-группа, относящаяся к одному из указанных типов, а через G_0 — квазиразложимая K-группа того же внутреннего типа, что и G.

Вначале разберем наиболее простой случай групп типа G_2 и дадим редукцию случая групп типа F_4 к группам типа D_4.

Группы типа G_2. Покажем вначале, что если K — локальное либо чисто мнимое числовое поле, то $H^1(K, G_0)=1$. Пусть $\xi\in$ $\in H^1(K, G_0)$. Тогда согласно предложению 19 найдется такой K-определенный максимальный тор $T\subset G_0$, что ξ лежит в образе отображения $H^1(K, T)\xrightarrow{\varphi}H^1(K, G_0)$. Покажем, что последнее отображение на самом деле тривиально. Обозначим через $R=R(T, G)$ соответствующую систему корней, и пусть $R_0\subset R$ подмножество, состоящее из длинных корней. Из описания системы корней типа G_2 (таблица IX в книге Бурбаки [4], гл. IV—VI) вытекает, что R_0 образует замкнутую подсистему корней в R типа A_2. Отсюда следует, что подгруппа $H\subset G_0$, порожденная корневыми группами G_α для $\alpha\in R_0$, является простой группой типа A_2. Далее, система R_0, очевидно, инвариантна при всех автоморфизмах системы R, поэтому автоморфизмы

$\sigma \in \mathrm{Gal}(\bar{K}/K)$ переставляют группы G_α, $\alpha \in R_0$, между собой, и таким образом группа H определена над K. Наконец, несложное вычисление с корнями, которое мы опускаем, позволяет установить, что для H выполняются условия критерия односвязности (см. теорему 2.6), так что H односвязна. Из справедливости теорем 4 и 6 для групп классических типов (см. предыдущий параграф) тогда вытекает, что $H^1(K, H) = 1$. Но φ, очевидно, раскладывается в композицию $H^1(K, T) \to H^1(K, H) \to H^1(K, G_0)$, и поэтому φ тривиально. Итак, $H^1(K, G_0) = 1$. Поскольку группа G_0 является одновременно односвязной и присоединенной, последнее означает, что G_0 является единственной K-формой типа G_2, т. е. любая K-группа этого типа разложима над K. Поэтому на самом деле $H^1(K, G) = 1$ для любой K-группы G типа G_2.

Нам остается показать, что для любого не вполне мнимого числового поля K отображение $H^1(K, G) \xrightarrow{\rho} \prod_{v \in V_\infty^K} H^1(K_v, G)$ имеет тривиальное ядро. Эта часть рассуждений в той или иной степени повторяется для групп всех типов, кроме E_6, и основывается на следующей лемме, которую мы докажем в самой общей ситуации.

Лемма 28. *Пусть G — полупростая алгебраическая группа, определенная над произвольным полем K. Предположим, что G обладает подгруппой Бореля B, определенной над квадратичным расширением L/K, причем $T = B \cap \sigma(B)$ — максимальный K-тор в G (σ — образующая группы $\mathrm{Gal}(L/K)$). Тогда любой коцикл $\xi \in Z^1(L/K, G)$ эквивалентен коциклу $\xi' \in Z^1(L/K, T)$. При этом если поле K — числовое и $\xi \in Z^1(L/K, G)$ представляет элемент из $\mathrm{Ker}\left(H^1(K, G) \to \prod_{v \in V_\infty^K} H^1(K_v, G)\right)$, то и коцикл $\xi' \in Z^1(L/K, T)$ представляет элемент из $\mathrm{Ker}\left(H^1(K, T) \to \prod_{v \in V_\infty^K} H^1(K_v, T)\right)$.*

Доказательство. Коцикл ξ задается элементом $a_\sigma \in G_L$ таким, что $a_\sigma \sigma(a_\sigma) = 1$. Обозначим через H группу $\mathbf{R}_{L/K}(G)$. Автоморфизм σ индуцирует K-определенный автоморфизм группы $H \simeq \mathbf{R}_{L/K}(G)$, который мы будем обозначать той же буквой. Введем в рассмотрение K-определенное подмногообразие $Z \subset H$, задаваемое уравнением $h\sigma(h) = 1$. Тогда коциклы $\xi \in Z^1(L/K, G)$ отвечают точкам из Z_K, а группа H действует на Z по формуле $(h, z) \mapsto h^{-1} z \sigma(h)$, причем это действие K-определено и транзитивно. Так как H_K плотно в H (теорема 2.2), то отсюда следует, что множество коциклов, эквивалентных ξ, образует плотное по Зарисскому подмножество в Z. С другой стороны, из соотношения $T = B \cap \sigma(B)$ вытекает, что $\sigma(B)$ совпадает с подгруппой B^-, противоположной B. Обозначим через U и U^-

унипотентные радикалы подгрупп B и B^- соответственно. Из разложения Брюа вытекает, что морфизм-произведение μ: $U \times \times T \times U^- \to G$ является определенным над L изоморфизмом на открытое подмножество $W \subset G$. Отсюда следует, что некоторый эквивалентный ξ коцикл задастся элементом $b_\sigma \in W_L$. Пусть $b_\sigma = u_1 t u_2$, где $u_1 \in U_L$, $t \in T_L$, $u_2 \in U_L^-$. Тогда из условия $\sigma(b_\sigma) = b_\sigma^{-1}$, единственности разложения Брюа и того, что $\sigma(U) = U^-$, $\sigma(U^-) = U$, вытекают соотношения $\sigma(u_1) = u_2^{-1}$, $\sigma(u_2) = u_1^{-1}$ и $\sigma(t) = t^{-1}$. Покажем, что коцикл ξ', определяемый элементом $a'_\sigma = t$, является искомым. Действительно, $a'_\sigma = = t = u_1^{-1} u_1 t u_2 u_2^{-1} = u_1^{-1} b_\sigma \sigma(u_1)$, т. е. коцикл ξ' эквивалентен ξ в $Z^1(L/K, G)$.

Чтобы получить в числовом случае коцикл $\xi' \in Z^1(L/K, T)$, задающий элемент из $\operatorname{Ker}\left(H^1(K, T) \to \prod_{v \in V_\infty^K} H^1(K_v, T)\right)$, предыдущие рассуждения следует немного уточнить. А именно, по условию для каждого вещественного нормирования v поля K со свойством $L_w = LK_v \neq K_v$ (множество таких v мы обозначим через S) найдется элемент $g_v \in G_{L_w}$, удовлетворяющий соотношению $a_\sigma = g_v^{-1} \sigma(g_v)$. Рассмотрим группу $B = \mathbf{R}_{L/K}(T)$, подмногообразие $D \subset B$, задающее коциклы из $Z^1(L/K, T)$, и действие B на D, аналогичное описанному выше действию H на Z. Тогда из предложения 3.3 вытекает существование такого открытого подмножества $\Delta_v \subset T_{L_w} \simeq B_{K_v}$, что если $t \in \Delta_v$ и $t\sigma(t) = 1$, то коцикл в $Z^1(L_w/K_v, T)$, определяемый элементом t, тривиален. Из разложения Брюа вытекает, что множество $F_v = = U_{L_w} \Delta_v U_{L_w}^-$ открыто в G_{L_w} в w-адической топологии. В силу предложения 7.9 G_L плотно в $\prod_{v \in S,\, w \mid v} G_{L_w}$. С другой стороны, если выбирать элемент g достаточно близким к g_v^{-1}, то можно сделать элемент $g^{-1} a_\sigma \sigma(g)$ произвольно близким к единице. Отсюда следует существование такого $g \in G_L$, что $b_\sigma = g^{-1} a_\sigma \sigma(g) \in \in F_v$ для всех $v \in S$. Тогда если $b_\sigma = u_1 t u_2$ — соответствующее разложение Брюа, то, как мы видели выше, коцикл ξ', задаваемый элементом $a'_\sigma = t$, эквивалентен ξ. При этом, по построению, $t \in \Delta_v$, так что ξ' становится тривиальным в $H^1(L_w/K_v, T)$. Остается заметить, что $L \subset K_v$ для $v \in V_\infty^K \setminus S$ и ξ' автоматически тривиален в $H^1(K_v, T)$. Лемма доказана.

Вернемся теперь к нашей K-группе G типа G_2. Пусть $\xi \in \in \operatorname{Ker} \rho$ и $L = K(\sqrt{-1})$, $\operatorname{Gal}(L/K) = \langle \sigma \rangle$. Согласно уже доказанному, ξ становится тривиальным коциклом в $H^1(L, G)$, т. е. $\xi \in H^1(L/K, G)$, и G является L-разложимой. Используя лемму 17, выберем L-определенную подгруппу Бореля $B \subset G$ такую, что $T = B \cap \sigma(B)$ — максимальный K-тор в G. Согласно

лемме 28, переходя к эквивалентному коциклу, можно без ограничения общности предполагать, что $\xi \in \operatorname{Ker}\left(H^1(K, T) \xrightarrow{\theta} \prod_{v \in V_\infty^K} H^1(K_v, T)\right)$. Но выше мы видели, что любой K-определенный тор $T \subset G$ содержится в некоторой односвязной K-подгруппе $H \subset G$ типа A_2. Поэтому из справедливости принципа Хассе для H вытекает, что ξ является тривиальным коциклом в $H^1(K, H)$, и тем более в $H^1(K, G)$.

Отметим, что доказательство теорем 4 и 6 для группы G типа G_2 можно было получить, воспользовавшись геометрической реализацией G как группы автоморфизмов некоторой K-определенной алгебры октав, однако мы предпочли дать рассуждение, основанное на структурных соображениях, тем более что оно содержит ряд типичных моментов.

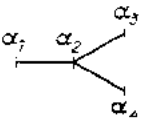
Группы типа F_4. Этот тип редуцируется к группам типа D_4 точно так же, как тип G_2 редуцировался к A_2. Пусть вначале поле K является локальным или вполне мнимым числовым, $\xi \in H^1(K, G_0)$. С помощью предложения 19 найдем такой максимальный K-тор $T \subset G_0$, что ξ лежит в образе отображения $H^1(K, T) \to H^1(K, G_0)$. Предположим теперь, что теоремы 4 и 6 доказаны для групп типа D_4 (включая внешние формы типов ${}^3D_4$ и ${}^6D_4$). Тогда для доказательства тривиальности ξ достаточно построить содержащую T односвязную K-определенную подгруппу $H \subset G$ типа D_4. Но из явного описания системы корней типа F_4 (см. таблицу VIII в книге Бурбаки [4]) вытекает, что таковой является подгруппа, порожденная корневыми подгруппами G_α, где α пробегает все длинные корни системы $R = R(T, G)$. Здесь также группа G_0 является одновременно односвязной и присоединенной, поэтому из тривиальности $H^1(K, G_0)$ получаем, что любая K-группа G типа F_4 разложима, а следовательно, $H^1(K, G) = 1$.

Доказательство принципа Хассе для группы G типа F_4 над числовым полем K, не являющимся вполне мнимым, дословно повторяет соответствующее рассуждение для типа G_2.

Группы типа ${}^{3,6}D_4$. Как обычно, покажем вначале, что $H^1(K, G_0) = 1$, если поле K — локальное или вполне мнимое числовое. Пусть $\xi \in H^1(K, G_0)$ и $G = {}_\xi G_0$. Установим, что G является K-квазиразложимой, т. е. $G \simeq G_0$. Предположим противное. Тогда возможны два случая: G изотропна над K и G анизотропна над K. В первом случае единственная возможность для индекса G имеет вид

(см. Титс [2]). Обозначим через S максимальный K-разложимый тор в G, и пусть T — некоторый K-определенный максимальный тор в его централизаторе $C = C_G(S)$. Согласно предложению 18 $G_0 = {}_\mu G$ для подходящего коцикла $\mu \in H^1(K, T)$, поэтому нам достаточно показать, что $H^1(K, C) = 1$. Но полупростая часть $H = [C, C]$ является односвязной K-группой типа $A_1 \times A_1 \times A_1$, и поэтому $H^1(K, H) = 1$. С другой стороны, факторгруппа C/H является одномерным K-разложимым тором, так что $H^1(K, C/H) = 1$. Поэтому из точной последовательности $H^1(K, H) \to H^1(K, C) \to H^1(K, C/H)$ вытекает, что $H^1(K, C) = 1$, и требуемое доказано.

Пусть теперь G K-анизотропна. Обозначим через L минимальное расширение Галуа поля K, над которым G_0 становится внутренней формой. Тогда $\mathscr{G} = \mathrm{Gal}(L/K)$ есть либо циклическая группа третьего порядка, либо симметрическая группа S_3. Разберем первый случай. Поскольку над L группа G_0 становится группой типа ${}^1D_4$, то согласно уже доказанному $H^1(L, G_0) = 1$; следовательно, над L $G \simeq G_0$ — разложимая группа. Занумеруем корни L-разложимого тора следующим образом:



и обозначим через P L-определенную параболическую подгруппу $P_\Delta \subset G$, где $\Delta = \{\alpha_2, \alpha_3, \alpha_4\}$. Простой подсчет показывает, что $\dim G = 28$, $\dim P = 22$, т. е. $\operatorname{codim} P = 6$. Пусть σ — образующая группы $\mathscr{G}$. Положим $C = P \cap \sigma(P) \cap \sigma^2(P)$. Ясно, что C является K-определенной подгруппой, которая редуктивна в силу K-анизотропности G. При этом $\dim C \geqslant \dim G - 3 \operatorname{codim} P = 10$. Выясним строение группы C. Пусть $H = [C, C]$ — полупростая часть C. По построению H должна содержаться в полупростой части P' группы P, которая является простой L-разложимой группой типа A_3. Кроме того, поскольку для групп меньшей размерности теоремы 4 и 6, а значит, и теоремы 5, 25 уже доказаны, то из K-анизотропности H вытекает, что все ее простые компоненты имеют тип A_i, и поэтому для типа H имеются лишь следующие возможности: A_1, $A_1 \times A_1$, A_2 и A_3. Первые два случая не реализуются из соображений размерности, а последний — в силу того, что здесь H должна совпадать с P' и, следовательно, является K-анизотропной группой типа A_3, которая становится разложимой над кубическим расширением K, что невозможно. Итак, H имеет тип A_2, так что $\dim H = 8$, и, значит, $C = HS$ — почти прямое произведение, где S — двумерный K-тор. Покажем, что S является L-разложимым. Обозначим

через S_0 максимальный L-разложимый подтор в S. Из наших построений вытекает, что $S_0 \neq (e)$, и поэтому остается исключить возможность $\dim S_0 = 1$. Так как L/K — расширение Галуа, то S_0 определен над K, и, следовательно, имеет вид $S_0 = \mathbf{R}^{(1)}_{E/K}(\boldsymbol{G}_m)$, где E/K — квадратичное расширение. Но такой тор остается анизотропным над L — противоречие. Вкладывая теперь S в максимальный L-разложимый тор и замечая, что $H \subset Z_G(S)$, получаем, что H также является L-разложимой. В частности, H — внутренняя форма над K, ибо $[L:K]=3$, т. е. $H = \boldsymbol{SL}_1(D)$, где D — тело индекса 3 над K такое, что $D \otimes_K L = M_3(L)$. Из последнего условия вытекает, что L вкладывается в D и, следовательно, определяет максимальный K-определенный и разложимый над L тор $S' = \mathbf{R}^{(1)}_{L/K}(\boldsymbol{G}_m) \subset H$. Тогда $T = SS'$ — максимальный K-определенный тор в C и G, который анизотропен над K и разложим над L. Отсюда следует, что для любого характера $\chi \in \mathbf{X}(T)$ имеем $\chi + \sigma(\chi) + \sigma^2(\chi) = 0$. Поэтому для любого корня $\alpha \in R(T, G)$ группа G_{Σ_α}, порожденная корневыми группами G_γ для $\gamma \in \Sigma_\alpha = \{\alpha, \sigma(\alpha)\}$, является K-определенной односвязной группой типа A_2. Положим $T_{\Sigma_\alpha} = T \cap G_{\Sigma_\alpha}$ и выберем такие два корня $\alpha, \beta \in R(T, G)$, что $T = T_{\Sigma_\alpha} \times T_{\Sigma_\beta}$ (читателю следует убедиться в их существовании). Согласно предложению 18 $G_0 = {}_\mu G$ для подходящего $\mu = \{a_\tau\} \in H^1(K, T)$. Покажем, что μ является тривиальным в G. Пусть $\mu_\alpha = \{a^\alpha_\tau\} \in H^1(K, T_{\Sigma_\alpha})$ и $\mu_\beta = \{a^\beta_\tau\} \in H^1(K, T_{\Sigma_\beta})$ — проекции μ на T_{Σ_α} и T_{Σ_β} соответственно. Так как $H^1(K, G_{\Sigma_\beta}) = 1$, то $a^\beta_\tau = g^{-1}\tau(g)$ для подходящего $g \in G_{\Sigma_\beta}$. Имеем $b_\tau = g a_\tau \tau(g)^{-1} = g a^\alpha_\tau g^{-1} \in F = g G_{\Sigma_\alpha} g^{-1}$. Остается установить, что группа F определена над K, ибо тогда $H^1(K, F) = 1$ и $\{b_\tau\}$ тривиален в G. Для произвольного $\tau \in \mathrm{Gal}(\bar{K}/K)$

$$\tau(F) = \tau(g)\, G_{\Sigma_\alpha} \tau(g)^{-1} = g a^\beta_\tau G_{\Sigma_\alpha} (a^\beta_\tau)^{-1} g^{-1} = F,$$

ибо $a^\beta_\tau \in T_{\Sigma_\beta}$ нормализует G_{Σ_α}. Таким образом, в случае $[L:K]=3$ изоморфизм $G \simeq G_0$ установлен.

Пусть теперь $\mathscr{G} = \mathrm{Gal}(L/K) \simeq S_3$. Обозначим через E квадратичное расширение K, содержащееся в L. Согласно уже доказанному, группа G становится квазиразложимой над E. Но тогда, как и при доказательстве теоремы 26, устанавливается, что G изотропна над K, а изотропный случай уже рассмотрен.

Итак, во всех случаях $G = {}_\xi G_0 \simeq G_0$. Это означает, что ξ проектируется в тривиальный коцикл в соответствующей присоединенной группе, т. е. ξ лежит в $H^1(K, Z)$, где Z — центр G_0.

Но тогда $\xi \in H^1(K, T_0)$, где T_0 — максимальный тор K-определенной подгруппы Бореля группы G_0. Анализ индекса

группы G_0 показывает, что T_0 имеет вид $T_0 = \mathbf{G}_m \times \mathbf{R}_{M/K}(\mathbf{G}_m)$, где $M \subset L$ — подполе третьей степени над K, так что $H^1(K, T_0) = 1$, и тем более ξ тривиален в $H^1(K, G_0)$. Таким образом, доказательство тривиальности $H^1(K, G_0)$ завершено.

Пусть теперь K — локальное поле. Так как тривиальность $H^1(K, G_0)$ уже доказана, то из предложения 15 вытекает, что любая простая односвязная K-группа G типов ${}^{3,6}D_4$ квазиразложима над K, т. е. $G \simeq G_0$. Поэтому $H^1(K, G) = H^1(K, G_0) = 1$, и теорема 4 доказана.

Для доказательства теоремы 6 нам понадобится

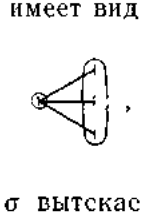
Лемма 29. *Пусть G — простая односвязная группа типа ${}^{3,6}D_4$ над числовым полем K, E/K — минимальное расширение Галуа, над которым G становится внутренней формой. Тогда существует квадратичное расширение L/K со следующими свойствами:*

1) *L и E линейно разделены над K;*
2) *L является вполне мнимым;*
3) *G становится квазиразложимой над L.*

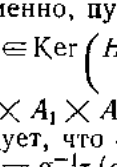
Доказательство получается несложным уточнением рассуждений из доказательства предложения 15 и оставляется читателю в качестве упражнения.

Пусть теперь $\xi \in \operatorname{Ker}\left(H^1(K, G) \xrightarrow{\rho} \prod_{v \in V_\infty^K} H^1(K_v, G)\right)$ и L/K — расширение, построенное в лемме 29. Так как над L $G \simeq G_0$, то согласно уже доказанному $H^1(L, G) = 1$, поэтому $\xi \in H^1(L/K, G)$. Пусть $B \subset G$ — такая L-определенная подгруппа Бореля, что $T = B \cap \sigma(B)$ — максимальный K-тор в G, где σ — образующая $\operatorname{Gal}(L/K)$ (см. лемму 17). Применяя лемму 28 и переходя к эквивалентному коциклу, можно считать, что $\xi = \{a_\tau\} \in \operatorname{Ker}\left(H^1(K, T) \to \prod_{v \in V_\infty^K} H^1(K_v, T)\right)$. Для дальнейшего нам понадобится описание действия σ на корни из $R(T, G)$. Более точно, поскольку полем разложения для T является LE, то действие $\operatorname{Gal}(L/K)$ на $\mathbf{X}(T)$ определить нельзя, а следует рассмотреть действие всей группы $\operatorname{Gal}(LE/K)$. По этой причине нам придется продолжить σ на LE, причем в силу линейной разделенности L и E можно считать, что это продолжение действует на E тривиально, и мы будем обозначать его той же буквой. Так как G становится над E внутренней формой, то σ обязан

действовать на $\mathbf{X}(T)$ как элемент группы Вейля $W(T, G)$. С другой стороны, поскольку $T = B \cap \sigma(B)$, то σ переводит положительные корни, связанные с B, в отрицательные. Но в группе Вейля системы корней типа D_4 единственным элементом с таким свойством является (-1) (см. таблицу IV в книге Бурбаки [4]). Поэтому σ действует на $\mathbf{X}(T)$ умножением на -1. Занумеруем простые корни в $R(T, G)$ следующим образом:



Поскольку индекс G над L имеет вид



,

то из описания действия σ вытекает, что подгруппа $G_1 = G_{\alpha_2}$ и подгруппа G_2, порожденная G_{α_i} $(i = 1, 3, 4)$, являются K-определенными. Положим $T_i = T \cap G_i$. Тогда $T = T_1 \times T_2$. Далее применяется уже использованный нами прием тривиализации коцикла ξ «по частям». А именно, пусть $\xi_i = \{a_\tau^i\} \in H^1(K, T_i)$ — проекция ξ на T_i; ясно, что $\xi_i \in \operatorname{Ker}\left(H^1(K, T_i) \to \prod_{v \in V_\infty^K} H^1(K_v, T_i)\right)$. Так как G_2 имеет тип $A_1 \times A_1 \times A_1$, то для нее выполняется принцип Хассе, откуда следует, что ξ_2 определяет тривиальный коцикл в $H^1(K, G_2)$, т. е. $a_\tau^2 = g^{-1}\tau(g)$ для подходящего $g \in G_2$. Тогда $b_\tau = g a_\tau \tau(g)^{-1} = g a_\tau^1 g^{-1} \in F = g G_1 g^{-1}$. Как и выше, устанавливается, что группа F и тор $T_1' = g T_1 g^{-1}$ определены над K. Далее, рассмотрим морфизм $\varphi\colon T_1 \to T_1'$, $t \mapsto g t g^{-1}$ и покажем, что он определен над K. Действительно, для любого $t \in T_1$ и любого $\tau \in \operatorname{Gal}(\overline{K}/K)$ имеем

$$(\tau\varphi)(t) = \tau(g)\, t\, \tau(g)^{-1} = g\,(g^{-1}\tau(g))\, t\, (g^{-1}\tau(g))^{-1} g^{-1} = g t g^{-1} = \varphi(t),$$

т. е. $\tau\varphi = \varphi$, ибо $g^{-1}\tau(g) = a_\tau^2 \in T_2$. Отсюда следует, что $\xi_1' = \{b_\tau\} = \varphi(\xi_1)$ лежит в $\operatorname{Ker}\left(H^1(K, T_1') \to \prod_{v \in V_\infty^K} H^1(K_v, T_1')\right)$, и поскольку для F выполняется принцип Хассе (F принадлежит типу A_1), то ξ_1' является тривиальным коциклом в $H^1(K, F)$. Но тогда ξ является тривиальным коциклом в $H^1(K, G)$, что и требовалось.

Группы типов E_6, E_7, E_8 (подготовительный этап). Рассмотрения предыдущих типов основывались на том факте, что легко указывался максимальный тор данной группы, который целиком или по частям вкладывался в группы меньшего ранга, для которых теоремы 4 и 6 уже доказаны. В случае групп серии E этот метод наталкивается на значительные трудности, ибо для этих групп априори невозможно указать поле разложения, имеющее сравнительно небольшую степень над K. Максимум, что в этой ситуации удается сделать, — построить поле разложения в виде башни 2-, 3- и 5-расширений. Для этого нам понадобится

Предложение 21. *Пусть G — произвольная K-группа одного из типов E_6, E_7 или E_8, $T \subset G$ — максимальный K-определенный тор. Тогда порядок любого элемента группы $H^1(K, T)$ имеет вид $2^\alpha 3^\beta$, если G — группа типа E_6 или E_7, и вид $2^\alpha 3^\beta 5^\gamma$, если G — группа типа E_8.*

Доказательство. Пусть L — минимальное поле разложения тора T, $\mathscr{G} = \mathrm{Gal}(L/K)$. Тогда $\mathscr{G}$ действует автоморфизмами на системе корней $R = R(T, G)$, так что возникает гомоморфизм $\mathscr{G} \to \mathrm{Aut}(R)$, который является вложением по той причине, что корни порождают векторное пространство $\mathbf{X}(T) \otimes_{\mathbf{Z}} \mathbf{R}$. В нашей ситуации группа $\mathrm{Aut}\, R$ совпадает с группой Вейля $W(R)$, если R — система типов E_7 или E_8, и содержит $W(R)$ в качестве подгруппы индекса 2 для типа E_6. Группы Вейля системы корней рассматриваемых типов имеют следующие порядки (см. таблицы V—VII в книге Бурбаки [4]): $[W(E_6)] = 2^7 \cdot 3^4 \cdot 5$, $[W(E_7)] = 2^{10} \cdot 3^4 \cdot 5 \cdot 7$ и $[W(E_8)] = 2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$. Поэтому сразу можно утверждать, что порядок любого элемента из $H^1(K, T)$ имеет вид $2^\alpha \cdot 3^\beta \cdot 5^\gamma$ в случае E_6 и вид $2^\alpha \cdot 3^\beta \cdot 5^\gamma \cdot 7^\delta$ — в случае E_7 и E_8. Наша цель — отсечь в этих значениях 5-компоненту для E_6 и E_7 и 7-компоненту для E_7 и E_8. С этой целью доказывается

Лемма 30. *Пусть H — определенная над K группа типа ${}^{1,2}D_n$ $(n \geqslant 4)$, $S \subset H$ — максимальный K-определенный тор. Тогда $H^1(K, S)$ является 2-группой.*

Доказательство. Достаточно доказать лемму для случая, когда H есть либо $\boldsymbol{SO}_{2n}(f)$ либо $\boldsymbol{SU}_n(D, f)$, т. е. изоморфна над K специальной ортогональной группе, ибо произвольная группа H' данного типа входит в диаграмму

$$\begin{tikzcd} & \tilde{H} \arrow[dl, "\pi"'] \arrow[dr, "\pi'"] & \\ H & & H' \end{tikzcd} \tag{1}$$

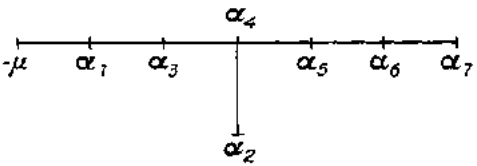
где π и π' — изогении, ядра которых являются 2-группами, и тогда

для любого K-тора $S' \subset H'$ и любого $p \neq 2$ p-компоненты групп $H^1(K, S')$ и $H^1(K, S)$, где $S = \pi((\pi')^{-1}(S'))$, изоморфны. В этом случае над R тор S приводится к виду $\{s = \operatorname{diag}(s_1, s_1^{-1}, \ldots, s_n, s_n^{-1})\}$, и поэтому $\mathbf{X}(T) = \mathbb{Z}\varepsilon_1 \oplus \ldots \oplus \mathbb{Z}\varepsilon_n$, где $\varepsilon_i(s) = s_i$. При этом система корней $R(S, H)$ состоит из $\pm\varepsilon_i \pm \varepsilon_j$ $(i \neq j)$, а группа автоморфизмов $\operatorname{Aut}(R(S, H))$ состоит из преобразований, которые ε_i переводят в $\pm\varepsilon_j$, т. е. является полупрямым произведением $A \cdot B$, где $B = \prod_{i=1}^{n} \{\pm 1\}$, а $A = S_n$ действует на ε_i перестановками индексов. Выше мы видели, что группа Галуа $\mathscr{H} = \operatorname{Gal}(E/K)$ минимального поля разложения тора S вкладывается в $\operatorname{Aut}(R(S, H))$, причем утверждение леммы эквивалентно тому, что для любого $p \neq 2$ группа $H^1(\mathscr{H}_p, S)$ тривиальна, где $\mathscr{H}_p$ — силовская p-подгруппа в $\mathscr{H}$. Положим $F = E^{\mathscr{H}_p}$. Так как $p \neq 2$, то $\mathscr{H}_p$ сопряжена в $\operatorname{Aut}(R(S, H))$ подгруппе группы A, и поэтому существует базис группы характеров $\mathbf{X}(S)$, на котором $\mathscr{H}_p$ действует перестановками. Отсюда следует, что тор S является квазиразложимым над F, и поэтому $H^1(\mathscr{H}_p, S) = H^1(E/F, S) = 1$. Лемма доказана.

Вернемся к доказательству предложения 21. Нам надо показать, что $H^1(\mathscr{G}_5, T) = 1$ в случае систем типов E_6 и E_7, где $\mathscr{G}_5$ — силовская 5-подгруппа в $\mathscr{G}$. Из рассмотрения диаграмм Дынкина вытекает, что система R в данном случае содержит замкнутую подсистему R_0 типа D_5. Имеем $[W(D_5)] = 2^8 \cdot 3 \cdot 5$, поэтому, анализируя указанные порядки групп Вейля $W(E_6)$ и $W(E_7)$, заключаем, что силовская 5-подгруппа в $W(R_0)$ является в то же время силовской в $W(R)$. Отсюда следует, что $\mathscr{G}_5$ сопряжена подгруппе $W(D_5)$, и, значит, всегда можно указать систему $R_0 \subset R$ типа D_5, инвариантную относительно $\mathscr{G}_5$. Пусть H — подгруппа в G типа D_5, порожденная корневыми группами G_α для $\alpha \in R_0$. Ясно, что H определена над полем $E = L^{\mathscr{G}_5}$. Положим $S = T \cap H$. Тогда из леммы 30 вытекает, что $H^1(L/E, S)$ является одновременно 2-группой и 5-группой, и поэтому тривиальна. С другой стороны, фактор $T_1 = T/S$ либо одномерен, либо двумерен. Так как группы $GL_1(\mathbb{Z})$ и $GL_2(\mathbb{Z})$ не имеют подгрупп порядка 5, то T_1 является E-разложимым. Поэтому $H^1(L/E, T_1) = 1$, и из точной последовательности $H^1(L/E, S) \to H^1(L/E, T) \to H^1(L/E, T_1)$ заключаем, что $H^1(L/E, T) = 1$, что и требовалось.

Система корней типа E_8 содержит подсистему типа D_7, причем $[W(E_8)_7] = [W(D_7)_7] = 7$ и аналогичное рассуждение позволяет установить отсутствие 7-элементов в $H^1(K, T)$. Для групп типа E_7 надо рассуждать по другому. Расширенная диаграмма

Дынкина системы типа E_7 имеет вид



(2)

(μ — максимальный корень, см. таблицу VI у Бурбаки [4]), причем корни $-\mu$ и α_i $(i \neq 2)$ порождают замкнутую подсистему R_0 типа A_7. Так как $[W(E_7)_7] = [W(A_7)_7] = 7$, то без ограничения общности можно предполагать R_0 инвариантной относительно $\mathcal{G}_7$. А тогда корневые группы G_α для $\alpha \in R_0$ порождают подгруппу H типа A_7, содержащую T, определенную над полем $E = L^{\mathcal{G}_7}$ и разложимую над полем L. Из описания групп типа A_n (см. § 2.3) теперь легко вытекает, что $H \simeq \boldsymbol{SL}_8$ над E, и следовательно, тор T изоморфен мультинорменному тору, ассоциированному с набором $P_1, \ldots, P_l$ расширений поля K таких, что $\sum_{i=1}^{l} [P_i : E] = 8$. Так как T становится разложимым над L, то единственным не разложимым над E тором такого вида является тор, ассоциированный с расширениями L, E в случае, когда $[L : E] = 7$, и тогда $T \simeq \mathbf{R}_{L/E}(\boldsymbol{G}_m)$. Во всех случаях $H^1(L/E, T) = 1$. Предложение полностью доказано.

Следствие. *Пусть K — совершенное поле и когомологическая размерность $\mathrm{cd}_p(K)$ не превосходит 1 для $p = 2, 3$. Тогда для односвязной K-определенной квазиразложимой группы G_0 типа E_6 или E_7 имеем $H^1(K, G_0) = 1$. Если к тому же $\mathrm{cd}_5(K) \leqslant 1$, то $H^1(K, G_0) = 1$ и для группы G_0 типа E_8.*

Действительно, согласно предложению 19 для любого $\xi \in H^1(K, G_0)$ найдется такой максимальный K-определенный тор $T \subset G_0$, что ξ лежит в образе отображения $H^1(K, T) \to H^1(K, G_0)$. При этом, как мы только что доказали, порядок любого элемента из $H^1(K, T)$ имеет вид $2^\alpha \cdot 3^\beta$ для типов E_6, E_7 и вид $2^\alpha \cdot 3^\beta \cdot 5^\gamma$ для E_8. С другой стороны, из условий на когомологическую размерность вытекает, что $H^1(K, T)$ не содержит нетривиальных элементов такого порядка (лемма 20). Таким образом, $H^1(K, T) = 1$ и, следовательно, $H^1(K, G_0) = 1$.

Применим утверждение следствия к полю K_Π, где $\Pi = \{2, 3\}$ для типов E_6, E_7 и $\Pi = \{2, 3, 5\}$ для E_8. (Напомним (см. формулировку предложения 20), что поле K_Π, где Π — некоторое множество простых чисел, получается присоединением к K корней ζ_n степени n из единицы для всех n, в разложение которых входят лишь простые числа из Π.) Тогда согласно предложению 20 $\mathrm{cd}_p(K_\Pi) \leqslant 1$ для $p \in \Pi$, и поэтому любой коцикл $\xi \in H^1(K, G_0)$ становится тривиальным над K_Π. В частности, су-

ществует конечное абелево расширение L/K степени $2^\alpha 3^\beta$ для типов E_6, E_7 и степени $2^\alpha 3^\beta 5^\gamma$ для типа E_8 такое, что ξ становится тривиальным в $H^1(L, G_0)$, т. е. лежит в $H^1(L/K, G_0)$. Расширение L/K раскладывается в башню $L = L_m \supset L_{m-1} \supset \ldots \ldots \supset L_1 \supset L_0 = K$, где каждый этаж L_{i+1}/L_i имеет степень p, $p \in \Pi$. Поэтому тривиальность $H^1(K, G_0)$ над локальным или вполне мнимым числовым полем K получается повторным применением следующего утверждения.

Теорема 29. *Пусть G_0 — простая односвязная квазиразложимая группа, относящаяся к одному из типов E_6, E_7, E_8, над полем K, которое является либо локальным либо вполне мнимым числовым. Если L/K — циклическое расширение степени p, где $p = 2, 3$ для типов E_6, E_7, и $p = 2, 3, 5$ для типа E_8, то $H^1(L/K, G_0) = 1$.*

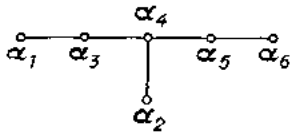
Мы разберем сейчас случаи $p = 2, 3$ и тем самым полностью докажем тривиальность $H^1(K, G_0)$ для групп типов E_6, E_7. Случай $p = 5$ для групп типа E_8 требует специального рассмотрения, что будет проделано позднее. Рассуждение будем вести индукцией по рангу группы. В основе индукции лежит следующее

Предложение 22. *Пусть в условиях теоремы 29 $\xi \in H^1(K, G_0)$ и $G = {}_\xi G_0$. Предположим, что группа G является K-изотропной и $H^1(K, H) = 1$ для любой полупростой односвязной квазиразложимой K-подгруппы $H \subset G_0$ меньшего ранга. Тогда $\xi = 1$.*

Доказательство. Предположим вначале, что G является внутренней формой, т. е. тип G_0 отличен от ${}^2E_6$. Пусть S — максимальный K-разложимый тор в G, $T \subset G$ — максимальный K-определенный тор, содержащий S. Тогда согласно предложению 19 существует такое K-определенное вложение $T \to G_0$, что ξ лежит в образе отображения $H^1(K, T) \to H^1(K, G_0)$. Последнее отображение раскладывается в композицию $H^1(K, T) \to H^1(K, C_0) \to H^1(K, G_0)$, где $C_0 = Z_{G_0}(S)$, поэтому достаточно показать, что $H^1(K, C_0) = 1$. Для этого заметим, что конструируемое в предложении 19 K-вложение $T \to G_0$ индуцируется $\bar{K}$-определенным изоморфизмом $G \to G_0$, в частности, группы C_0 и $C = Z_G(S)$ изоморфны над $\bar{K}$. Но поскольку G является внутренней формой, то связная компонента центра C совпадает с S, так что связная компонента центра C_0 также совпадает с S. Поэтому $C_0 = HS$ — почти прямое произведение, где $H = [C, C]$ — полупростая часть C_0, являющаяся полупростой односвязной квазиразложимой K-группой. По условию $H^1(K, H) = 1$. С другой стороны, фактор C_0/H является разложимым тором, и поэтому $H^1(K, C_0/H) = 1$. Таким образом, из точной последовательности $H^1(K, H) \to H^1(K, C_0) \to H^1(K, C_0/H)$ получаем $H^1(K, C_0) = 1$, что и требовалось.

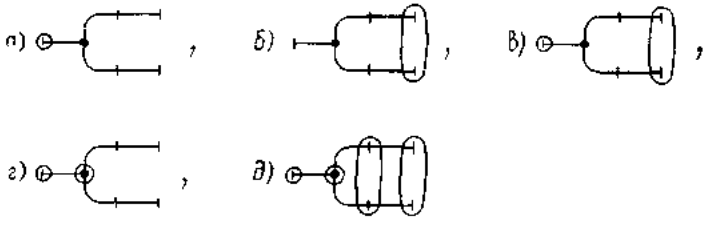
В случае групп типа ${}^2E_6$ предыдущее рассуждение требует некоторой модификации. Анализируя его, мы видим, что нам

в действительности достаточно найти такой K-разложимый тор $S \subset G$, что связный центр группы $C = Z_G(S)$ совпадает с S. Пусть $S_0 \subset G$ — максимальный K-разложимый тор и $T \subset G$ — максимальный K-тор, его содержащий. Занумеруем простые корни системы $R = R(T, G)$ следующим образом:



(3)

и выпишем все возможности для индекса группы G (см. Титс [2]):



(4)

В случае б) анизотропное ядро имеет тип D_4. Но для групп этого типа теоремы 4, 6, а следовательно, и теоремы 5, 25 уже доказаны, поэтому такая группа не может быть K-анизотропной, т. е. случай б) в нашей ситуации не реализуется. В остальных случаях положим $S = \left(\bigcap_{i \neq 2} \operatorname{Ker} \alpha_i\right)^0$. Поскольку всюду вершина α_2 является отмеченной, то S является одномерным K-разложимым тором, причем полупростая часть H его централизатора C является простой группой типа A_5, так что из подсчета рангов получаем, что $C = HS$, и, значит, связная компонента центра C совпадает с S. Предложение доказано.

Чтобы применить в нашей ситуации предложение 22, нам понадобятся две леммы.

Лемма 31. *Пусть G — простая односвязная группа одного из типов E_6, E_7, E_8, определенная над полем K и разложимая над его квадратичным расширением L. Тогда G является K-изотропной.*

Доказательство. Используя лемму 23, выберем максимальный K-определенный тор $T \subset G$, разложимый над полем L. Если предположить, что G является K-анизотропной, то нетождественный автоморфизм $\sigma \in \mathrm{Gal}(L/K)$ действует на $\mathbf{X}(T)$ умножением на (-1). Отсюда следует, что любая корневая подгруппа G_α, порожденная одномерными унипотентными подгруппами U_α и $U_{-\alpha}$, определена над K. Пусть F — подгруппа, порожденная двумя корневыми подгруппами G_α и G_β для двух

соседних корней α, β в диаграмме Дынкина. Тогда F — простая односвязная K-группа типа A_2, разложимая над L. Из описания групп типа A_n вытекает, что $F = \boldsymbol{SU}_3(f)$, где f — невырожденная трехмерная эрмитова форма, связанная с расширением L/K. Но поскольку поле K предполагается локальным либо вполне мнимым, то группа F изотропна над K (см. доказательство теоремы 26), и тем более K-изотропна группа G.

Лемма 32. *Пусть G — простая односвязная группа одного из типов E_6, E_7, E_8, определенная над полем K и разложимая над его циклическим расширением L степени 3. Тогда G либо K-изотропна, либо обладает собственной полупростой K-подгруппой, тип которой отличен от $A_{l_1} \times A_{l_2} \times \ldots \times A_{l_t}$.*

Доказательство. Пусть $T \subset G$ — максимальный L-разложимый тор, $R = R(T, G)$ — соответствующая система корней, $\Pi \subset R$ — подсистема простых корней. Отметим в каждой из соответствующих диаграмм Дынкина по одному корню, как указано ниже:

Обозначим через P стандартную L-определенную параболическую подгруппу P_Δ, где $\Delta = \Pi \setminus \{\alpha\}$, и положим $C = P \cap \sigma(P) \cap \sigma^2(P)$. Ясно, что $\dim C \geqslant \dim G - 3 \operatorname{codim}_G P$, поэтому прямой подсчет с использованием данных таблиц систем корней в книге Бурбаки [4] приводит нас к следующей таблице:

Тип R	$\dim G$	$\dim P$	$\dim C$
E_6	78	62	$\geqslant 30$
E_7	133	106	$\geqslant 52$
E_8	248	191	$\geqslant 77$

Предположим теперь, что группа G анизотропна над K. Тогда группа C, будучи K-определенной, является редуктивной, т. е. $C = HS$, где $H = [C, C]$ — полупростая часть C, S — ее центральный тор. Пусть $H_1, \ldots, H_t$ — абсолютно простые компоненты группы H. Нам надо показать, что не все H_i принадлежат типу A_n. Предположив противное, покажем, что для $\dim C$ не выполняются оценки, указанные в таблице. Положим $l_i = \operatorname{rang} H_i$, $s = \dim S$, $r = \operatorname{rang} G$. Тогда, очевидно,

$$\dim C = \sum_{i=1}^{t} ((l_i + 1)^2 - 1) + s, \tag{5}$$

причем

$$\sum_{i=1}^{t} l_i \leqslant \min(r-s,\ r-1) = f. \tag{6}$$

Обозначим через d количество тех групп H_i, для которых $l_i=1$. Тогда, используя (5), (6), легко получить следующую оценку:

$$\dim C \leqslant s + 3d + (f-d)^2 + 2(f-d) - 4(f-d)(t-d-1). \tag{7}$$

Для случая E_6 $f \leqslant 5$, так что из (7), в частности, должно получаться, что $s+3d+(5-d)^2+2(5-d)=s+d^2-9d+35\geqslant 30$. Для целых d, $0<d\leqslant 5$, имеем $d^2-9d\geqslant -8$, откуда $s\geqslant 3$. Но тогда $f\leqslant 3$ и $s+3d+(f-d)^2+2(f-d)<30$. Итак, $d=0$, и (7) принимает вид $35+s-4t(t-1)\geqslant 30$. Если $t>1$, то $s\geqslant 3$ и (7) уточняется до оценки $s+15-4t(t-1)\geqslant 30$, что невозможно. Таким образом, $t=1$, и единственный случай, удовлетворяющий (5), доставляет в качестве H простую группу типа A_5. Но H должна изоморфно вкладываться в полупростую часть P, которая является группой типа D_5. Однако группа типа D_5 не может содержать группу типа A_5, скажем, потому, что порядок группы Вейля $[W(A_5)]=2^4\cdot 3^2\cdot 5$ не делит $[W(D_5)]=2^7\cdot 3\cdot 5$.

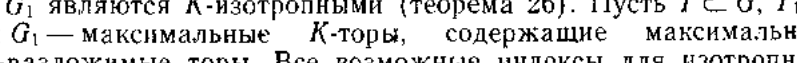
Для случая E_7 $f\leqslant 6$, и тогда $s+3d+(6-d)^2+2(6-d)=$ $=s+d^2-11d+48\geqslant 52$ возможно лишь в случае $d=0$, $s\geqslant 4$. Но тогда $f\leqslant 2$ и $s+3d+(2-d)^2+2(2-d)\leqslant 15$ — противоречие. Наконец, для E_8 $f\leqslant 7$, и тогда $s+3d+(7-d)^2+2(7-$ $-d)=s+d^2-13d+63\geqslant 77$ — не имеет целочисленных решений в области $0\leqslant s,\ d\leqslant 8$. Лемма доказана.

Завершим рассмотрение случаев $p=2, 3$ в теореме 29. Пусть $\xi\in H^1(L/K, G_0)$, где $[L:K]=p$ и $G={}_\xi G_0$. Рассмотрим случай, когда G_0 имеет тип ${}^1E_6$. Если $p=2$, то в силу леммы 31 группа G K-изотропна. Если же $p=3$ и группа G K-анизотропна, то согласно лемме 32 G должна содержать K-определенную полупростую подгруппу H, тип которой отличен от $A_{l_1}\times\ldots$ $\ldots\times A_{l_t}$. Но для односвязных групп меньшего ранга теоремы 4 и 6, а следовательно, и теоремы 5, 25 уже доказаны, и поэтому H является K-изотропной. Таким образом, и для $p=3$ группа G K-изотропна, поэтому из предложения 22 и справедливости теорем 4 и 6 для групп меньшего ранга вытекает, что $\xi=1$, т. е. $H^1(L/K, G_0)=1$. Но как мы видели, отсюда следует, что $H^1(K, G_0)=1$. Пусть теперь G_0 имеет тип ${}^2E_6$, и E/K — квадратичное расширение, над которым G_0 становится внутренней формой. Тогда согласно уже доказанному $H^1(E, G_0)=1$, откуда следует, что над E группа $G={}_\xi G_0$, $\xi\in H^1(K, G_0)$, становится разложимой. Поэтому в силу леммы 31 группа G K-изотропна, и в силу предложения 22 $\xi=1$, т. е. $H^1(K, G_0)=1$.

Перейдем к рассмотрению типа E_7. Так как для всех квазиразложимых односвязных групп H меньшего ранга уже доказана тривиальность $H^1(K, H)$, то в силу теоремы 26 любая полупростая K-группа меньшего ранга, тип которой отличен от $A_{l_1} \times \ldots \times A_{l_t}$, является K-изотропной. Поэтому из лемм 31, 32 вытекает, что $G = {}_\xi G_0$, $\xi \in H^1(L/K, G_0)$ является K-изотропной, и в силу предложения 22 $\xi = 1$. Окончательно, $H^1(L/K, G_0) = 1$, и тогда $H^1(K, G_0) = 1$. Для групп типа E_8 рассуждение аналогично.

Перейдем теперь непосредственно к доказательству теорем 4 и 6 для групп серии E.

Группы типа ${}^1E_6$. Покажем сначала, что $H^1(K, G) = 1$ для любой односвязной K-группы типа ${}^1E_6$, если поле K является локальным либо вполне мнимым. Пусть $\xi \in H^1(K, G)$ и $G_1 = {}_\xi G$. Так как тривиальность $H^1(K, G_0)$ уже доказана, то группы G и G_1 являются K-изотропными (теорема 26). Пусть $T \subset G$, $T_1 \subset G_1$ — максимальные K-торы, содержащие максимальные K-разложимые торы. Все возможные индексы для изотропных групп типа ${}^1E_6$ имеют следующий вид (см. Титс [2]):



(8)

В случае а) анизотропное ядро должно иметь тип D_4, что невозможно, ибо все группы этого типа изотропны над K. В оставшихся диаграммах вершина α_2 является отмеченной (мы придерживаемся нумерации, указанной в (3)). Положим

$$S = \Big(\bigcap_{i \neq 2} \operatorname{Ker} \alpha_i\Big)^0, \quad S_1 = \Big(\bigcap_{i \neq 2} \operatorname{Ker} \alpha_i^1\Big)^0,$$

где $\Pi = \{\alpha_1, \ldots, \alpha_6\}$ и $\Pi_2 = \{\alpha_1^1, \ldots, \alpha_6^1\}$ — подсистемы простых корней в системах $R = R(T, G)$ и $R_1 = R(T_1, G_1)$ соответственно. Тогда существует $\bar{K}$-определенный изоморфизм φ: $G \to G_1$, переводящий S в S_1. Рассмотрим коцикл $\theta = \{a_\sigma = \varphi^{-1}\sigma(\varphi)\} \in Z^1(K, \bar{G})$, где $\bar{G}$ — соответствующая присоединенная группа, которую мы, как обычно, отождествляем с группой внутренних автоморфизмов. Ясно, что θ эквивалентен образу ξ в $Z^1(K, \bar{G})$, так что заменяя коцикл ξ на эквивалентный, можно считать, что θ в точности совпадает с образом ξ. Поскольку торы S и S_1 являются K-разложимыми, то ограничение φ_S: $S \to S_1$ определено над K, и поэтому a_σ действует на S тривиально. Отсюда следует, что $\xi \in H^1(K, C)$, где $C = Z_G(S)$. Но $C = HS$, где H — простая односвязная группа типа A_5. Поэтому $H^1(K, H) = 1$, и из точной последовательности

$$H^1(K, H) \to H^1(K, C) \to H^1(K, \bar{S}) = 1,$$

где $S = C/H = S/S \cap H$ — разложимый тор, получаем, что $H^1(K, C) = 1$, и тем более ξ тривиален в $H^1(K, G)$.

Осталось показать, что для групп типа ${}^1E_6$ над числовым полем K выполняется принцип Хассе. Для этого нам понадобятся две леммы, обобщающие соответственно леммы 17 и 28. Перед их формулировкой напомним, что класс сопряженности $\mathscr{P}$ параболических подгрупп группы G называется *противоположным самому себе*, если для $P \in \mathscr{P}$ противоположная параболическая подгруппа P^- также лежит в $\mathscr{P}$ (см. Борель, Титс [1], § 4). (Отметим также, что $P^- \cap P$ является редуктивной частью P.) Например, борелевские подгруппы образуют класс, который противоположен самому себе.

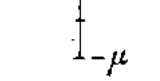
Лемма 17′. *Пусть G — полупростая алгебраическая группа, определенная над произвольным бесконечным совершенным полем K и обладающая над его квадратичным расширением L такой параболической подгруппой P_0, что соответствующий класс сопряженности $\mathscr{P}$ противоположен самому себе. Тогда существует такая L-определенная параболическая подгруппа $P \subset G$, $P \in \mathscr{P}$, что пересечение $C = P \cap \sigma(P)$ совпадает с редуктивной частью P, где σ — образующая $\mathrm{Gal}(L/K)$.*

Лемма 28′. *Сохраним обозначения леммы 17′ и предположим дополнительно, что поле K числовое. Тогда если $\xi \in Z^1(L/K, G)$ — коцикл, представляющий элемент из $\mathrm{Ker}\left(H^1(K, G) \to \prod_{v \in V_\infty^K} H^1(K_v, G)\right)$, то существует коцикл $\xi' \in Z^1(L/K, C)$, эквивалентный исходному в $Z^1(L/K, G)$ и представляющий элемент из $\mathrm{Ker}\left(H^1(K, C) \to \prod_{v \in V_\infty^K} H^1(K_v, C)\right)$.*

Леммы 17′ и 28′ доказываются точно так же, как леммы 17 и 28. Мы предоставляем читателю в качестве упражнения провести соответствующие рассуждения. Отметим только, что при доказательстве леммы 28′ вместо обычного разложение Брюа используется обобщенное (см. Борель, Титс [1], § 5).

Пусть теперь $\xi \in \mathrm{Ker}\left(H^1(K, G) \to \prod_{v \in V_\infty^K} H^1(K_v, G)\right)$. Положим $L = K(\sqrt{-1})$. Тогда уже доказано, что $H^1(L, G) = 1$, и поэтому можно считать, что $\xi \in Z^1(L/K, G)$. Группа G над L является изотропной, причем ее индекс имеет вид (8), случаи б) или в). Обозначим через P_0 стандартную параболическую подгруппу P_Δ, где $\Delta = \Pi \setminus \{\alpha_2, \alpha_4\}$ в нумерации (3). Поскольку множество $\{\alpha_2, \alpha_4\}$ инвариантно относительно симметрий диаграммы Дынкина, то класс сопряженности P_0 является противоположным самому себе (см. Борель, Титс [1], 4.9). Полупростая часть P_0 является полупростой односвязной группой типа $A_2 \times A_2$, при-

чем простые компоненты отвечают системам $\{\alpha_1, \alpha_3\}$ и $\{\alpha_5, \alpha_6\}$. Пользуясь леммой 17′, найдем L-определенную параболическую подгруппу $P \subset G$, сопряженную P_0 и такую, что $C = P \cap \sigma(P)$ — редуктивная часть P. Согласно лемме 28′ можно заменить коцикл ξ на эквивалентный в $Z^1(L/K, G)$ таким образом, чтобы $\xi \in \operatorname{Ker}\left(H^1(K, C) \to \prod_{v \in V_\infty^K} H^1(K_v, C)\right)$. Для доказательства тривиальности ξ построим вспомогательную полупростую K-определенную подгруппу в G, содержащую C. А именно, обозначим через $H = [C, C]$ полупростую часть C. Тогда из рассмотрения расширенной диаграммы Дынкина



системы типа E_6, где μ — максимальный корень (см. таблицу V в книге Бурбаки [4]), вытекает, что централизатор $B = Z_G(H)$ является простой односвязной группой типа A_2, отвечающей системе $\{\alpha_2, \mu\}$. Положим $D = HB$. Ясно, что $C \subset D$, поэтому доказательство завершает

Лемма 33. *Если* $\xi \in H^1(L/K, D)$ *и* $\xi \in \operatorname{Ker}\left(H^1(K, D) \to \prod_{v \in V_\infty^K} H^1(K_v, D)\right)$, *то* $\xi = 1$ *в* $H^1(L/K, D)$.

Доказательство. Положим $F = H \cap B$ и рассмотрим коммутативную диаграмму

$$\begin{tikzcd}
H^1(K, F) \arrow[r, "\alpha_1"] \arrow[d, "\gamma_1"] & H^1(K, H \times B) \arrow[r, "\alpha_2"] \arrow[d, "\gamma_2"] & H^1(K, D) \arrow[r, "\alpha_3"] \arrow[d, "\gamma_3"] & H^2(K, F) \arrow[d, "\gamma_4"] \\
\prod_{v \in V_\infty^K} H^1(K_v, F) \arrow[r, "\beta_1"] & \prod_{v \in V_\infty^K} H^1(K_v, H \times B) \arrow[r, "\beta_2"] & \prod_{v \in V_\infty^K} H^1(K_v, D) \arrow[r, "\beta_3"] & \prod_{v \in V_\infty^K} H^2(K_v, F)
\end{tikzcd}$$

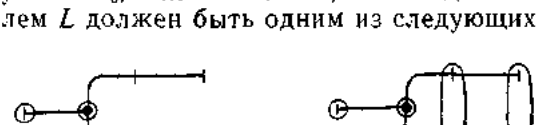
отвечающую универсальному накрытию $1 \to F \to H \times B \to D \to 1$. Ясно, что $\alpha_3(\xi)$ лежит в ядре отображения $H^2(K, F) \xrightarrow{\mathrm{Res}} H^2(L, F)$. Используя отображение Cor: $H^2(L, F) \to H^2(K, F)$ и тот факт, что $\mathrm{Cor} \circ \mathrm{Res}$ совпадает с умножением на $[L : K] = 2$, получаем $\alpha_3(\xi) = 1$, ибо $[F]$ делит $[Z(B)] = 3$. Тогда $\xi = \alpha_2(\zeta)$, $\zeta \in H^1(K,$

$H \times B$). Имеем $\beta_2(\gamma_2(\zeta)) = \gamma_3(\alpha_2(\zeta)) = 1$, так что $\gamma_2(\zeta) = \operatorname{Im}\beta_1$. Но опять, используя тот факт, что $[F] \mid 3$, а $[\operatorname{Gal}(\overline{K}_v/K_v)] \leqslant 2$ для $v \in V_\infty^K$, получаем, что здесь $H^1(K_v, F) = 1$, т. е. $\operatorname{Im}\beta_1 = (1)$. Поэтому $\zeta \in \operatorname{Ker}\gamma_2$, и, следовательно, $\zeta = 1$, ибо для групп типа A_2 принцип Хассе уже доказан. Окончательно, $\xi = \alpha_2(\zeta) = 1$, и лемма доказана.

Группы типа $^2E_6$. Если K — локальное поле, то в силу предложения 15 любая K-группа G типа $^2E_6$ является квазиразложимой, т. е. $G \simeq G_0$, ибо тривиальность $H^1(K, G_0)$ уже доказана. Но тогда $H^1(K, G) = H^1(K, G_0) = 1$.

Доказательство тривиальности $H^1(K, G)$ для чисто мнимого поля K аналогично соответствующему рассуждению для $^1E_6$. Действительно, из тривиальности $H^1(K, G_0)$ вытекает, что группа G является K-изотропной (теорема 26). Тогда ее индекс является одним из указанных в (4), причем, как мы отметили при доказательстве предложения 22, случай б) над вполне мнимым полем не реализуется. В остальных случаях вершина α_2 является отмеченной. Дальнейшее рассуждение проводится, как и в случае типа $^1E_6$.

Доказательство принципа Хассе также можно провести аналогично случаю $^1E_6$, если известно, что индекс G над вполне мнимым полем L должен быть одним из следующих:



т. е. вершины α_2, α_4 должны быть отмеченными. Покажем это. Обозначим через S_0 двумерный L-разложимый тор $\left(\bigcap_{i \neq 2,4} \operatorname{Ker}\alpha_i\right)^0$ в G_0, и пусть C — его централизатор в G_0, $H = [C, C]$ — полупростая часть C. Положим $\bar{H} = \pi(H)$, где π: $G_0 \to \bar{G}_0$ — изогения на присоединенную группу. Так как G получается из G_0 скручиванием при помощи коцикла $\theta \in H^1(L, \bar{G}_0)$, то нам достаточно показать, что отображение $H^1(L, \bar{H}) \to H^1(L, \bar{G}_0)$ сюръективно. Легко показать, что центр Z группы G_0 содержится в H. Имеем коммутативную диаграмму с точными строками

$$\begin{array}{ccccc} H^1(L, H) & \xrightarrow{\alpha_1} & H^1(L, \bar{H}) & \xrightarrow{\alpha_2} & H^2(L, Z) \\ \downarrow{\scriptstyle\gamma_1} & & \downarrow{\scriptstyle\gamma_2} & & \downarrow{\scriptstyle\gamma_3} \\ H^1(L, G_0) & \xrightarrow{\beta_1} & H^1(L, \bar{G}_0) & \xrightarrow{\beta_2} & H^2(L, Z) \end{array}$$

Согласно теореме 20 α_2 сюръективно. Отсюда следует, что для данного $\theta \in H^1(L, \bar{G}_0)$ найдется $\zeta \in H^1(L, \bar{H})$ такой, что $\beta_2(\theta) = \beta_2(\gamma_2(\zeta))$. Но поскольку тривиальность когомологий односвяз-

ных групп типа ${}^2E_6$ над вполне мнимым полем уже доказана, то из соображений скручивания β_2 инъективно. Поэтому $\theta = \gamma_2(\xi)$, что и требовалось.

Группы типа E_7. Так как $H^1(K, G_0) = 1$, то в силу предложения 16 для любой K-группы G типа E_7 найдется такое квадратичное расширение L/K, являющееся вполне мнимым в числовой ситуации, над которым G становится разложимой. Применяя лемму 17, найдем L-определенную подгруппу Бореля $B \subset G$ такую, что $T = B \cap \sigma(B)$ — максимальный K-тор в G, разложимый над L (σ — образующая группы $\mathrm{Gal}(L/K)$). Покажем, что тор T является K-анизотропным, т. е. σ действует на $\mathbf{X}(T)$ умножением на -1. Действительно, поскольку $B \cap \sigma(B) = T$, то σ переводит положительные корни системы $R(T, G)$, ассоциированные с B, в отрицательные. Но поскольку диаграмма Дынкина не имеет нетривиальных симметрий, то единственным автоморфизмом с таким свойством является -1. Отсюда следует, что любая корневая подгруппа G_α определена над K, и, следовательно, определена над K построенная при доказательстве предложения 21 односвязная подгруппа $H \subset G$ типа A_7, содержащая тор T.

Пусть теперь $\xi \in H^1(K, G)$, где поле K локальное. Так как $G \simeq G_0$ над L, то $H^1(L, G) = H^1(L, G_0) = 1$, и поэтому $\xi \in H^1(L/K, G)$. В силу леммы 28 существует эквивалентный ξ коцикл $\xi' \in H^1(L/K, T)$. Но так как для H теорема 4 уже доказана, то сквозное отображение $H^1(K, T) \to H^1(K, H) \to H^1(K, G)$ тривиально и $\xi = 1$.

В числовой ситуации рассмотрим $\xi \in \mathrm{Ker}\,(H^1(K, G) \to \prod_{v \in V_\infty^K} H^1(K_v, G))$. Как и выше, устанавливается, что $\xi \in H^1(L/K, G)$, так что в силу леммы 28, заменяя коцикл ξ на эквивалентный, можно считать, что $\xi \in \mathrm{Ker}\,(H^1(K, T) \to \prod_{v \in V_\infty^K} H^1(K_v, T))$. Тогда, используя теорему 6 для группы H, получим, что $\xi = 1$.

Группы типа E_8. Для групп этого типа нам, фактически, осталось рассмотреть лишь случай $p = 5$ в теореме 29, ибо тогда $H^1(K, G) = 1$ над локальным или вполне мнимым числовым полем K. Отсюда следует, что любая группа G типа E_8 над таким K разложима, поэтому можно утверждать, что здесь $H^1(K, G) = 1$ для всех групп G. Последующий вывод принципа Хассе ничем не отличается от случая E_7.

Итак, пусть L — циклическое расширение Галуа степени 5 локального либо вполне мнимого числового поля K, G_0 — простая разложимая K-группа типа E_8. Наша цель — показать, что $H^1(L/K, G_0) = 1$. Обозначим через E композит всех конечных разрешимых расширений Галуа поля K степени вида $2^\alpha 3^\beta$

(максимальное разрешимое $\{2, 3\}$-расширение поля K; отметим, что в действительности любая группа порядка $2^\alpha 3^\beta$ разрешима (теорема Бернсайда), так что слово «разрешимое» здесь может быть опущено). Нам достаточно показать, что $H^1(LE/E, G_0) = 1$, ибо тогда любой коцикл $\xi \in H^1(L/K, G_0)$ лежит в $H^1(E/K, G_0)$ и, значит, в $H^1(P/K, G_0)$ для некоторого конечного разрешимого расширения P/K степени $2^\alpha \cdot 3^\beta$. Существует башня $P = P_0 \supset P_1 \ldots \supset P_{n-1} \supset P_n = K$, каждый этаж P_i/P_{i+1} которой является циклическим расширением степени 2 или 3. Так как случаи $p = 2, 3$ в теореме 29 уже рассмотрены, то, применяя ее последовательно к каждому этажу, получим, что $H^1(P/K, G_0) = 1$, и, значит, $\xi = 1$. Таким образом, мы будем доказывать тривиальность множества $H^1(L/E, G_0)$, где L/E — циклическое расширение поля E степени 5. При этом будет использоваться следующее свойство поля E (ради которого мы и осуществили переход от K к E): поле E не имеет расширений степеней 2, 3, 4, в частности, если $a \in E$, то $\sqrt{a}$, $\sqrt[3]{a} \in E$. Ключевую роль в доказательстве играет следующая

Теорема 30 (Черноусов [6]). *Пусть G — анизотропная группа типа E_8, определенная над полем E и разложимая над его циклическим расширением L степени 5. Тогда G обладает собственной полупростой E-определенной подгруппой $H \subset G$, изотропной над L.*

Доказательство. Пусть σ — образующая группы $\mathrm{Gal}(L/E)$. Мы установим существование такой одномерной унипотентной подгруппы $U = U_\alpha$, отвечающей некоторому корню $\alpha \in R(T, G)$ относительно подходящего максимального L-разложимого тора $T \subset G$, что подгруппа $H_0 \subset G$, порожденная группами $\sigma^i(U)$, $i = 0, 1, 2, 3, 4$, является собственной. Тогда H_0, очевидно, определена над E и, в частности, является редуктивной, ибо G E-анизотропна. По построению группа H_0 над L содержит унипотентные элементы, поэтому H_0 не сводится к тору, и ее коммутант $H = [H_0, H_0]$ является искомой группой. Чтобы удостовериться в том, что $H_0 \neq G$, мы покажем, что ее алгебра Ли $\mathfrak{h}_0 = L(H_0)$ отлична от $\mathfrak{g} = L(G)$. Для этого заметим, что поскольку $\mathrm{char}\, K = 0$, алгебра $\mathfrak{h}_0$ порождается как алгебра Ли элементами $\sigma^i(X)$, $i = 0, 1, 2, 3, 4$, где $X \in L(U)_L$ — произвольный ненулевой элемент (см. Борель [8], § 7). Поэтому наша задача сводится к нахождению элемента $X \in \mathfrak{g}_L$, порождающего алгебру Ли некоторой корневой унипотентной подгруппы U и такого, что подалгебра в $\mathfrak{g}$, порожденная элементами $\sigma^i(X)$, $i = 0, 1, 2, 3, 4$, является собственной. Элементы, удовлетворяющие первому требованию, будем называть *корневыми*. Более точно, элемент $X \in \mathfrak{g}_L$ — корневой, если существует такой максимальный L-разложимый тор $T \subset G$, что X является собственным вектором относительно $\mathrm{Ad}\, T$, т. е. $\mathrm{Ad}(t)(X) = \alpha(t) X$ для подходящего $\alpha \in \mathbf{X}(T)$ и всех $t \in T$, причем $\alpha \neq 1$. Тогда в слу-

чае $X \neq 0$ характер α оказывается корнем G относительно T и одномерное пространство, натянутое на X, имеет вид $L(U_\alpha)$, где U_α — отвечающая α корневая унипотентная подгруппа. Таким образом, нам достаточно найти ненулевой корневой элемент $X \in \mathfrak{g}_L$, все сдвиги $\sigma^i(X)$ которого порождают собственную подалгебру в $\mathfrak{g}$.

Начнем с установления необходимых для дальнейшего свойств корневых элементов. Пусть $X \in L(U_\alpha)_L$, где $\alpha \in R = R(T, G)$. Так как в системе типа E_8 все корни имеют одинаковую длину, то можно без ограничения общности предполагать, что α является максимальным корнем относительно упорядочения, определяемого системой простых корней $\Pi \subset R$. Пусть $\{H_\alpha, \alpha \in \Pi, X_\alpha; \alpha \in R\}$ — базис Шевалле в $\mathfrak{g}_L$ (см. § 2.1, п. 13). Тогда из соотношений $[X_\alpha, X_{-\alpha}] = H_\alpha$, $[X_\alpha, X_\beta] = 0$ или $\pm X_{\alpha+\beta}$ и максимальности α вытекает, что для любого $Y \in \mathfrak{g}_L$ выражение $[X_\alpha, [X_\alpha, Y]]$ пропорционально X_α. Так как X в свою очередь пропорционален X_α, то в итоге $[X, [X, Y]] = \langle X, Y\rangle X$ для любого $Y \in \mathfrak{g}_L$ и подходящего $\langle X, Y\rangle \in L$ (мы полагаем $\langle X, Y\rangle = 0$, если $X = 0$). Это свойство корневых элементов является основным для дальнейших вычислений. Легко видеть, что символ $\langle X, Y\rangle$ линеен по второму аргументу. Предположим теперь, что оба элемента $X, Y \in \mathfrak{g}_L$ являются корневыми. Тогда умножая равенства

$$\begin{aligned} [X, [X, Y]] &= \langle X, Y\rangle X, \\ [Y, [Y, X]] &= \langle Y, X\rangle Y \end{aligned} \tag{9}$$

слева на Y и X соответственно и используя соотношение $[Y, [X, [X, Y]]] = -[X, [Y, [Y, X]]]$, вытекающее из тождества Якоби, легко получить, что $\langle X, Y\rangle = \langle Y, X\rangle$. Таким образом, для корневого Y символ $\langle X, Y\rangle$ линеен по X, если X изменяется в некотором линейном пространстве, состоящем из корневых элементов. Установим еще несколько свойств корневых элементов.

Лемма 34. *Пусть $X, Y, Z \in \mathfrak{g}_L$, причем элемент X — корневой. Тогда*:

1) *справедливы тождества*

$$2[[X, Z], [X, Y]] = \langle X, Y\rangle [X, Z] - \langle X, Z\rangle [X, Y] - \langle X, [Y, Z]\rangle X, \tag{10}$$

$$2[X, [Y, [Z, X]]] = \langle X, Z\rangle [X, Y] + \langle X, Y\rangle [X, Z] + \langle X, [Z, Y]\rangle X; \tag{11}$$

2) *если $[X, Y] = 0$, то $\langle X, [Y, Z]\rangle = 0$.*

Доказательство. Из тождества Якоби вытекает, что

$$\begin{aligned} [[X, Z], [X, Y]] &= [Y, [X, [X, Z]]] - [X, [Y, [X, Z]]] = \\ &= \langle X, Z\rangle [Y, X] + [X, [Y, [Z, X]]]. \end{aligned} \tag{12}$$

Аналогично получается, что

$$[[X, Y], [X, Z]] = \langle X, Y\rangle [Z, X] + [X, [Z, [Y, X]]]. \tag{13}$$

При этом

$$[X, [Y, [Z, X]]] = -\langle X, [Y, Z]\rangle X + [X, [Z, [Y, X]]]. \quad (14)$$

Сравнивая (12)—(14), легко получить (10), (11). Если $[X, Y] = 0$, причем $X \neq 0$, то из (10) непосредственно вытекает утверждение 2). Лемма доказана.

Исходным пунктом для построения искомого корневого элемента $X \in \mathfrak{g}_L$ служит

Предложение 23. *Пусть $X \in \mathfrak{g}_L$ — такой корневой элемент, что $[X, \sigma(X)] = 0$. Тогда подалгебра $\mathfrak{h}_0 \subset \mathfrak{g}$, порожденная всеми его сдвигами $\sigma^i(X)$, $i = 0, \ldots, 4$, имеет размерность, не превосходящую 25, и поэтому является собственной.*

Доказательство. Положим $X_i = \sigma^{2i-2}(X)$. Тогда $\mathfrak{h}_0$ порождается элементами X_i, причем из соотношения $[X, \sigma(X)] = 0$ вытекает, что $[X_i, X_j] = 0$, кроме случая $i \equiv j \pm 1 \pmod 5$. Для краткости положим

$$(i_1, \ldots, i_s) = [X_{i_1}, [X_{i_2}, \ldots, [X_{i_{s-1}}, X_{i_s}] \ldots],$$

где $1 \leqslant i_l \leqslant 5$, $1 \leqslant l \leqslant s$, и будем называть такое выражение *мономом* длины s. Ясно, что $\mathfrak{h}_0$ совпадает с линейным пространством, натянутым на всевозможные мономы. Будем называть моном *приводимым*, если он является линейной комбинацией мономов строго меньшей длины. Кроме того, моном $(i_1, \ldots, i_l)$ называется *стандартным*, если $i_{h+1} \equiv i_h + 1 \pmod 5$, $h = 1, \ldots, l-1$. Число стандартных мономов любой длины равно 5, поэтому число стандартных мономов длины, не превосходящей 5, равно 25. Таким образом, указанная оценка размерности алгебры получается из следующих двух утверждений:

(*) любой моном длины, не превосходящей 5, является линейной комбинацией стандартных мономов;

(**) любой моном длины 6 приводим.

Для доказательства (*) рассмотрим моном $m = (i_1, \ldots, i_l)$ длины $l \leqslant 5$ и предположим, что для мономов меньшей длины (*) уже доказано. Тогда можно считать, что моном $(i_2, \ldots, i_l)$ стандартный, причем без ограничения общности можно полагать, что $i_h = h$, $2 \leqslant h \leqslant l$. Если $i_1 = 1$, то моном m — стандартный. Если $i_1 = 2$, то из основного свойства корневых элементов вытекает, что m пропорционален X_{i_2}, и доказывать нечего. Если $2 < i_1 \leqslant l$, то, используя тот факт, что $[X_i, X_j] = 0$ при $i \not\equiv j \pm 1 \pmod 5$ и тождество Якоби, легко показать, что

$$m = (i_1, 2, \ldots, l) = (2, 3, \ldots, i_1, i_1 - 1, i_1, \ldots, l),$$

а приводимость последнего монома вытекает из (11). Если $i_1 = l + 1$, то $m = (l+1, 2, \ldots, l) = (2, \ldots, l-1, l+1, l) = -(2, \ldots, l-1, l, l+1)$ — стандартный моном. Наконец, если $i_1 > l + 1$, то $m = 0$.

Для доказательства (**) достаточно установить приводимость монома $(i, 1, 2, \ldots, 5)$, что проделывается при помощи аналогичных рассуждений. Предложение доказано.

Построение ненулевого корневого элемента $X \in \mathfrak{g}_L$, для которого $[X, \sigma(X)] = 0$, представляет наиболее технически сложную часть доказательства теоремы 30. Для этого вначале строится корневой элемент $Y \in \mathfrak{g}_L$ со следующими свойствами:

$$\langle Y, \sigma(Y)\rangle = 0, \langle \sigma(Y), [Y, \sigma^2(Y)]\rangle = 0. \tag{15}$$

Если при этом $[Y, \sigma(Y)] = 0$, то элемент $X = Y$ искомый. В противном случае положим $X = [Y, \sigma(Y)]$. Тогда из условий (15) и соотношения (10) вытекает, что

$$[X, \sigma(X)] = [[Y, \sigma(Y)], [\sigma(Y), \sigma^2(Y)]] =$$
$$= -\frac{1}{2}(\langle\sigma(Y), \sigma^2(Y)\rangle[\sigma(Y), Y] - \langle\sigma(Y), Y\rangle[\sigma(Y), \sigma^2(Y)] -$$
$$- \langle\sigma(Y), [\sigma^2(Y), Y]\rangle\sigma(Y)) = 0.$$

Остается доказать, что элемент X корневой.

Лемма 35. *Пусть $X, Y \in \mathfrak{g}_L$ — два корневых элемента. Тогда существует максимальный L-разложимый тор $T \subset G$ такой, что X и Y являются собственными векторами относительно* $\mathrm{Ad}\, T$. *При этом если $\langle X, Y\rangle = 0$, то элемент $[X, Y]$ также корневой.*

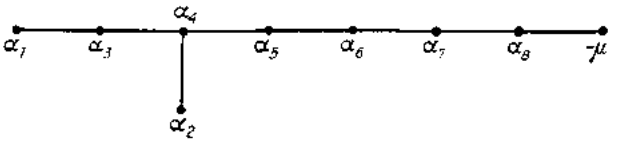
Доказательство. Пусть $T_X \subset G$ — максимальный L-разложимый тор такой, что X является собственным вектором для преобразований из $\mathrm{Ad}\, T_X$. Выше мы видели, что можно без ограничения общности считать X пропорциональным X_α, где $\alpha \in R_X = R(T_X, G)$ — максимальный корень относительно упорядочения на R_X, задаваемого системой простых корней Π_X. Пусть $B_X = T_X U_X$ — отвечающая Π_X подгруппа Бореля. В силу максимальности α унипотентная часть U_X централизует X, и поэтому X является собственным для всех преобразований из $\mathrm{Ad}\, B_X$. Аналогичным образом найдем подгруппу Бореля $B_Y \subset G$ такую, что Y является собственным для $\mathrm{Ad}\, B_Y$. Тогда пересечение $B_X \cap B_Y$ содержит максимальный тор T группы G, который и будет искомым. Пусть $X \in L(U_\alpha)$, $Y \in L(U_\beta)$, где $\alpha, \beta \in R(T, G)$. Если $\beta \neq -\alpha$, то либо $[X, Y] = 0$, либо $\alpha + \beta$ — корень и $[X, Y] \in L(U_{\alpha+\beta})$. Покажем, что случай $\beta = -\alpha$, $\langle X, Y\rangle = 0$ невозможен. Действительно, если $\beta = -\alpha$, то элемент $[X, Y]$ пропорционален H_α с ненулевым коэффициентом пропорциональности. Тогда $[X, [X, Y]] = cX$, где $c = \langle X, Y\rangle \neq 0$ — противоречие. Лемма доказана.

Завершает доказательство теоремы 30

Предложение 24. *Существует ненулевой корневой элемент $Y \in \mathfrak{g}_L$, удовлетворяющий* (15).

Доказательство. Покажем вначале, как найти корневой элемент $Z \in \mathfrak{g}_L$, удовлетворяющий первому условию в (15). Для этого зафиксируем на время максимальный L-разложимый тор

$T \subset G$, систему корней $R = R(T, G)$, подсистему простых корней $\Pi = \{\alpha_1, \ldots, \alpha_8\}$, и пусть $\mu \in R$ — соответствующий максимальный корень. Напомним, что расширенная диаграмма Дынкина здесь имеет вид



Элементы $X_{\pm\alpha}$, $\alpha \in \{\alpha_i \mid i \neq 2\} \cup \{\mu\}$ порождают в $\mathfrak{g}_L$ подалгебру $\mathfrak{b}_L$ типа A_8. Отождествляя $\mathfrak{b}_L$ с алгеброй Ли $\mathfrak{sl}_9(L)$, состоящей из матриц $Z \in M_9(L)$ со следом нуль, мы видим, что $\mathfrak{b}_L$ содержит 8-мерное подпространство V, целиком состоящее из корневых элементов (таковым будет, например, подпространство $V = \{(z_{ij}) \mid z_{ij} = 0$, если $i = j = 1$, либо $i \neq 1\}$; отметим, что поскольку ранги алгебр $\mathfrak{b}$ и $\mathfrak{g}$ совпадают, то элементы из V, являясь, очевидно, корневыми в $\mathfrak{b}_L$, будут корневыми и в $\mathfrak{g}_L$). Покажем, что существует элемент $Z \in V \setminus (0)$ такой, что

$$\langle Z, \sigma(Z) \rangle = 0. \tag{16}$$

Пространство V, являясь 8-мерным над L, имеет размерность 40 над E. При этом условие (10) равносильно системе пяти однородных квадратичных уравнений относительно E-координат элемента Z. Поэтому существование ненулевого Z, удовлетворяющего (16), вытекает из следующего простого утверждения

Упражнение. Пусть $f_1, \ldots, f_l$ — квадратичные формы с коэффициентами из E от n переменных. Если $n > \frac{1}{2} l(l+1)$, то система $f_1(x) = \ldots = f_l(x) = 0$ имеет над E ненулевое решение. (Доказательство проводится индукцией по l и использует возможность извлечения квадратных корней из элементов E.)

Зафиксируем ненулевой корневой элемент $Z \in \mathfrak{g}_L$ со свойством (16). Чтобы построить корневой элемент $Y \in \mathfrak{g}_L$, удовлетворяющий обоим равенствам в (15), необходимо провести перестройку исходного тора T. А именно, переходя с помощью леммы 35 к другому тору, можно предполагать, что Z и $\sigma(Z)$ являются собственными векторами относительно $\operatorname{Ad} T$, т. е. порождают алгебры $L(U_\alpha)$ и $L(U_\beta)$ для некоторых корней $\alpha, \beta \in R(T, G)$. Если $[Z, \sigma(Z)] = 0$, то из тождества Якоби вытекает, что $[\sigma(Z), [Z, \sigma^2(Z)]] = 0$, и элемент $Y = Z$ искомый. Поэтому в дальнейшем предполагаем, что $[Z, \sigma(Z)] \neq 0$. Тогда с учетом (16) получаем, что $\beta \neq -\alpha$, и, следовательно, $\alpha + \beta$ — также корень. Мы уже отмечали, что можно выбрать систему $\Pi \subset R(T, G)$ простых корней таким образом, что α является максимальным корнем относительно соответствующего упорядочения. Покажем, что, варьируя Π, можно также добиться выпол-

нения условия $\beta = -\alpha_8$, где $\Pi = \{\alpha_1, \ldots, \alpha_8\}$, причем нумерация корней совпадает с указанной выше. Для этого рассмотрим совокупность $\{\tilde{\Pi}\}$ всех систем простых корней $\tilde{\Pi} \subset R(T, G)$, относительно которых α является максимальным корнем, и подчиним выбор Π условию: $\mathrm{ht}_\Pi \beta = \max\limits_{\tilde{\Pi}} \mathrm{ht}_{\tilde{\Pi}} \beta$, где $\mathrm{ht}_\Pi \beta = \sum\limits_{i=1}^{8} n_i$ — высота корня $\beta = \sum\limits_{i=1}^{8} n_i \alpha_i$ относительно системы $\Pi = \{\alpha_1, \ldots, \alpha_8\}$. Поскольку $\alpha + \beta$ — корень, и корень α максимальный, то корень β отрицательный. С другой стороны, если $\gamma \in \{\alpha_1, \ldots, \alpha_7\}$, то необходимо $(\gamma | \beta) \geqslant 0$, где $(\mid)$ обозначает скалярное произведение, ибо в противном случае высота β относительно системы $\Pi' = w_\gamma(\Pi) \in \{\tilde{\Pi}\}$ (w_γ — соответствующее отражение) была бы больше $\mathrm{ht}_\Pi \beta$. Из описания системы корней типа E_8 (таблица VII в книге Бурбаки [4]) ясно, что β имеет вид $\beta = \delta - \alpha_8$, где δ является линейной комбинацией корней $\alpha_1, \ldots, \alpha_7$ с целыми неположительными коэффициентами. Тогда $(\beta | \beta) = (\delta | \delta) - 2(\delta | \alpha_8) + (\alpha_8 | \alpha_8)$, откуда $(\delta | \delta) = 2(\delta | \alpha_8)$, ибо $(\beta | \beta) = (\alpha_8 | \alpha_8)$, и поэтому $(\delta | \delta) = (\delta | \beta + \alpha_8) = (\delta | \beta) + (\delta | \alpha_8) \leqslant \frac{1}{2}(\delta | \delta)$, и окончательно $(\delta | \delta) = 0$, т. е. $\delta = 0$, что и требовалось.

Итак, заменяя элемент Z на пропорциональный, можно считать, что $Z = X_\alpha$, где α — максимальный корень, а $\sigma(Z) = cX_{-\alpha_8}$.

Лемма 36. *Существует такое 6-мерное подпространство $W \subset \mathfrak{g}_L$, что пространство $LZ + W$ состоит из корневых элементов и для любого $S \in W$ выполняются следующие соотношения:*

$$\begin{gathered} \langle Z, \sigma(S) \rangle = \langle S, \sigma(S) \rangle = 0, \\ [Z, S] = [Z, \sigma(S)] = 0. \end{gathered} \tag{17}$$

Доказательство. Обозначим через W_1 подпространство в $\mathfrak{g}_L$, натянутое на элементы $X_{\alpha_7}, X_{\alpha_7+\alpha_5}, \ldots, X_{\alpha_7+\ldots+\alpha_3}, X_{\alpha_7+\ldots+\alpha_2+\alpha_1}$; $\dim W_1 = 6$. Отождествляя, как и выше, алгебру типа A_8, порожденную X_γ, $\gamma \in \{\alpha_i \mid i \neq 2\} \cup \{\alpha\}$ с $\mathfrak{sl}_9(L)$, легко показать, что пространство $LX_{-\alpha_8} + W_1$ состоит из корневых элементов. Из соотношений для элементов базиса Шевалле вытекают следующие свойства:

$$W_1 \subset [X_{-\alpha_8}, \mathfrak{g}_L], \ [X_{-\alpha_8}, W_1] = 0, \ [X_\alpha, W_1] = 0. \tag{18}$$

Положим $W = \sigma^{-1}(W_1)$. Тогда пространство $LX_\alpha + W$ состоит из корневых векторов. Из (18) вытекают все соотношения в (17), кроме $\langle S, \sigma(S) \rangle = 0$ для $S \in W$. Но для любого $S_1 \in W_1$, согласно (18), $[X_\alpha, S_1] = 0$. Поэтому, применяя утверждение 2) леммы 34, получим $\langle S_1, [X_\alpha, \mathfrak{g}_L] \rangle = 0$. Но из (18) вытекает, что

$[X_\alpha, \mathfrak{g}_L]$ содержит W, поэтому $\langle W_1, W\rangle = 0$, откуда $\langle W, \sigma(W)\rangle = 0$. Лемма доказана.

Используя указанные свойства пространства W, теперь уже легко завершить построение искомого ненулевого элемента Y, удовлетворяющего (15). Вначале найдем ненулевой $S \in W$ со следующими свойствами:

$$\langle \sigma(Z), S\rangle = \langle \sigma(Z), [S, \sigma^2(Z)]\rangle = 0, \tag{19}$$

$$\langle \sigma(S), [S, \sigma^2(Z)]\rangle = 0. \tag{20}$$

Элементы $S \in W$, удовлетворяющие (19), образуют подпространство размерности, не меньшей 4, над L, т. е. размерности не меньшей 20, над E. При этом (20) эквивалентно системе пяти однородных квадратичных уравнений относительно E-координат S. Поэтому еще раз применяя утверждение упражнения, получаем существование элемента S. Далее, мы можем предполагать, что $z = \langle \sigma(Z), [Z, \sigma^2(Z)]\rangle \neq 0$, $s = \langle \sigma(S), [S, \sigma^2(S)]\rangle \neq 0$. Положим $q = -zs^{-1}$, $r = \sqrt[3]{N_{L/E}(q)} \in E$, $t = rq\sigma^3(q)$ и покажем, что корневой элемент $Y = Z + tS$ — искомый.

Имеем

$$\langle Y, \sigma(Y)\rangle = \langle Z + tS, \sigma(Z) + \sigma(t)\sigma(S)\rangle = 0$$

в силу условий (17) и (19). Чтобы избежать громоздких вычислений при подсчете $y = \langle \sigma(Y), [Y, \sigma^2(Y)]\rangle = \langle \sigma(Z) + \sigma(t)\sigma(S), [Z + tS, \sigma^2(Z) + \sigma^2(t)\sigma^2(S)]\rangle$, заметим, что в силу утверждения 2) леммы 34 и условий (17) все члены, кроме $\langle \sigma(Z), [Z, \sigma^2(Z)]\rangle$, $\langle \sigma(S), [S, \sigma^2(S)]\rangle$, $\langle \sigma(Z), [S, \sigma^2(Z)]\rangle$ и $\langle \sigma(S), [S, \sigma^2(Z)]\rangle$, обращаются в нуль, причем два последние также равны нулю благодаря выполнению условий (19), (20). Отсюда следует, что $y = z - t\sigma(t)\sigma^2(t)s = 0$. Доказательство предложения 24, а вместе с тем и теоремы 30 завершено.

Переходим теперь непосредственно к доказательству тривиальности $H^1(L/E, G_0)$. Пусть $\xi \in H^1(L/E, G_0)$, $G = {}_\xi G_0$. Если группа G изотропна над E, то применяя предложение 22 с учетом того, что для всех групп, отличных от E_8, теоремы 4 и 6 уже доказаны, получаем, что $\xi = 1$. Поэтому всюду ниже будем предполагать, что группа G E-анизотропна. Тогда согласно теореме 30 существует собственная E-определенная и L-изотропная полупростая подгруппа $H \subset G$. Без ограничения общности можно считать группу H E-простой. Тогда H изогенна группе вида $\mathbf{R}_{P/E}(F)$. Так как для всех групп, кроме E_8, теорема 29 уже доказана, то F в силу E-анизотропности G имеет тип A_n. Так как E по построению не имеет расширений степени $\leqslant 4$, то априори возможны лишь случаи 1) $[P:E] \geqslant 5$, $n = 1$; 2) $P = E$. Используя тот факт, что H является E-анизотропной и L-изотропной, легко показать, что в действительности возможен лишь случай $P = E$, $n = 4$, т. е. H — простая группа типа A_4. Поскольку E не имеет квадратичных расширений, то H авто-

матически является внутренней формой, другими словами, $H = \boldsymbol{SL}_1(D)$, где D — тело индекса 5 над E. При этом $D \otimes_E L \simeq M_5(L)$, так что L вкладывается в D в качестве максимального подполя. Пусть $T_1 = \mathbf{R}^{(1)}_{L/E}(\boldsymbol{G}_m)$ — соответствующий E-определенный норменный тор в G. Группа G является L-разложимой, и поэтому централизатор $C_1 = Z_G(T_1)$ также является E-определенной L-разложимой группой. Если полупростая часть $H_1 = [C_1, C_1]$ нетривиальна, то применяя к ней те же рассуждения, что и к группе H, установим существование тора $T_2 \subset H_1$ вида $T_2 = \mathbf{R}^{(1)}_{L/E}(\boldsymbol{G}_m)$. Тогда тор $T = T_1T_2$ является E-определенным L-разложимым тором в G. Если же $H_1 = 1$, то таким тором будет группа $T = C_1$.

Согласно предложению 19 существует E-определенное вложение $T \to G_0$ такое, что ξ лежит в образе отображения φ: $H^1(E, T) \to H^1(E, G_0)$, поэтому завершает доказательство тривиальности $H^1(L/E, G_0)$

Предложение 25. *Отображение φ тривиально.*

Доказательство. Для каждого корня $\alpha \in R = R(T, G)$ обозначим через $G(\alpha)$ подгруппу в G, порожденную корневыми подгруппами $G_{\sigma^i(\alpha)}$, $i = 0, 1, 2, 3, 4$. Утверждается, что $G(\alpha)$ является простой односвязной E-группой типа A_4. Легко видеть, что система корней $R(T(\alpha), G(\alpha))$, где $T(\alpha) = T \cap G(\alpha)$ — максимальный тор в $G(\alpha)$, совпадает с подсистемой $\Sigma_\alpha \subset R$, образованной всеми корнями, которые являются целочисленными линейными комбинациями корней $\sigma^i(\alpha)$, $i = 0, \ldots, 4$. Так как тор T E-анизотропен, то $\alpha + \sigma(\alpha) + \ldots + \sigma^4(\alpha) = 0$, и, следовательно, $\operatorname{rang} \Sigma_\alpha \leqslant 4$. С другой стороны, σ индуцирует автоморфизм Σ_α порядка пять. Но единственной системой корней ранга, не превосходящего 4, обладающей таким свойством, является A_4. При доказательстве предложения 24 мы показали, что любые два корня $\alpha, \beta \in R$ такие, что $\alpha + \beta \in R$, в подходящем базисе являются соответственно максимальным корнем и корнем $-\alpha_8$. Рассуждая аналогично, несложно показать, что в подходящем базисе $\Pi \subset R$ группа $G(\alpha)$ совпадает с группой, порожденной корневыми подгруппами G_γ, где $\gamma \in \{\alpha_8, \alpha_7, \alpha_6, \mu\}$, μ — максимальный корень. Отсюда следует, что группа $G(\alpha)$ односвязна.

Далее, образуем произведение $T_0 = \prod_{\alpha \in R} T(\alpha)$, и пусть θ_0: $H^1(E, T_0) \to H^1(E, T)$ индуцируется отображениями θ_α: $H^1(E, T(\alpha)) \to H^1(E, T)$. Ниже мы покажем, что отображение θ_0 сюръективно, а сейчас, пользуясь этим фактом, завершим доказательство предложения 25. Пусть $\xi \in H^1(E, T)$ и $\xi = \prod_{i=1}^{n} \theta_{\alpha_i}(\xi_i)$, где $\xi_i \in H^1(E, T(\alpha_i))$. Проведем индукцию по n.

Если $n=1$, то $\xi=\theta_{\alpha_1}(\xi_1)$ и $\xi\in H^1(E, G(\alpha_1))=1$. В общем случае воспользуемся известной процедурой тривиализации ξ «по частям». А именно, так как $H^1(E, G(\alpha_n))=1$, то $\xi_n=\{a_\tau\}$, где $a_\tau=g^{-1}\tau(g)$, $\tau\in\mathrm{Gal}(\overline{E}/E)$ для подходящего $g\in G(\alpha_n)$. Рассмотрим тор $T'=gTg^{-1}$ и изоморфизм ψ: $T\to T'$, $\psi(x)=gxg^{-1}$. Используя тот факт, что $g^{-1}\tau(g)\in T$, легко показать, что тор T' и морфизм ψ определены над E. Положим $\xi'=\psi(\theta_{\alpha_1}(\xi_1), \ldots, \theta_{\alpha_{n-1}}(\xi_{n-1}))\in H^1(E, T')$. Непосредственно проверяется, что $\xi'=g\xi\tau(g)^{-1}$, поэтому достаточно установить тривиальность ξ'. С другой стороны, $\xi'=\psi(\theta_{\alpha_1}(\xi_1))\ldots$ $\ldots\psi(\theta_{\alpha_{n-1}}(\xi_{n-1}))$, причем $\psi(\theta_{\alpha_i}(\xi_i))\in\theta_{\alpha_i'}(H^1(E, T'(\alpha_i')))$, где $\alpha_i'=\psi(\alpha_i)$, и тривиальность ξ' вытекает из предположения индукции.

Для доказательства сюръективности θ_0 укажем способ вычисления $H^1(L/E, S)$ для произвольного E-анизотропного L-разложимого тора S в терминах когомологий группы однопараметрических подгрупп $\mathbf{X}_*(S)$.

Лемма 37. *Изоморфизм* $\mathbf{X}_*(S)\otimes L^*\to S_L$ *и* $\smile$*-произведение индуцируют изоморфизм*

$$\Phi_S\colon \hat{H}^{-1}(L/E, \mathbf{X}_*(S))\otimes\hat{H}^2(L/E, L^*)\to\hat{H}^1(L/E, S).$$

Доказательство. Положим $\Gamma=\langle\sigma\rangle$, обозначим через ε элемент $1+\sigma+\ldots+\sigma^4$ группового кольца $\mathbb{Z}[\Gamma]$ и рассмотрим Γ-модуль $I=\mathbb{Z}[\Gamma]/\mathbb{Z}\varepsilon$. Изучим вначале «модельный» случай $\mathbf{X}_*(S)=I$. Тогда модуль $\mathbf{X}_*(S)$ входит в точную последовательность

$$0\to\mathbb{Z}\xrightarrow{[\varepsilon]}\mathbb{Z}[\Gamma]\to I\to 0,$$

где $[\varepsilon]$ означает умножение на ε, а тор S — в точную последовательность

$$1\to\mathbf{G}_m\to\mathbf{R}_{L/E}(\mathbf{G}_m)\to S\to 1.$$

Из этих последовательностей получаются изоморфизмы

$$H^1(L/E, S)\simeq H^2(L/E, L^*),$$
$$\hat{H}^{-1}(L/E, I)\simeq\hat{H}^0(L/E, \mathbb{Z})=\mathbb{Z}/5\mathbb{Z},$$

которые объединяются в коммутативную диаграмму

$$\begin{array}{ccccc}
\hat{H}^{-1}(L/E, I)\otimes & \hat{H}^2(L/E, L^*) & \xrightarrow{\Phi_S} & H^1(L/E, S) \\
\wr\| & \| & & \wr\| \\
\hat{H}^0(L/E, \mathbb{Z})\otimes & \hat{H}^2(L/E, L^*) & \longrightarrow & H^2(L/E, L^*)
\end{array}$$

Так как нижняя строка, очевидно, является изоморфизмом, то Φ_S — также изоморфизм.

Из доказанного вытекает, что Φ_S является изоморфизмом и в случае $\mathbf{X}_*(S) = I^n$. С другой стороны, I можно отождествить с кольцом $\mathbb{Z}[\zeta_5]$ (где ζ_5 — примитивный корень степени 5 из единицы), которое является кольцом главных идеалов. Но для любого E-анизотропного тора S имеем $\varepsilon\mathbf{X}_*(S) \subset \mathbf{X}_*(S)^{\mathrm{Gal}(L/E)} = (0)$, так что $\mathbf{X}_*(S)$ можно рассматривать как модуль над $\mathbb{Z}[\Gamma]/\mathbb{Z}\varepsilon = I \simeq \mathbb{Z}[\zeta_5]$, и поэтому $\mathbf{X}_*(S)$ имеет вид $\mathbf{X}_*(S) = \mathbb{Z}[\zeta_5]^n = I^n$, что и доказывает лемму.

Из леммы вытекает, что для доказательства сюръективности отображения θ_0 достаточно установить сюръективность отображения $\widehat{H}^{-1}(L/E, \mathbf{X}_*(T_0)) \to \widehat{H}^{-1}(L/E, \mathbf{X}_*(T))$. Но по определению $\widehat{H}^{-1}(L/E, X) = \operatorname{Ker} N/(1-\sigma)X$, где $N\chi = \varepsilon\chi$ — норменное отображение. Поэтому $\widehat{H}^{-1}(L/E, \mathbf{X}_*(S)) = \mathbf{X}_*(S)/(1-\sigma)\mathbf{X}_*(S)$ для E-анизотропного тора S, и поэтому в нашем случае все следует из сюръективности отображения $\bigoplus_{\alpha \in R} \mathbf{X}_*(T(\alpha)) \to \mathbf{X}_*(T)$, которая очевидна.

Доказательство теорем 4 и 6 завершено.

Вопрос о справедливости теорем 6 для групп типа E_8 в течение долгого времени оставался открытым. Решающий шаг, позволивший завершить доказательство, состоит в получении теоремы 30, что было проделано совсем недавно В. И. Черноусовым [6]. Тем не менее теорема 4 в этом случае была известна ранее (Кнезер [9]). Ключевое отличие локальной ситуации от глобальной состоит в существовании локальной двойственности Накаямы — Тейта, что в сочетании с тщательным анализом подгрупп группы Вейля позволяет доказать предложение 25 для практически произвольных торов, а не только для торов специального вида, использованных нами.

Библиографические замечания. Значительная часть материала, изложенного в § 6.2—6.3, является традиционной (см. Борель [8], § 16, Воскресенский [3], гл. VI). Содержание § 6.4 практически полностью заимствовано из статьи Бореля, Серра [1]. Напротив, результаты, связанные с точным вычислением когомологий полупростых групп над локальными и числовыми полями, в таком целостном и завершенном виде излагаются впервые. Тривиальность $H^1(K, G)$ для односвязных групп над локальным полем K была установлена Кнезером [9]. В лекциях [12] им было показано, что теоремы 4 и 6 для групп классических типов эквивалентны известным результатам о свойствах и классификации квадратичных, эрмитовых и т. д. форм (так как эти результаты могут быть получены без использования когомологической техники, то тем самым мы получаем доказательство теорем 4, 6 для классических групп). Избранный нами вариант изложения использует лишь один результат из теории квадратичных форм — теорему Минковского — Хассе.

Следует указать также на определенные усовершенствования в доказательстве принципа Хассе для групп типа ${}^2A_n$, связанные с использованием мультинорменного принципа. Теорема 6 для исключительных групп, кроме типа E_8, была получена Хардером [1], [2]; случай типа E_8 был рассмотрен Черноусовым [6] (отметим, что для функциональных глобальных полей тривиальность $H^1(K, G)$ для полупростых односвязных групп всех типов была установлена Хардером [11]). Ряд результатов о когомологиях Галуа содержится в статье Сансюка [1]. Мы совсем не затрагиваем вопрос о когомологиях Галуа конечных коммутативных групп, которые описываются так называемыми теоремами Пуату — Тейта (см. Серр [1]). Подробное изложение этих результатов содержится в недавней книге Милна [2].

При изучении когомологий полупростых групп мы неоднократно использовали аппроксимационные результаты, которые будут подробно рассматриваться в следующей главе. Вот их полный список: 1) слабая аппроксимация в многообразии торов; 2) слабая аппроксимация в «сферах», определяемых квадратичными, эрмитовыми и т. д. формами; 3) слабая аппроксимация в любом торе относительно множества $S = V_\infty^K$; 4) сюръективность отображения $H^1(K, T) \to \prod_{v \in V_K^\infty} H^1(K_v, T)$ для любого тора T; 5) сильная аппроксимация для группы $G = \boldsymbol{SL}_n(D)$. Читатель может проверить, что эти факты не зависят ни от каких результатов о когомологиях Галуа полупростых групп, и поэтому их использование в настоящей главе допустимо.

ГЛАВА VII

АППРОКСИМАЦИЯ В АЛГЕБРАИЧЕСКИХ ГРУППАХ

В этой главе мы будем заниматься метрическим аспектом локально-глобального принципа, а именно, изучим вопрос о том, когда элементы локальных групп G_{K_v} и их произведений можно с любой степенью точности приблизить элементами группы G_K. В случае когда такое приближение возможно, говорят, что для группы G справедлива слабая аппроксимация. Хотя это понятие имеет смысл для произвольного поля K, мы, естественно, будем в основном интересоваться числовым случаем (см., однако, замечания в заключительной части § 7.3). Напротив, сильная аппроксимация (т. е. приближение при помощи элементов, которые дополнительно удовлетворяют некоторым условиям целочисленности) относится только к глобальным полям. Мы дадим определения как сильной, так и слабой аппроксимации применительно к произвольным многообразиям, однако содержательные результаты об аппроксимации к настоящему времени получены лишь для случая алгебраических групп. Дело в том, что имеющиеся методы в существенной степени используют групповую структуру рациональных точек, и по этой причине мы предваряем собственно аппроксимационные результаты обсуждением известной гипотезы Кнезера — Титса об изотропных группах (см. § 7.2). Отметим также, что начиная с этой главы все отчетливее будет проявляться синтетический характер арифметической теории алгебраических групп. Это относится как к основным идеям, так и к применяемым техническим средствам. В частности, в этой главе будет использовано большинство результатов предшествующих разделов.

§ 7.1. Сильная и слабая аппроксимация в алгебраических многообразиях

Пусть X — алгебраическое многообразие, определенное над числовым полем K. Возможность сколь угодно точного приближения элементов локальных пространств X_{K_v} элементами из X_K в действительности означает плотность X_K при вложении в некоторые топологические пространства, конструируемые из X_{K_v}. Так, с точки зрения топологии естественно рассмотреть топологическое прямое произведение $\underline{X} = \prod_{v \in V^K} X_{K_v}$ или его часть

$X_S = \prod_{v \in S} X_{K_v}$, где $S \subset V^K$ — некоторое подмножество, в то время как с точки зрения арифметики следует обратиться к пространствам S-аделей X_{A_S} с соответствующей топологией (см. § 5.1). И в том и в другом случае имеется естественное диагональное вложение $X_K \hookrightarrow \underline{X}$ ($X_K \hookrightarrow X_S$) и $X_K \hookrightarrow X_{A_S}$. В этих терминах мы и дадим следующее.

Определение. 1) Говорят, что для X имеет место *слабая аппроксимация* (соответственно *слабая аппроксимация относительно подмножества* $S \subset V^K$), если диагональное вложение $X_K \hookrightarrow \underline{X}$ (соответственно $X_K \hookrightarrow X_S$) является плотным.

2) Многообразие X обладает свойством *сильной аппроксимации* относительно конечного подмножества $S \subset V^K$, если плотно диагональное вложение $X_K \hookrightarrow X_{A_S}$ *). В случае $S = V^K_\infty$ говорят об *абсолютной сильной аппроксимации.*

Опишем вначале функториальные свойства этих понятий.

Предложение 1. 1) *Если многообразия X и Y бирегулярно изоморфны над K, то они одновременно обладают или не обладают сильной (соответственно слабой) аппроксимацией.*

2) *Если $X = X_1 \times X_2$ над K, то наличие сильной (соответственно слабой) аппроксимации в X равносильно наличию аппроксимации того же типа в обоих сомножителях.*

3) *Если $X = \mathbf{R}_{L/K}(Y)$, то наличие сильной (соответственно слабой) аппроксимации в X над K относительно подмножества $S \subset V^K$ равносильно наличию аппроксимации того же типа в Y над L относительно подмножества $\bar{S} \subset V^L$, образованного всеми продолжениями нормирований из S.*

Доказательство вытекает из существования естественных гомеоморфизмов между пространствами, участвующими в определении аппроксимации. Например, $X_S \simeq Y_S$ в условиях пункта 1), а $X_S \simeq Y_{\bar{S}}$ в условиях пункта 3) для любого $S \subset V^K$ (детали рассуждений мы оставляем читателю).

Следует обратить внимание, что в случае $X = \mathbb{A}^1$ приведенные определения переходят в классические определения сильной и слабой аппроксимации для поля K. В частности, из соответствующих аппроксимационных теорем (см. теоремы 1.4 и 1.5) и п. 2) предложения 1 получаем, что аффинное пространство $\mathbb{A}^n$ обладает слабой аппроксимацией и сильной аппроксимацией относительно любого непустого S. Так как многообразие произвольной унипотентной K-группы U бирегулярно изоморфно над K аффинному пространству $\mathbb{A}^n$, $n = \dim U$, то из п. 1), 2) получаем

---

*) Отметим, что в случае, когда X является алгебраической группой, можно дать эквивалентную формулировку: произведение $X_S X_K$ должно быть плотным в X_A.

Следствие. *Пусть $G = HR_u(G)$ — разложение Леви связной группы G. Тогда наличие сильной (соответственно слабой) аппроксимации для G равносильно наличию аппроксимации того же типа для H.*

Приведем теперь для удобства ссылок несколько простых фактов о сильной и слабой аппроксимации.

Предложение 2. 1) *Наличие слабой аппроксимации в X относительно произвольного $S \subset V^K$ равносильно наличию слабой аппроксимации относительно любого конечного подмножества $S' \subset S$.*

2) *Многообразие X обладает сильной аппроксимацией относительно конечного подмножества $S \subset V^K$ в том и только том случае, если для любого конечного подмножества $T \subset V^K$, содержащего $S \cup V^K_\infty$, множество $X_{\mathcal{O}(T)}$ T-целых точек плотно в $X_{T \setminus S}$ (при диагональном вложении). В частности, если группа G обладает сильной аппроксимацией относительно S, то она обладает слабой аппроксимацией относительно $V^K \setminus S$. Если многообразие X проективно, то верно и обратное: слабая аппроксимация относительно $V^K \setminus S$ влечет сильную аппроксимацию относительно S.*

3) *Если для X имеет место слабая (соответственно сильная) аппроксимация относительно произвольного (соответственно конечного) подмножества $S \subset V^K$, то аппроксимация того же типа имеет место и для любого $S_1 \subset S$ (соответственно конечного $S_1 \supset S$).*

4) *Если многообразие X обладает слабой апроксимацией относительно S, то любое открытое K-подмногообразие $U \subset X$ также обладает слабой аппроксимацией относительно S.*

Доказательство утверждения 1) вытекает из определения топологии на прямом произведении. Для доказательства 2) напомним, что базу открытых множеств в X_{A_S} составляют множества вида $W = \prod_{v \in T \setminus S} U_{K_v} \times \prod_{v \notin T} X_{\mathcal{O}_v}$, где $T \subset V^K$ — конечное подмножество, содержащее $S \cup V^K_\infty$, и $U_v \subset X_{K_v}$ открыто для $v \in T \setminus S$. Поэтому сильная аппроксимация для X относительно S сводится к условию $X_K \cap W \neq \varnothing$ для любого такого W, что, очевидно, равносильно непустоте пересечения $X_{\mathcal{O}(T)} \cap \prod_{v \in T \setminus S} U_v$, т. е. плотности $X_{\mathcal{O}(T)}$ в $X_{T \setminus S}$. В § 3.1 мы видели, что $\mathbb{P}^n_{\mathcal{O}_v} = \mathbb{P}^n_{K_v}$ для всех $v \in V^K_f$, поэтому при любой реализации проективного многообразия X всегда $X_{\mathcal{O}_v} = X_{K_v}$ для почти всех $v \in V^K_f$. Таким образом, здесь топологическое пространство X_{A_S} совпадает с пространством $X_{V^K \setminus S}$, откуда и следует требуемое. Утверждение п. 3) вытекает из того обстоятельства, что при $S_1 \subset S$ (соответственно $S_1 \supset S$) имеется естественная непрерывная

проекция $X_S \to X_{S_1}$ (соответственно $X_{A_S} \to X_{A_{S_1}}$), согласованная с соответствующими диагональными вложениями X_K. Наконец, для доказательства 4) достаточно заметить, что поскольку v-адическая топология на X_{K_v}, определенная в § 3.1, сильнее топологии Зарисского, то любое открытое множество $W \subset U_S$ является в то же время открытым в X_S, поэтому пересечение $W \cap X_K$ непусто и, очевидно, содержится в U_K. Предложение 2 полностью доказано.

Сильная аппроксимация имеет ярко выраженный арифметический характер. А именно, в основном случае, когда $S \supset V_\infty^K$, ее выполнимость равносильна разрешимости в целых числах некоторой системы сравнений для элементов многообразия X. Более точно, пусть $X \subset \mathbb{A}^n$. Тогда любое открытое подмножество в X_{A_S} содержит подмножество вида

$$W = \prod_{i=1}^{r} \left(X_{K_{v_i}} \cap \left(\left(a_1^i + \mathfrak{p}_{v_i}^{m_i}\right) \times \ldots \times \left(a_n^i + \mathfrak{p}_{v_i}^{m_i}\right)\right)\right) \times \prod_{v \notin S_1} X_{O_v},$$

где $v_1, \ldots, v_r \notin S$, $m_1, \ldots, m_r$ — целые > 0, $S_1 = S \cup \{v_1, \ldots, v_r\}$, $a^i = (a_1^i, \ldots, a_n^i) \in X_{K_v}$. Поэтому вопрос о непустоте пересечения $X_K \cap W$ сводится к разрешимости относительно точек $x \in X_{O(S_1)}$ системы сравнений

$$x \equiv a^i \left(\operatorname{mod} \mathfrak{p}_{v_i}^{m_i}\right), \tag{1}$$

где запись $a \equiv b \left(\operatorname{mod} \mathfrak{p}_v^m\right)$ для элементов $a = (a_1, \ldots, a_n)$ и $b = (b_1, \ldots, b_n)$, лежащих в K_v^n, но не обязательно в O_v^n означает, что $a_i - b_i \in \mathfrak{p}_v^m$ для всех $i = 1, \ldots, n$. Поэтому вопрос о сильной аппроксимации для X представляет алгебро-геометрическую версию «китайской теоремы об остатках». Учитывая ту фундаментальную роль, которую последняя играет в классической арифметике, естественно предположить, что сильная аппроксимационная теорема для алгебраических групп, которую мы докажем в § 7.4, должна лежать в основе получения важных результатов нашей теории. В справедливости этого предположения мы убедимся в последующих главах.

На этом мы закончим обсуждение аппроксимационных задач в контексте произвольных многообразий, и большинство последующих результатов будет относиться только к алгебраическим группам. Такое ограничение вполне естественно, ибо если исследовать вопрос о разрешимости системы (1) только с позиций диофантовой геометрии, т. е. не используя групповую структуру, то задача становится исключительно сложной. Так, ниже мы покажем, что для группы $G = \boldsymbol{SL}_2$ имеет место абсолютная сильная аппроксимация, поэтому соответствующая система (1) должна иметь решение. С другой стороны, G как алгебраическое многообразие задается уравнением $xy - zt = 1$, и

мы настоятельно рекомендуем читателю убедиться, что установить возможность подъема решений этого уравнения по некоторой системе модулей до целочисленного решения не так-то легко. Этот пример показывает, что в проблеме сильной аппроксимации ключевую роль играют не столько геометрические свойства G, сколько групповая структура. Наоборот, слабая аппроксимация связана с геометрией G более тесным образом.

Предложение 3. *Пусть X — неприводимое гладкое K-рациональное многообразие. Тогда для X имеет место слабая аппроксимация.*

Доказательство. Условие K-рациональности многообразия X означает существование бирегулярного K-изоморфизма $\varphi\colon U \to W$ между открытыми подмножествами $U \subset \mathbb{A}^l$ $(l = \dim X)$ и $W \subset X$. Из предложений 1 и 2 вытекает, что W обладает слабой аппроксимацией, т. е. W_K плотно в $\prod_v W_{K_v}$. С другой стороны, согласно лемме 3.2, W_{K_v} плотно в X_{K_v} для любого v. Отсюда следует, что W_K, и тем более X_K, плотно в $\prod_v X_{K_v}$.

Доказанное предложение является для нас первым примером связей, существующих между геометрией линейных алгебраических групп и их арифметикой. Эти связи охватывают целый комплекс вопросов, таких как слабая аппроксимация, справедливость принципа Хассе, вычисление чисел Тамагавы и др. Однако в данной книге мы не имеем возможности подробно заниматься этими вопросами и ограничимся краткими замечаниями в § 7.3. В действительности для наших целей вполне хватает следствий, получаемых непосредственно из предложения 3.

Следствие 1. *Пусть X — квадрика, т. е. поверхность в $\mathbb{A}^n$ $(n \geqslant 1)$, задаваемая уравнением вида $f(x_1, \ldots, x_n) = a$, где f — невырожденная квадратичная форма над K, $a \in K^*$. Если $X_K \neq \varnothing$, то для X имеет место слабая аппроксимация.*

Действительно, хорошо известно, что X является гладким, а в случае $X_K \neq \varnothing$ — и K-рациональным многообразием. Отметим, что вопрос о сильной аппроксимации для X оказывается более тонким (см. Рапинчук [8]).

Доказанное утверждение частично восполняет пробел, который остался у нас в предыдущей главе, где мы использовали наличие слабой аппроксимации для «сфер», связанных с формами всех типов, т. е. для многообразий вида $f(x) = a$, где f — квадратичная, эрмитова и т. д. форма. Как мы видели в § 6.6, «сферы», отвечающие эрмитовым формам над квадратичным расширением L/K или телом кватернионов D/K, в действительности эквивалентны квадрикам большей размерности, и поэтому слабую аппроксимацию для них можно считать доказанной. С другой стороны, для косоэрмитовых форм над телом

кватернионов D рациональность соответствующих сфер пока неизвестна, так что непосредственно предложение 3 здесь неприменимо. По этой причине приходится использовать несколько другой подход, который позволяет рассмотреть все типы форм одновременно и основывается на следующем обобщении предложения 3.

Предложение 3′. *Пусть X — гладкое неприводимое K-многообразие такое, что для подходящего K-многообразия Y произведение $X \times Y$ рационально над K. Тогда для X имеет место слабая аппроксимация.*

Доказательство легко получается из предложения 3 и утверждения 2) предложения 1.

Пусть теперь f — невырожденная n-мерная эрмитова (косоэрмитова) форма над телом D, снабженным инволюцией τ такой, что поле неподвижных относительно τ элементов центра D совпадает с K.

Предложение 4. *Пусть G — связная компонента унитарной группы $U_n(f)$. Тогда многообразие G рационально над K. В частности, для G имеет место слабая аппроксимация.*

Доказательство получается при помощи известной параметризации Кэли — Диксона. А именно, обозначим через $\mathfrak{g} = L(G)$ алгебру Ли группы G и рассмотрим соответствие

$$\rho\colon X \longmapsto \frac{E_n - X}{E_n + X}, \quad X \in \mathfrak{g}. \tag{2}$$

Тогда оказывается, что ρ задает K-определенный бирациональный изоморфизм между $\mathfrak{g}$ и G. Для доказательства следует заметить, что поскольку $U_n(f) = \{x \in M_n(D) \otimes_K \overline{K} \mid {}^*xFx = F\}$, где для $x = (x_{ij})$ полагаем ${}^*x = (\tau(x_{ji}))$, F — матрица формы f, то $\mathfrak{g} = \{X \in M_n(D) \otimes_K \overline{K} \mid {}^*XF + FX = 0\}$. Поэтому прямое вычисление, использующее (2), показывает, что образ ρ попадает в $U_n(f)$, а следовательно, и в G, ибо $\rho(0) = E_n \in G$ и G является связной компонентой $U_n(f)$. При этом обратное к ρ отображение задается той же формулой (2). Таким образом, рациональность G доказана. Остается заметить, что групповые многообразия являются гладкими, и поэтому для них слабая аппроксимация автоматически вытекает из рациональности.

Теперь у нас уже есть все необходимое, чтобы завершить доказательство слабой аппроксимации для «сфер».

Следствие 2. *Пусть f — невырожденная n-мерная ($n \geqslant 2$) эрмитова (косоэрмитова) форма, $a \in D^*$ — соответственно эрмитов (косоэрмитов) элемент. Положим $X = \{x \in D^n \otimes_K K \mid f(x) = a\}$. Тогда если $X_K \neq \varnothing$, то X обладает слабой аппроксимацией.*

Действительно, пусть $x \in X_K$. Рассмотрим отображение φ: $G \to X$, $\varphi(g) = gx$, где G, как и выше, — связная компонента со-

ответствующей унитарной группы $\boldsymbol{U}_n(f)$. Из теоремы Витта вытекает, что φ сюръективно, т. е. X можно отождествить с однородным пространством G/H, где $H = G(x)$ — стабилизатор точки x, в частности, X является гладким. Более того, теорема Витта позволяет утверждать, что $\varphi(G_L) = X_L$ для любого расширения L поля K. Применяя это к полю рациональных функций $L = K(X)$, получаем рациональное K-определенное сечение ψ: $X \to G$, так что бирационально G изоморфно $X \times H$. Но в силу предложения 4 G рационально, поэтому доказательство завершается применением предложения 3′.

В связи с обсуждением проблемы рациональности отметим, что, к сожалению, группами, описанными в предложении 4, и K-разложимыми группами в основном исчерпываются те групповые многообразия, о которых известно, что они рациональны. В частности, долгое время оставался не решенным вопрос о рациональности спинорных многообразий $\boldsymbol{Spin}_n(f)$, являющихся двулистными накрытиями специальной ортогональной группы $\boldsymbol{SO}_n(f)$, рациональность которой вытекает из предложения 4. Несложно показать, что многообразие $\boldsymbol{Spin}_n(f)$ при $n \leqslant 5$ является K-рациональным (см. Платонов [18]), однако, как показано первым из авторов, для $n \geqslant 6$ вида $4k+2$ над подходящим полем K существуют нерациональные спинорные многообразия (см. Платонов [18], [19]). Этот результат был получен на основе развития методов приведенной K-теории, позволивших в свое время установить существование нерациональных многообразий типа $\boldsymbol{SL}_1(D)$ (см. Платонов [17], Воскресенский [3]). С другой стороны, если поле K является локально компактным, то любое спинорное многообразие над K всегда K-рационально (см. Платонов [18], Платонов, Черноусов [1]), причем для $K = \mathbb{R}$ известна рациональность большинства групповых K-многообразий. Для числовых полей рациональность $\boldsymbol{Spin}_n(f)$ известна лишь над полем рациональных чисел (см. Черноусов [1]). Отметим, однако, что вопрос о слабой аппроксимации для алгебраических групп над числовыми полями решается другими методами (см. § 7.3).

Еще одно важное для нас применение предложения 3 содержит

Следствие 3. *Пусть G — редуктивная алгебраическая группа над числовым полем K и $\mathcal{T}$ — многообразие ее максимальных торов. Тогда для $\mathcal{T}$ имеет место слабая аппроксимация. В частности, если $S \subset V^K$ — конечное подмножество и для каждого $v \in S$ задан K_v-определенный максимальный тор $T(v) \subset G$, то существует такой K-определенный максимальный тор $T \subset G$, который для любого $v \in S$ сопряжен с тором $T(v)$ при помощи элемента из G_{K_v}.*

Действительно, будучи однородным пространством группы G, многообразие $\mathcal{T}$ является гладким. Его рациональность над K

мы установили в теореме 2.18. Поэтому $\mathcal{T}$ обладает слабой аппроксимацией. Далее, если $x_v \in \mathcal{T}$ — отвечающая $T(v)$ точка $\mathcal{T}$ $(v \in S)$, то торы из класса сопряженности $\{gT(v)g^{-1} \mid g \in G_{K_v}\}$ в точности соответствуют точкам орбиты $U_v = G_{K_v} x_v$. Но U_v открыто в $\mathcal{T}_{K_v}$ (см. следствие 2 из предложения 3.3), поэтому по свойству слабой аппроксимации для $\mathcal{T}$ найдется точка $x \in \mathcal{T}_K \cap \prod_{v \in S} U_v$. Отвечающий ей максимальный тор $T \subset G$ и будет искомым. (Обратим внимание читателя на то обстоятельство, что слабая аппроксимация для многообразия торов имеет место всегда, вне зависимости от слабой аппроксимации в группе G. Уникальность этого явления заключается в том, что обычно слабая аппроксимация в однородном пространстве выводится из слабой аппроксимации в группе (ср. доказательство следствия 2), а не наоборот.)

§ 7.2. Гипотеза Кнезера — Титса

Выше мы отмечали, что далеко продвинуться в вопросах аппроксимации для алгебраических групп, не используя групповую структуру, по-видимому, нельзя. Это объясняет появление в главе об аппроксимации параграфа, посвященного чисто структурным вопросам. Их последовательное изложение может составить предмет отдельной книги, так что настоящий параграф неминуемо приобретает обзорный характер. Тем не менее основной необходимый нам для дальнейшего результат о справедливости гипотезы Кнезера — Титса над локальными полями (теорема 6) мы доказываем фактически полностью.

Структурная теория линейных алгебраических групп дает, практически, исчерпывающую информацию о строении алгебраической группы G над алгебраически замкнутым полем. Однако ситуация резко меняется, если рассматривать группы рациональных точек G_K над полем K, которое не является алгебраически замкнутым. Основные трудности при этом сосредоточены в случае простой группы G, которым мы и будем здесь заниматься. Необходимо различать также K-анизотропный и K-изотропный случаи. В первом структура G_K в существенной степени определяется не только самой группой G, но и арифметикой поля K. В частности, в зависимости от G и K группа G_K может быть финитно аппроксимируемой или даже проразрешимой (см. § 1.4, п. 4). Наоборот, в изотропном случае G_K всегда содержит «большой» нормальный делитель, который уже не содержит собственных нецентральных нормальных подгрупп. Более точно, для абсолютно простой, определенной и изотропной над полем K группы G обозначим через G_K^+ подгруппу (в действительности, нормальную подгруппу) в G_K, порожденную

K-рациональными элементами унипотентных радикалов K-определенных параболических подгрупп (отметим, что в основном для нас случае совершенного поля K можно определить G_K^+ просто как подгруппу, порожденную K-рациональными унипотентными элементами). Тогда имеет место следующая

Теорема 1 (Титс [1]). *Пусть поле K содержит не менее четырех элементов. Тогда любая подгруппа в G_K, нормализуемая группой G_K^+, либо содержит G_K^+, либо центральна. В частности, G_K^+ не имеет нетривиальных нецентральных нормальных делителей.*

Доказательство этой теоремы, которое мы здесь не приводим, использует построение в группе G_K некоторой BN-пары (см. § 3.4). Отметим, что для классических групп утверждение теоремы может быть получено методами геометрической алгебры (см. Артин [1], Дьедонне [2]).

Из теоремы 1 вытекает, что строение (по крайней мере нормальное) группы G_K можно считать известным, если $G_K^+ = G_K$. Уже довольно давно было показано, что это действительно так, если односвязная группа G является K-разложимой (Шевалле [4]) или K-квазиразложимой (Стейнберг [2]). Это, в частности, в силу предложения 6.1 дает полную картину в случае конечного поля K.

Предложение 5. *Если группа G односвязна, а поле K конечно, то $G_K^+ = G_K$. В частности, если $|K| \geqslant 4$, то группа G_K не имеет нетривиальных нецентральных нормальных делителей.*

(Исключительные случаи полей F_2 и F_3 разобраны в работе Титса [1].)

Имеются результаты о совпадении G_K^+ и G_K для других типов полей, о которых мы расскажем ниже. Кроме того, известно, что $G_K^+ = G_K$, если G является группой типов B_n, C_n $(n \geqslant 1)$ либо некоторой специальной формой одной из исключительных групп (см. Титс [4]). Эти результаты, по-видимому, послужили мотивировкой для формулировки следующей естественной гипотезы (см. Титс [1]):

Гипотеза (Кнезер — Титс). *Для односвязной простой группы G, определенной и изотропной над произвольным полем K, всегда $G_K^+ = G_K$.*

Условие односвязности здесь существенно и заведомо не может быть опущено. Чтобы показать это, прежде всего заметим, что если π: $\tilde{G} \to G$ — универсальное K-определенное накрытие и поле K совершенно, то $\pi(\tilde{G}_K^+) = G_K^+$. В самом деле, пусть $g \in G_K$ — унипотентный элемент, причем $g = \pi(x)$, где $x \in \tilde{G}$. Если $x = x_s x_u$ — разложение Жордана, то, очевидно, $\pi(x_s) = 1$, $\pi(x_u) = g$, так что можно считать элемент x унипотентным. Для любого $\sigma \in \mathrm{Gal}(\bar{K}/K)$ имеем $\pi(\sigma(x)) = \sigma(g) = g = \pi(x)$, так что

$\sigma(x) = fx$, где $f \in F = \operatorname{Ker} \pi$. Но F состоит из полупростых элементов, поэтому из унипотентности x и $\sigma(x)$ вытекает, что $f = 1$, т. е. $x \in \tilde{G}_K$. Мы показали, что любой унипотентный элемент из G_K является образом унипотентного элемента из $\tilde{G}_K$. Так как в силу совершенности K любой унипотентный элемент из G_K лежит в унипотентном радикале подходящей K-определенной параболической подгруппы, то отсюда вытекает, что $\pi(\tilde{G}_K^+) = G_K^+$, что и требовалось. С другой стороны, имеется обширный класс полей K, для которых $\pi(\tilde{G}_K) \neq G_K$ при $\operatorname{Ker} \pi \neq 1$.

Теорема 2 (Платонов [10]). *Пусть K — конечно порожденное бесконечное поле, π: $\tilde{G} \to G$ — нетривиальная центральная K-изогения связных алгебраических K-групп. Тогда $\pi(\tilde{G}_K) \neq G_K$. В частности, если группа G неодносвязна и изотропна над бесконечным конечно порожденным полем K, то $G_K \neq G_K^+$.*

Гипотеза Кнезера — Титса очевидным образом справедлива для алгебраически замкнутого поля K. Однако уже случай поля вещественных чисел требует более тонких рассуждений.

Предложение 6 (Э. Картан [1]). *Пусть G — простая односвязная алгебраическая группа над полем вещественных чисел $\mathbb{R}$. Тогда группа $G_{\mathbb{R}}$ не имеет нетривиальных нецентральных нормальных делителей. В частности, группа $G_{\mathbb{R}}$ связна, и для $\mathbb{R}$-изотропной группы G всегда $G_{\mathbb{R}}^+ = G_{\mathbb{R}}$.*

Доказательство для случая $\mathbb{R}$-анизотропной группы G, т. е. когда $G_{\mathbb{R}}$ компактна, было проведено нами в § 3.2 (см. предложение 3.6). В изотропном случае оно использует некоторые структурные результаты о группе G (см. Борель, Титс [1]), которые справедливы над любым полем K и понадобятся нам также и в дальнейшем. Пусть S — максимальный K-разложимый тор группы G, $H = Z_G(S)$ — его централизатор, U и U^- — унипотентные радикалы двух противоположных минимальных параболических подгрупп, содержащих тор S. Тогда морфизм-произведение задает K-определенный изоморфизм $U \times H \times U^-$ на открытое по Зарисскому подмножество $W \subset G$. Для любого $g \in G_K$ множество $V = W \cap gW^{-1}$ в силу связности G является непустым и открытым, поэтому $V \cap G_K = W_K \cap gW_K^{-1} \neq \varnothing$, ибо G_K плотно в G (теорема 2.2). Таким образом, $g \in W_K W_K$; в частности, W_K порождает G_K, откуда следует, что

$$G_K/G_K^+ \simeq H_K/(H_K \cap G_K^+),$$

и поэтому $G_K^+ = G_K$ в том и только том случае, если $H_K \subset G_K^+$. Далее, разложим H на составные части. Пусть S' — связная компонента центра группы H (отметим, что, вообще говоря, $S' \neq S$). Тогда S' является тором, а S — его максимальным K-разложимым подтором. Поэтому S' представляется в виде почти прямого произведения $S' = S \cdot S''$, где S'' — макси-

мальный K-анизотропный подтор в S'. В свою очередь, $H = D \cdot S'$, где $D = [H, H]$ — полупростая K-анизотропная группа. Положим $B = D \cdot S''$. Тогда $H = B \cdot S$ — почти прямое произведение, причем группа B анизотропна над K. Известно (см. Борель, Титс [2]), что S содержится в односвязной K-разложимой полупростой подгруппе в G, и, следовательно, $S_K \subset G_K^+$. Воспользуемся теперь спецификой поля $\mathbb{R}$. Рассмотрим коммутативную диаграмму

$$\begin{array}{ccc} H & \longrightarrow & H/S \\ \uparrow & & \wr\downarrow \\ B & \xrightarrow{\alpha} & B/B \cap S \end{array}$$

и покажем, что $\alpha(B_{\mathbb{R}}) = (B/B \cap S)_{\mathbb{R}}$. Группа $B/B \cap S$ анизотропна над $\mathbb{R}$, поэтому группа $(B/B \cap S)_{\mathbb{R}}$ компактна и, следовательно, связна (следствие 1 из теоремы 3.6). Поэтому в силу следствия 3 из теоремы 3.6 $\alpha(B_{\mathbb{R}}) = (B/B \cap S)_{\mathbb{R}}$, откуда $H_{\mathbb{R}} = B_{\mathbb{R}} S_{\mathbb{R}}$. Так как $S_{\mathbb{R}} \subset G_{\mathbb{R}}^+$, то достаточно установить включение $B_{\mathbb{R}} \subset G_{\mathbb{R}}^+$. Поскольку группа $B_{\mathbb{R}}$ также компактна, а значит, и связна, то это вытекает из открытости $G_{\mathbb{R}}^+$ (теорема 3.3). Предложение 6 доказано.

Случай поля вещественных чисел является, по-видимому, единственным, где доказательство гипотезы Кнезера — Титса основывается на общих структурных соображениях. Во всех остальных случаях приходится, как правило, отдельно разбираться с каждым из типов простых групп. Это отчетливо видно уже в случае неархимедова локально-компактного поля K, который наиболее важен для нас с точки зрения задач аппроксимации. Здесь доказательство гипотезы Кнезера — Титса было впервые получено В. П. Платоновым. Оно основывается на классификации простых алгебраических групп над локальными полями и состоит в редукции к группам классического типа, для которых доказательство получается из других соображений. Изложение доказательства мы начнем с напоминания используемых фактов о классических группах.

Доминирующее положение в классических группах занимают группы типа A_n. Если G является внутренней формой типа A_n, то $G = \boldsymbol{SL}_m(D)$, где D — конечномерная центральная алгебра с делением над K (см. § 2.3). Условие K-изотропности G равносильно неравенству $m \geqslant 2$, и в этом случае обозначим через $SL'_m(D)$ подгруппу в $G_K = SL_m(D)$, порожденную трансвекциями, т. е. такими матрицами $x \in SL_m(D)$, которые в подходящем базисе пространства D^m имеют вид элементарной матрицы $e_{ij}(\alpha)$, $\alpha \in D$, $i \neq j$. Легко видеть, что каждая элементарная матрица является унипотентным элементом (более того, лежит в унипотентном радикале подходящей параболической подгруппы),

и поэтому $SL'_m(D) \subset G_K^+$. С другой стороны, подгруппа $SL'_m(D)$ нормальна в $SL_m(D)$ (и даже в $GL_m(D)$), так что в силу теоремы 1 $G_K^+ = SL'_m(D)$. Таким образом,

$$G_K/G_K^+ \simeq SL_m(D)/SL'_m(D).$$

Но определитель Дьедонне (см. Артин [1], Дьедонне [2]) индуцирует изоморфизм последней факторгруппы на приведенную группу Уайтхеда $SK_1(D) = SL_1(D)/[D^*, D^*]$ алгебры D. Итак, для группы $G = \boldsymbol{SL}_m(D)$ $(m \geqslant 2)$ справедливость гипотезы Кнезера — Титса равносильна высказанной в 1943 г. гипотезе Таннаки — Артина о тривиальности приведенной группы Уайтхеда $SK_1(D)$ (см. также Басс [2], с. 222).

Аналогично, если G — внешняя форма типа A_n, то $G = \boldsymbol{SU}_m(f)$, где f — невырожденная m-мерная эрмитова форма над телом D с инволюцией τ второго рода, причем K совпадает с подполем τ-инвариантных элементов центра L тела D. Условие K-изотропности G сводится к изотропности формы f (см. § 2.3), и в этом случае группа G_K^+ совпадает с подгруппой $TU_m(f)$, порожденной так называемыми унитарными трансвекциями. Далее, норма Уолла индуцирует изоморфизм факторгруппы $SU_m(f)/TU_m(f)$ на приведенную унитарную группу Уайтхеда $SUK_1(D)$. Последняя определяется как факторгруппа Σ'/Σ, где Σ — подгруппа в D^*, порожденная всеми симметрическими относительно τ элементами, а Σ' состоит из элементов с симметрической приведенной нормой (подробности см. в работе Янчевского [2]).

Теорема 3. *Пусть D — конечномерная алгебра с делением (соотв., конечномерная алгебра с делением, снабженная инволюцией второго рода) над локальным или глобальным полем. Тогда приведенная группа Уайтхеда $SK_1(D)$ (соответственно приведенная унитарная группа Уайтхеда $SUK_1(D)$) тривиальна.*

Доказательство тривиальности $SK_1(D)$ мы провели в гл. I (см. § 1.4—1.5). Тривиальность $SUK_1(D)$ над локальным полем очевидна, ибо здесь $D = L$; случай глобальных полей разобран в работе Платонова, Янчевского [1].

Теорема 3 перестает быть справедливой над произвольным полем K, т. е. гипотеза Кнезера — Титса в общем случае неверна. Круг связанных с этим вопросов мы обсудим в заключительной части параграфа, а сейчас укажем класс групп, для которых гипотеза Кнезера — Титса, наоборот, справедлива над произвольным полем. Это, в первую очередь, спинорные группы $G = \boldsymbol{Spin}_n(f)$, $n \geqslant 3$, где f — невырожденная K-определенная квадратичная форма. Условие K-изотропности G эквивалентно K-изотропности f (см. § 2.3), и тогда известные результаты геометрической алгебры (см. Артин [1], Дьедонне [2]) дают полную картину строения соответствующей специальной ортого-

нальной группы $\boldsymbol{SO}_n(f)_K$: образ $\boldsymbol{Spin}_n(f)_K$ в $\boldsymbol{SO}_n(f)_K$ при естественном двулистном накрытии π: $\boldsymbol{Spin}_n(f) \to \boldsymbol{SO}_n(f)$ (который совпадает с ядром так называемой «спинорной нормы») не имеет собственных нецентральных нормальных делителей и

$$\boldsymbol{SO}_n(f)_K/\pi(\boldsymbol{Spin}_n(f)_K) \simeq K^*/K^{*2}.$$

С другой стороны, $\operatorname{Ker}\pi = \{\pm 1\}$ вкладывается в группу $\boldsymbol{Spin}_3(g)$, где g — трехмерная изотропная подформа f, а так как $\boldsymbol{Spin}_3(g) \simeq \boldsymbol{SL}_2$ над K, то

$$-1 \in \boldsymbol{Spin}_3(g)_K^+ \subset \boldsymbol{Spin}_3(f)_K^+,$$

и, окончательно, $\boldsymbol{Spin}_n(f)_K^+ = \boldsymbol{Spin}_n(f)_K$.

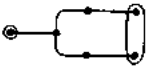
Осталось разобрать случай унитарных групп над телами с инволюцией первого рода. Итак, пусть D — тело над K с инволюцией τ первого рода и первого типа $\left(\text{это означает, что если } [D:K] = m^2, \text{ то } \dim D^\tau = \frac{m(m+1)}{2}\right)$. Если невырожденная полуторалинейная форма f степени n является косоэрмитовой, то в силу результатов § 2.3 группа $G = \boldsymbol{SU}_n(f)$ является простой односвязной группой типа C_l, причем, как показал Дьедонне [1], для нее всегда выполняется гипотеза Кнезера — Титса. Для эрмитовой формы f группа $G = \boldsymbol{SU}_n(f)$ является неодносвязной группой типа D_l, причем для односвязной накрывающей $\tilde{G}$ гипотеза Кнезера — Титса выполняется при условии, что D — тело кватернионов (см. Сейп — Хорникс [1]). Таким образом, гипотеза Кнезера — Титса выполняется над произвольным полем для всех групп типов B_l, C_l и групп типа D_l, связанных либо с полем, либо с телом кватернионов. Так как над локальными и глобальными полями этими группами исчерпываются все группы классических типов (см. § 2.3), то мы можем подвести итог нашего обсуждения гипотезы Кнезера — Титса для таких групп.

Предложение 7. *Пусть K — локальное или глобальное поле. Тогда для любой простой односвязной K-группы G, относящейся к одному из типов A_l, B_l, C_l, D_l (кроме ${}^3D_4$, ${}^6D_4$), выполняется гипотеза Кнезера — Титса.*

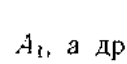
Редукция доказательства гипотезы Кнезера — Титса для произвольных групп к группам классического типа проводится по следующей схеме. Пусть простая односвязная K-группа G изотропна над K и $S \subset G$ — максимальный K-разложимый тор. При доказательстве предложения 6 мы видели, что равенство $G_K^+ = G_K$ равносильно включению $H_K \subset G_K^+$, где $H = Z_G(S)$ — централизатор тора S. Чтобы установить это включение, строятся такие простые односвязные K-изотропные подгруппы $G_i \subset G$, нормализуемые тором S, для которых гипотеза Кнезера — Титса

уже доказана (скажем, G_i — группы классического типа), и группы H_{i_K}, где $H_i = Z_{G_i}(S \cap G_i)^0$, порождают H_K (отметим, что $(S \cap G_i)^0$ — максимальный K-разложимый тор в G_i и $H_i \subset H$). Если такое построение возможно, то $H_{i_K} \subset G_{i_K} = G_{i_K}^+ \subset G_K^+$, и, следовательно, $H_K \subset G_K^+$, что и требовалось. Впервые этот метод был применен В. П. Платоновым [4] для доказательства гипотезы Кнезера — Титса над локальными полями. Подгруппы G_i строились при этом путем выбрасывания одной или нескольких выделенных вершин в соответствующем индексе Титса группы G, поэтому этот метод получил название «процедуры выбрасывания вершин». Позднее Прасад и Рагунатан [3] развили этот метод и показали, что в качестве групп G_i можно всегда выбрать группы K-ранга 1. Тем самым получена редукция доказательства гипотезы Кнезера — Титса над произвольным полем к группам относительного ранга 1. Для точной формулировки этого результата нам понадобятся некоторые напоминания и дополнительные обозначения.

Выберем максимальный K-определенный тор $T \subset G$, содержащий максимальный K-разложимый тор S. Пусть $R = R(T, G)$ — соответствующая система корней, $\Pi \subset R$ — подсистема простых корней, которая (однозначно) определяется заданием подгруппы Бореля $B \subset G$, содержащей тор T и содержащейся в некоторой минимальной параболической K-подгруппе. Обозначим через Π_0 подмножество в Π, состоящее из корней с тривиальным ограничением на S; тогда $\Pi \setminus \Pi_0$ — это в точности множество выделенных вершин в индексе Титса группы G. В § 2.1, п. 14 мы определили естественное действие группы Галуа $\mathcal{G} = \mathrm{Gal}(\bar{K}/K)$ на Π (так называемое $*$-действие). Тогда оказывается, что относительно этого действия множества Π_0 и $\Pi \setminus \Pi_0$ инвариантны, причем число $\mathcal{G}$-орбит на $\Pi \setminus \Pi_0$ совпадает с K-рангом G. Для произвольного подмножества $\Theta \subset \Pi$ положим $T(\Theta) = \bigcap_{\theta \in \Theta} (\mathrm{Ker}\, \theta)^0$, $H(\Theta) = Z_G(T(\Theta))$ и обозначим через $G(\Theta)$ коммутант группы $H(\Theta)$ (в частности, $H = H(\Pi_0)$ — централизатор максимального K-разложимого тора и $G_0 = G(\Pi_0)$ — анизотропное ядро группы G). Мы будем в основном работать с $\mathcal{G}$-инвариантными подмножествами Θ, содержащими Π_0. Тогда соответствующая группа $G(\Theta)$ является односвязной полупростой (но не обязательно простой) K-группой, причем ее K-простые компоненты легко найти, пользуясь индексом Титса: они соответствуют орбитам группы $\mathcal{G}$ на множестве связных компонент поддиаграммы в Π, в которой оставлены лишь вершины из Θ и соответствующие связи (пример: если индекс имеет вид



и $\Theta = \Pi_0$, то $G(\Theta)$ имеет две K-простые компоненты



одна из которых имеет тип A_1, а другая получается из группы типа A_1 путем ограничения поля с квадратичного расширения K). Пусть $\Theta_1, \ldots, \Theta_r$ — все $\mathcal{G}$-орбиты на множестве $\Pi \setminus \Pi_0$. Тогда K-ранг группы $G(\Theta_i \cup \Pi_0)$ равен 1, и, следовательно, она обладает единственным K-простым K-изотропным сомножителем G_i. В этих обозначениях справедлива

Теорема 4 (Прасад, Рагунатан [3]). *Предположим, что* $\operatorname{rang}_K G \geqslant 2$. *Тогда группа H_K порождается группами H_{i_K}, где $H_i = H \cap G_i$. В частности, если гипотеза Кнезера — Титса справедлива для всех G_i, то она справедлива и для G.*

Доказательство получается редукцией к следующему когомологическому утверждению, которое представляет независимый интерес.

Теорема 5. *Пусть $\Pi_1, \ldots, \Pi_d$ — такие $\mathcal{G}$-инвариантные подмножества в $\Pi \setminus \Pi_0$, что $\bigcap_{i=1}^{d} \Pi_i = \varnothing$. Тогда естественное отображение*

$$H^1(K, G_0) \to \prod_{i=1}^{d} H^1(K, G(\Pi_i \cup \Pi_0))$$

имеет тривиальное ядро.

Доказательство теоремы 5, которое мы опускаем, отсылая читателя к работе Прасада, Рагунатана [3], становится тривиальным в основном интересующем нас случае неархимедовых локальных полей, ибо здесь $H^1(K, G_0) = 1$ (теорема 6.4).

Доказательство теоремы 4. Обозначим через Π_i дополнение к Θ_i в $\Pi \setminus \Pi_0$ и положим $C_i = H(\Pi_i \cup \Pi_0)$, $D_i = G(\Pi_i \cup \Pi_0)$. Отметим, что $H \subset C_i$, $G_0 \subset D_i$ для любого $i = 1, \ldots, r$.

Лемма 1. *Каноническое отображение*

$$H/G_0 \to \prod_{i=1}^{r} C_i/D_i$$

является изоморфизмом.

Доказательство. Положим $T_\alpha = T \cap G_\alpha$, где G_α — соответствующая корневая подгруппа, совпадающая в наших обозначениях с $G(\{\alpha\})$. Хорошо известно (см. Стейнберг [2]), что $T = \prod_{\alpha \in \Pi} T_\alpha$, и, следовательно, для любого подмножества $\Theta \subset \Pi$ подгруппа T_Θ, порожденная T_α для $\alpha \in \Theta$, совпадает с прямым

произведением $\prod_{\alpha\in\Theta} T_\alpha$. Легко видеть, что $T_\Theta \subset G(\Theta)$. Но

$$\operatorname{rang} G(\Theta) = \dim T - \dim Z(H(\Theta)) \leqslant$$
$$\leqslant \dim T - \dim T(\Theta) = \dim T_\Theta, \qquad (1)$$

так что T_Θ является в действительности максимальным тором в $G(\Theta)$ и $T \cap G(\Theta) = T(\Theta)$. Отсюда получаем также, что неравенство в (1) на самом деле является равенством, и, следовательно, $Z(H(\Theta))^0 \subset T(\Theta) \subset T$. Так как $H(\Theta) = G(\Theta)\, Z(H(\Theta))^0$, то $H(\Theta) = G(\Theta)\, T$. Но $T = T_\Theta \times T_{\Pi\setminus\Theta}$ и $T_\Theta \subset G(\Theta)$, поэтому $H(\Theta) = G(\Theta)\, T_{\Pi\setminus\Theta}$. С другой стороны,

$$T_{\Pi\setminus\Theta} \cap G(\Theta) = T_{\Pi\setminus\Theta} \cap (T \cap G(\Theta)) = T_{\Pi\setminus\Theta} \cap T_\Theta = 1,$$

так что в действительности $H(\Theta)$ является полупрямым произведением $G(\Theta)$ и $T_{\Pi\setminus\Theta}$. Отсюда следует, что в коммутативной диаграмме

$$\begin{array}{ccc} H/G_0 & \xrightarrow{\alpha} & \prod_{i=1}^{r} C_i/D_i \\ \uparrow & & \uparrow \\ T(\Pi\setminus\Pi_0) & \to & \prod_{i=1}^{r} T(\Theta_i), \end{array}$$

индуцированной соответствующими вложениями, все стрелки, кроме α, являются изоморфизмами. Поэтому α — также изоморфизм. Лемма 1 доказана.

Коммутативная диаграмма

$$\begin{array}{ccccccccc} 1 & \to & G_0 & \longrightarrow & H & \dashrightarrow & H/G_0 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & \prod_{i=1}^{r} D_i & \to & \prod_{i=1}^{r} C_i & \to & \prod_{i=1}^{r} (C_i/D_i) & \to & 1 \end{array}$$

индуцирует следующую коммутативную диаграмму когомологий Галуа с точными строками:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_{0_K} & \longrightarrow & H_K & \longrightarrow & (H/G_0)_K & \longrightarrow & H^1(K,\ G_0) \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow\beta \\ 1 & \to & \prod_{i=1}^{r} D_{i_K} & \to & \prod_{i=1}^{r} C_{i_K} & \to & \prod_{i=1}^{r} (C_i/D_i)_K & \to & \prod_{i=1}^{r} H^1(K,\ D_i) \end{array}$$

Так как $D_i = G(\Pi_i \cup \Pi_0)$ и $\bigcap_{i=1}^{r} \Pi_i = \varnothing$, то из теоремы 5 получаем, что β имеет тривиальное ядро. Поэтому естественный

гомоморфизм

$$H_K/G_{0_K} \to \prod_{i=1}^{r} C_{i_K}/D_{i_K}$$

является изоморфизмом. Отсюда следует, что группа H_K порождается подгруппами

$$F_i = H_K \cap \left(\bigcap_{j \neq i} D_{j_K}\right) = (H \cap G(\Theta_i \cup \Pi_0))_K.$$

Имеем $H \cap G(\Theta_i \cup \Pi_0) = A_i \times H_i$, где A_i — произведение K-анизотропных множителей группы $G(\Theta_i \cup \Pi_0)$, так что $F_i = A_{i_K} H_{i_K}$. Остается заметить, что для любого i $A_i \subset G_0$, а в силу связности индекса Титса группы G каждая компонента G_0 лежит в подходящей группе G_j, следовательно, и в H_j. Теорема 4 полностью доказана.

Теперь уже несложно завершить доказательство основного результата этого параграфа.

Теорема 6 (Платонов [4]). *Пусть K — неархимедово локально компактное поле. Тогда для любой простой односвязной K-изотропной группы G выполняется гипотеза Кнезера — Титса, т. е. $G_K^+ = G_K$.*

Доказательство. Так как группы типов ${}^3D_4$ и ${}^6D_4$ являются квазиразложимыми (см. предложение 6.15) и, следовательно, в специальном рассмотрении не нуждаются, то принимая во внимание предложение 7 и теорему 4, мы видим, что достаточно установить отсутствие исключительных групп K-ранга 1. Воспользуемся предложениями 6.15 и 6.16. Тогда все группы типов E_8, F_4, G_2 разложимы над K, так что их можно не рассматривать. Любая группа типа E_7 разложима над квадратичным расширением поля K, и значит, аналогичным свойством обладает ее анизотропное ядро. С другой стороны, как следует из теоремы 6.5, анизотропное ядро является произведением групп, которые являются внутренними формами типа A_n. Поэтому анизотропное ядро должно иметь тип $A_1 + \ldots + A_1$. Но диаграмму такого типа невозможно получить из диаграммы типа E_7, выбросив одну вершину, так что K-ранг исходной группы типа E_7 необходимо больше 1. Аналогичное рассуждение применимо к внутренним формам типа E_6. Эти формы разложимы над расширением K третьей степени, откуда вытекает, что анизотропное ядро должно иметь тип $A_2 + \ldots + A_2$. Но чтобы получить диаграмму такого типа, из E_6 необходимо выбросить, как минимум, две вершины. Любая внешняя форма типа ${}^2E_6$ квазиразложима над K и ее ранг равен 4. Доказательство теоремы 6 завершено.

Таким образом, имеется значительное число результатов, подтверждающих гипотезу Кнезера — Титса для различных

групп G и классов полей K. Эти результаты способствовали формированию мнения, что и в общем случае ответ на эту гипотезу должен быть утвердительным. Однако в 1975 г. первым из авторов был получен отрицательный ответ. А именно, вначале в работе [13] были построены первые примеры тел D над полем рациональных функций $\mathbb{Q}(x, y)$, для которых $SK_1(D) \neq 1$, а затем в серии работ [14]—[16] была развита приведенная K-теория для вычисления группы $SK_1(D)$. Оказалось, что группа $SK_1(D)$ может быть любой конечной и даже бесконечной абелевой группой конечного периода для подходящих тела D и поля K. После выхода работ [13]—[16] исследования по приведенной K-теории стали интенсивно проводиться рядом других авторов (см. Дракел, Кнезер [1]). Полученные в этих последующих работах результаты представляют некоторое обобщение и детализацию первоначальных теорем. Обзор основных результатов приведенной K-теории содержится в докладе Платонова [17] на Международном математическом конгрессе в Хельсинки, докладе Титса [4] на семинаре Бурбаки и трудах семинара Дракела — Кнезера [1].

Аналогичные результаты были получены и для приведенной унитарной группы Уайтхеда. А именно, в работе Платонова, Янчевского [3] показано, что группа $SUK_1(D)$ может быть нетривиальной, а затем Янчевским в [2] была развита приведенная унитарная K-теория, являющаяся аналогом приведенной K-теории в унитарной ситуации и позволяющая во многих случаях вычислить группу $SUK_1(D)$.

В заключение отметим, что недавно были построены примеры односвязных K-изотропных групп G типа D_n, для которых $G_K^+ \neq G_K$ (см. Монастырный, Янчевский [1]). Таким образом, для групп классических типов в отношении гипотезы Кнезера — Титса имеется вполне завершенная картина. Рассмотрение некоторых исключительных типов содержится в докладе Титса [4].

§ 7.3. Слабая аппроксимация в алгебраических группах

В этом параграфе мы покажем, что для связной алгебраической группы G слабая аппроксимация «почти всегда» имеет место. А именно, справедлива

Теорема 7. *Пусть G — связная алгебраическая группа, определенная над полем алгебраических чисел K. Тогда существует такое конечное подмножество $S_0 \subset V_f^K$, что группа G обладает слабой аппроксимацией относительно $V^K \setminus S_0$. В частности, G всегда обладает слабой аппроксимацией относительно $S = V_\infty^K$.*

Как показывают примеры, в общем случае нельзя положить $S_0 = \varnothing$, даже если группа G полупроста. Однако в «крайних»

случаях односвязной и присоединенных групп слабая аппроксимация всегда имеет место.

Теорема 8. *Пусть G — полупростая группа над числовым полем K, являющаяся либо односвязной, либо присоединенной. Тогда G обладает слабой аппроксимацией.*

Доказательство этих фактов использует теорию приведения, справедливость гипотезы Кнезера — Титса для локальных полей, принцип Хассе для односвязных групп и одно достаточное условие наличия слабой аппроксимации в алгебраических торах, впервые отмеченное Ж.-П. Серром (неопубликовано).

Предложение 8. *Пусть T — алгебраический K-тор, разложимый над расширением Галуа L/K, $\mathcal{G} = \mathrm{Gal}(L/K)$ и $S \subset V^K$ — конечное подмножество. Предположим, что для каждого $v \in S$ выполнено следующее условие:*

$$\text{существует } v' \notin S, \text{ для которого группы разложения } \mathcal{G}(w) \text{ и } \mathcal{G}(w') \text{ подходящих продолжений } w|v \text{ и } w'|v' \text{ совпадают.} \tag{1}$$

Тогда T обладает слабой аппроксимацией относительно S. Условие (1) автоматически выполняется, если для $w|v$ локальная группа Галуа $\mathrm{Gal}(L_w/K_v)$ циклическая.

Доказательство. Положим $H = \mathbf{R}_{L/K}(T)$ и обозначим через φ: $H \to T$ — «норменное» отображение (см. доказательство предложения 6.7). Легко видеть, что ядро $N = \mathrm{Ker}\,\varphi$ также является K-определенным алгебраическим тором. Имеем $H^1(K, H) = H^1(L, T) = 1$, ибо тор T является L-разложимым. Аналогично устанавливается, что $H^1(K_v, H) = 1$ для любого $v \in V^K$. Точная последовательность

$$1 \to N \to H \xrightarrow{\varphi} T \to 1 \tag{2}$$

для любого конечного $S \subset V^K$ индуцирует следующую коммутативную диаграмму когомологий Галуа с точными строками:

$$\begin{tikzcd}
H_K \arrow[r, "\varphi"] \arrow[d, "\alpha"] & T_K \arrow[r] \arrow[d, "\beta"] & H^1(K, N) \arrow[r] \arrow[d, "\gamma"] & 1 \\
H_S \arrow[r, "\Phi"] & T_S \arrow[r] & \prod\limits_{v \in S} H^1(K_v, N) \arrow[r] & 1,
\end{tikzcd}$$

в которой α, β являются диагональными вложениями, γ есть произведение отображений ограничения $H^1(K, N) \to H^1(K_v, N)$, а Φ индуцировано φ. Поскольку T разложим над L, то

$$H_K \simeq T_L \simeq L^{*d}, \quad H_S \simeq T_{\bar{S}} \simeq \prod_{w \in \bar{S}} L_w^{*d},$$

где $d = \dim T$, $\bar{S}$ — совокупность всех продолжений на L нормирований из S, так что из слабой аппроксимации для поля L

вытекает, что вложение α является плотным. Отсюда следует, что $\beta(\varphi(H_K))$ плотно в $\Phi(H_S)$, и, учитывая открытость $\Phi(H_S)$ в T_S (см. следствие 1 из предложения 3.3), получаем, что слабая аппроксимация для T относительно S равносильна равенству

$$T_S = \beta(T_K)\,\Phi(H_S).$$

Последнее, как легко видеть, в точности эквивалентно сюръективности γ. Для вычисления образа γ рассмотрим точную последовательность

$$1 \to N_L \to N_{A_L} \to C_L(N) \to 1,$$

где N_{A_L} — группа аделей тора N над L, $C_L(N) = N_{A_L}/N_L$ — соответствующая группа классов аделей. Переходя к когомологиям, получим точную последовательность

$$H^1(L/K,\ N_L) \to H^1(L/K,\ N_{A_L}) \xrightarrow{\delta} H^1(L/K,\ C_L(N)).$$

Далее, представим N_{A_L} в виде $N_{A_L} = N_{\overline{S}} \times N_{(A_L)_{\overline{S}}}$ и заметим, что

$$H^1(L/K,\ N_{\overline{S}}) = \prod_{v\in S} H^1\Big(L/K,\ \prod_{w|v} N_{L_w}\Big) = \prod_{v\in S} H^1(L_w/K_v,\ N).$$

Поэтому в смысле этих отождествлений

$$\operatorname{Im}\gamma = \{x \in H^1(L/K,\ N_{\overline{S}}) \mid \exists y \in H^1\big(L/K,\ N_{(A_L)_{\overline{S}}}\big),\ \delta(x+y) = 0\}.$$

Отсюда следует, что γ сюръективно в том и только том случае, когда

$$\delta(H^1(L/K,\ N_{\overline{S}})) \subset \delta\big(H^1\big(L/K,\ N_{(A_L)_{\overline{S}}}\big)\big). \tag{3}$$

Воспользуемся теперь теоремами Накаямы — Тейта (см. § 6.3), из которых вытекает существование естественных изоморфизмов

$$H^1(L_w/K_v,\ N) \simeq \widehat{H}^{-1}(L_w/K_v,\ \mathbf{X}_*(N)),$$
$$H^1(L/K,\ C_L(N)) \simeq \widehat{H}^{-1}(L/K,\ \mathbf{X}_*(N)),$$

где $\mathbf{X}_*(N)$ — группа кохарактеров тора N. При этом, как показывает предложение 6.8, сквозное отображение

$$\widehat{H}^{-1}(L_w/K_v,\ \mathbf{X}_*(N)) \simeq \widehat{H}^1(L_w/K_v,\ N) = H^1\Big(L/K,\ \prod_{w|v} N_{L_w}\Big) \to$$
$$\to H^1(L/K,\ C_L(N)) \simeq \widehat{H}^{-1}(L/K,\ \mathbf{X}_*(N)),$$

индуцированное композицией $\prod_{w|v} N_{L_w} \to N_{A_L} \to C_L(N)$, совпадает с гомоморфизмом коограничения $\mathrm{Cor}^{\mathcal{G}}_{\mathcal{G}(w)}$, который мы обозначим через $\rho(w)$. Принимая во внимание описание когомологий групп аделей (см. предложение 6.6), получаем, что включение

(3) эквивалентно следующему:

$$\sum_{v\in S} \operatorname{Im}\rho(w) \subset \sum_{v\notin S} \operatorname{Im}\rho(w) \tag{4}$$

(для каждого v выбирается одно продолжение $w|v$). Если теперь выполняется условие (1), то для каждого $v\in S$ найдутся $v'\notin S$ и такие продолжения $w|v$ и $w'|v'$, что $\operatorname{Im}\rho(w)=\operatorname{Im}\rho(w')$, и тогда, очевидно, (4) выполняется. Следовательно, T обладает слабой аппроксимацией относительно S. Остается заметить, что если группа $\mathcal{G}(w)=\operatorname{Gal}(L_w/K_v)$ циклическая, скажем, $\mathcal{G}(w)=\langle\sigma\rangle$, то в соответствии с теоремой плотности Чеботарева существует бесконечно много таких $v'\in V_f^K$, что расширение $L_{w'}/K_{v'}$ неразветвлено и автоморфизм Фробениуса $\operatorname{Fr}(L_{w'}/K_{v'})=\sigma$; в частности, v' с указанным свойством можно выбрать вне S. Тогда $\mathcal{G}(w')=\langle\sigma\rangle=\mathcal{G}(w)$. Предложение 8 полностью доказано. (Отметим, что другое доказательство предложения 8 можно найти у Воскресенского [3], см. теорему 3.36.)

Следствие 1. *Пусть T — K-определенный тор. Тогда существует такое конечное подмножество $S_0\subset V_f^K$, что T обладает слабой аппроксимацией относительно $V^K\setminus S_0$.*

Действительно, пусть L — поле разложения тора T. Возьмем в качестве S_0 множество тех нормирований $v\in V_f^K$, которые разветвлены в L; конечность множества S_0 хорошо известна. Тогда любое нормирование $v\in V^K\setminus S_0$ либо архимедово, либо неразветвлено в L; и в том и в другом случае локальное расширение L_w/K_v $(w|v)$ является циклическим. Поэтому из предложения 8 вытекает, что T обладает слабой аппроксимацией относительно любого конечного подмножества $S\subset V^K\setminus S_0$, а следовательно, и относительно всего множества $V^K\setminus S_0$ (см. предложение 1).

Следствие 2. *Пусть F — диагонализируемая K-группа. Для $v\in V^K$ обозначим через $\mathcal{G}(F,v)$ ядро действия группы Галуа $\mathcal{G}(v)=\operatorname{Gal}(\bar K_v/K_v)$ на группе характеров $\mathbf{X}(F)$ и пусть S_0 — множество таких неархимедовых v, что факторгруппа $\mathcal{G}(v)/\mathcal{G}(F,v)$ не является циклической. Тогда S_0 — конечное множество, и для любого конечного подмножества $S\subset V^K\setminus S_0$ естественное отображение $H^1(K,F)\to\prod_{v\in S}H^1(K_v,F)$ сюръективно. В частности, отображение $H^1(K,F)\to\prod_{v\in V_\infty^K}H^1(K_v,F)$ всегда сюръективно.*

Доказательство. Обозначим через $\mathcal{G}(F)$ ядро естественного действия группы Галуа $\mathcal{G}=\operatorname{Gal}(\bar K/K)$ на группе характеров $\mathbf{X}(F)$, и пусть P — отвечающее $\mathcal{G}(F)$ неподвижное поле. Тогда P является минимальным полем разложения для F; в частности, расширение P/K конечно. Ясно, что факторгруппа $\mathcal{G}/\mathcal{G}(F)$

совпадает с группой Галуа $\mathrm{Gal}(P/K)$, а факторгруппа $\mathcal{G}(v)/\mathcal{G}(F, v)$ для $v \in V^K$ — с группой Галуа $\mathrm{Gal}(P_w/K_v)$ соответствующего локального расширения. С учетом этих замечаний рассуждения, использованные при доказательстве следствия 1, позволяют установить конечность S_0. Воспользуемся теперь предложением 2.1 и включим F в точную последовательность

$$1 \to F \to T_1 \to T_2 \to 1, \tag{5}$$

где T_1 и T_2 — торы, разложимые над P, причем тор T_1 квазиразложим над K. Тогда для любого расширения L поля K $H^1(L, T_1) = 1$, так что точная последовательность (5) для любого конечного $S \subset V^K$ индуцирует следующую коммутативную диаграмму с точными строками:

$$\begin{tikzcd} T_{1K} \arrow[r, "\alpha"] \arrow[d] & T_{2K} \arrow[r, "\beta"] \arrow[d] & H^1(K, F) \arrow[r] \arrow[d, "\chi"] & 1 \\ T_{1S} \arrow[r, "\theta"] & T_{2S} \arrow[r, "\varphi"] & \prod\limits_{v \in S} H^1(K_v, F) \arrow[r] & 1 \end{tikzcd} \tag{6}$$

Если теперь предположить, что $S \subset V^K \setminus S_0$, то из предложения 8 вытекает, что для T_2 имеет место слабая аппроксимация относительно S. В частности, учитывая открытость $\theta(T_{1S})$ в T_{2S}, получаем, что

$$T_{2S} = \rho(T_{2K})\theta(T_{1S}).$$

Для доказательства сюръективности χ теперь остается применить φ к обеим частям этого равенства и воспользоваться коммутативностью (6).

Разобрав случай алгебраических торов, мы начнем последовательно продвигаться в направлении доказательства теорем 7 и 8. Первый этап заключается в доказательстве теоремы 8 для односвязных групп.

Предложение 9. *Пусть G — полупростая односвязная K-группа. Тогда G обладает слабой аппроксимацией относительно любого конечного подмножества $S \subset V^K$.*

Доказательство с помощью предложений 1, 2 легко сводится к случаю простой односвязной K-группы G. Как мы отмечали в § 2.4, п. 3, многообразие G унирационально над K, т. е. существует доминантный K-определенный морфизм $f\colon U \to G$, где U — открытое подмножество подходящего аффинного пространства $\mathbb{A}^d$. Из предложения 3.3 вытекает, что $f(U_S)$ содержит открытое в G_S подмножество. Но в силу утверждения 4) предложения 2 U обладает слабой аппроксимацией, так что замыкание $\overline{G}_K$ группы G_K в G_S содержит $\overline{f(U_K)} \supset f(\overline{U}_K) = f(U_S)$ и поэтому является открытой подгруппой. С другой стороны, в силу теоремы 5.5

факторпространство G_A/G_K имеет конечный объем, так что, представляя G_A в виде $G_A = G_S \times G_{A_S}$ и используя лемму 3.17, получаем, что факторпространство $G_S/\bar{G}_K$ также имеет конечный объем. Отсюда следует, что индекс $[G_S : \bar{G}_K]$ обязан быть конечным (отметим, что при доказательстве этого факта мы не использовали ни односвязность, ни простоту, так что он сохраняет силу для любой полупростой K-группы). Пусть теперь G является односвязной простой K-группой типа, отличного от A_n. Тогда для всех неархимедовых v группа G является K_v-изотропной (теорема 6.5), и поэтому из предложения 6 и теоремы 6 вытекает, что для любого $v \in V^K$ группа G_{K_v} не имеет собственных нецентральных нормальных делителей. Отсюда следует, что группа G_S не имеет собственных подгрупп конечного индекса, и, значит, $G_S = \bar{G}_K$. Случай групп типа A_n требует специального рассмотрения.

Лемма 2. *Пусть G — односвязная простая K-группа типа A_n. Тогда G обладает свойством слабой аппроксимации относительно любого конечного S.*

Доказательство. Здесь имеется две возможности: $G = \boldsymbol{SL}_m(D)$ или $G = \boldsymbol{SU}_m(f)$, где f — невырожденная m-мерная эрмитова форма над телом D с инволюцией τ второго рода, причем поле неподвижных относительно τ элементов центра D совпадает с K. Положим тогда соответственно $H = \boldsymbol{GL}_m(D)$ или $H = \boldsymbol{U}_m(f)$. Утверждается, что $G_{K_v} = [H_{K_v}, H_{K_v}]$ для любого $v \in V^K$. Если G изотропна над K_v или $v \in V^K_\infty$, то это вытекает из теоремы 6 и предложения 6. В противном случае $G_{K_v} \simeq \boldsymbol{SL}_1(A)$, $H_{K_v} \simeq \boldsymbol{GL}_1(A)$, где A — алгебра с делением над K_v, и требуемое в точности эквивалентно тривиальности $SK_1(A)$ (см. § 1.4, п. 3). Так как рациональность многообразия $\boldsymbol{GL}_m(D)$ очевидна, а рациональность многообразия $\boldsymbol{U}_m(f)$ вытекает из предложения 4, то многообразие H всегда рационально над K. Поэтому из предложения 3 вытекает, что H обладает слабой аппроксимацией, т. е. $\bar{H}_K = H_S$. Тогда $[H_K, H_K]$ плотно в $[H_S, H_S] = G_S$, и, следовательно, $G_S = \overline{[H_K, H_K]} \subset \bar{G}_K$. Доказательство леммы 2 и предложения 9 завершено.

Установим теперь когомологический критерий слабой аппроксимации в произвольной полупростой группе G, принадлежащий Кнезеру [5]. Как и следует ожидать после предложения 9, этот критерий формулируется в терминах соответствующей фундаментальной группы F, т. е. ядра универсального K-определенного накрытия π: $\tilde{G} \to G$. Имея, однако, в виду доказательство теоремы 7, мы сформулируем несколько более общее утверждение, относящееся к так называемым *специальным накрытиям* π: $\tilde{H} \to H$ произвольных редуктивных групп (см. § 2.2, п. 4), т. е. таким изогениям, что $\tilde{H}$ является прямым

произведением односвязной полупростой группы и квазиразложимого тора.

Предложение 10. *Пусть* $\pi\colon \tilde{H} \to H$ — *специальное* K-*определенное накрытие редуктивной группы* H, $\operatorname{Ker}\pi = F$. *Тогда группа* H *обладает слабой аппроксимацией относительно конечного подмножества* $S \subset V^K$, *содержащего* V^K_∞ *в том и только том случае, если каноническое отображение* $H^1(K, F) \to \prod_{v\in S} H^1(K_v, F)$ *сюръективно.*

Доказательство. Имеем следующую диаграмму традиционного для нас вида:

$$\begin{tikzcd}
\tilde{H}_K \arrow[r, "\pi"] \arrow[d, "\alpha"] & H_K \arrow[r, "\psi"] \arrow[d, "\beta"] & H^1(K, F) \arrow[r, "\theta"] \arrow[d, "\gamma"] & H^1(K, \tilde{H}) \arrow[d, "\delta"] \\
\tilde{H}_S \arrow[r, "\Pi"] & H_S \arrow[r, "\Psi"] & \prod_{v\in S} H^1(K_v, F) \arrow[r, "\Theta"] & \prod_{v\in S} H^1(K_v, \tilde{H})
\end{tikzcd} \tag{7}$$

Так как $\tilde{H} = D \times T$, где D — односвязная полупростая K-группа, а T — квазиразложимый тор, то из предложения 9 и утверждения 4) предложения 2 вытекает, что α является плотным вложением. Отсюда следует, что слабая аппроксимация для H равносильна равенству $H_S = \beta(H_K)\Pi(\tilde{H}_S)$, что в свою очередь сводится к сюръективности индуцированного отображения γ': $\operatorname{Ker}\theta \to \operatorname{Ker}\Theta$. Заметим теперь, что для любого расширения P/K имеем $H^1(P, \tilde{H}) = H^1(P, D)$. Поэтому из теорем 6.4 и 6.6 вытекает, что $H^1(K_v, \tilde{H}) = 1$ для неархимедовых v, и отображение $H^1(K, \tilde{H}) \to \prod_{v\in V^K_\infty} H^1(K_v, \tilde{H})$ биективно. В частности, поскольку $S \supset V^K_\infty$, то δ инъективно. Отсюда без труда следует, что если γ сюръективно, γ' также сюръективно, и, значит, группа H обладает слабой аппроксимацией относительно S. Обратно, слабая аппроксимация для H влечет сюръективность γ'. Но тогда

$$\prod_{v\in V^K_\infty} \{0\} \times \prod_{v\in S\setminus V^K_\infty} H^1(K_v, F) \subset \operatorname{Ker}\Theta = \operatorname{Im}\gamma' \subset \operatorname{Im}\gamma.$$

Так как отображение $H^1(K, F) \to \prod_{v\in V^K_\infty} H^1(K_v, F)$ всегда сюръективно (следствие 2 из предложения 8), то отсюда получается сюръективность γ. Предложение 10 доказано.

Теперь уже легко доказать теорему 7. Если группа G полупроста, то ее универсальное накрытие $\pi\colon \tilde{G} \to G$ является специальным, и требуемое утверждение непосредственно вытекает из предложения 9 и из следствия 2 предложения 8. Случай произвольной связной группы легко сводится к редуктивному (см. следствие из предложения 1). К сожалению, не любая редук-

тивная группа G обладает специальным накрытием, и непосредственно воспользоваться предложением 10 нельзя. Однако согласно предложению 2.11 найдется такое целое $m > 0$ и такой квазиразложимый тор T, что группа $H = G^m \times T$ обладает специальным накрытием π: $\tilde{H} \to H$. Применяя тогда предложение 10 и следствие 2 из предложения 8, получаем существование конечного исключительного подмножества $S_0 \subset V_f^K$ для H. Однако из утверждения 2) предложения 1 вытекает, что это же множество годится и для G. Тем самым доказательство теоремы 7 завершено.

В действительности доказательство теоремы 7 позволяет получить дополнительную информацию о слабой аппроксимации в редуктивной группе G. Для этого вернемся к специальному накрытию π: $\tilde{H} \to H$ группы $H = G^m \times T$ и соответствующей диаграмме (7). Из слабой аппроксимации для $\tilde{H}$ вытекает, что замыкание $\overline{H}_K$ в H_S содержит $\pi(\overline{H}_S) \supset [H_S, H_S]$ и поэтому является нормальным делителем в H_S. При этом имеет место следующая оценка для индекса:

$$[H_S : \overline{H}_K] \leqslant [\operatorname{Coker} \gamma] \leqslant \sum_{v \in S_0} [H^1(K_v, F)],$$

где S_0 — исключительное подмножество, введенное в следствии 2 предложения 8, т. е. индекс $[H_S : \overline{H}_K]$ ограничен числом, не зависящим от S. Отсюда следует, что замыкание $\overline{H}_K$ в полном прямом произведении $\underline{H} = \prod_v H_{K_v}$ также является нормальным делителем, а (абелева) группа $A(H) = \underline{H}/\overline{H}_K$, измеряющая отклонение от слабой аппроксимации, конечна. Используя каноническую проекцию $H \to G$, легко показать, что это утверждение сохраняет силу для произвольной редуктивной группы G. Переход к произвольным связным группам не представляет труда (см. следствие из предложения 1). Таким образом, получается

Теорема 9. *Для произвольной связной K-группы G замыкание $\overline{G}_K$ группы G_K в полном прямом произведении $\underline{G} = \prod_{v \in V^K} G_{K_v}$ является нормальным делителем, причем соответствующая факторгруппа $A(G) = \underline{G}/\overline{G}_K$, измеряющая отклонение от слабой аппроксимации, является конечной абелевой группой.*

Нам осталось завершить доказательство теоремы 8. Для этого мы сначала приведем два следствия, которые представляют также и самостоятельный интерес.

Следствие 3. *Пусть G — полупростая K-группа, фундаментальная группа F которой имеет циклическую группу автоморфизмов. Тогда G обладает слабой аппроксимацией.*

Действительно, для любого $v \in V^K$ в обозначениях следствия 2 факторгруппа $\mathcal{G}(v)/\mathcal{G}(F, v)$ вкладывается в $\operatorname{Aut} \mathbf{X}(F) \simeq \simeq \operatorname{Aut} F$ и поэтому является циклической. Тогда для любого конечного подмножества $S \subset V^K$ отображение $H^1(K, F) \to \to \prod_{v \in S} H^1(K_v, F)$ сюръективно, так что группа G обладает слабой аппроксимацией относительно любого S.

Следствие 4. *Пусть G — полупростая K-группа, $S \subset V^K$ — конечное подмножество. Предположим, что для любого $v \in S$ группа G обладает максимальным K_v-определенным тором, который разложим над циклическим расширением поля K_v (в частности, G разложима над K_v). Тогда G обладает слабой аппроксимацией относительно S.*

Доказательство. Без ограничения общности можно считать, что $S \supset V_\infty^K$, так что, как и выше, достаточно показать, что для любого $v \in S$ факторгруппа $\mathcal{G}(v)/\mathcal{G}(F, v)$ является циклической. Пусть $T \subset G$ — максимальный K_v-определенный тор, поле минимального разложения L которого циклично над K_v. Тогда факторгруппа $\mathcal{G}(v)/\mathcal{G}(T, v)$, где $\mathcal{G}(T, v)$ — ядро действия $\mathcal{G}(v)$ на группе характеров $\mathbf{X}(T)$, изоморфна $\operatorname{Gal}(L/K_v)$ и следовательно, циклична. С другой стороны, из включения $F \subset T$ вытекает, что $\mathcal{G}(T, v) \subset \mathcal{G}(F, v)$, и поэтому факторгруппа $\mathcal{G}(v)/\mathcal{G}(T, v)$ также циклична.

Предложение 11. *Простая K-определенная группа G обладает слабой аппроксимацией.*

Доказательство. Группы типов E_8, F_4, G_2 односвязны, и поэтому для них слабая аппроксимация вытекает из предложения 9. Центр односвязной группы, относящийся к одному из типов B_n, C_n, E_6, E_7, имеет порядок, не превосходящий 3, поэтому для любой возникающей здесь фундаментальной группы F группа $\operatorname{Aut} F$ циклична, и можно воспользоваться следствием 3. Центр односвязной группы типа D_{2n+1} изоморфен $\mathbb{Z}/4\mathbb{Z}$, так что опять группа $\operatorname{Aut} F$ циклична. Нам осталось рассмотреть типы D_{2n} и A_n. Для группы G типа A_n можно воспользоваться следствием 4, ибо для каждого $v \in V^K$ легко указывается K_v-определенный тор $T \subset G$, имеющий циклическое над K_v поле разложения. В самом деле, если $G \simeq \boldsymbol{SL}_m(D)$ над K_v, то искомым будет тор вида $T = (\mathbf{R}_{L/K}(\boldsymbol{G}_m) \times \ldots \times \mathbf{R}_{L/K}(\boldsymbol{G}_m)) \cap \boldsymbol{SL}_m(D)$, где $L \subset D$ — максимальное подполе, являющееся циклическим расширением K. Отметим, что такое L всегда существует. Это очевидно, если D является телом кватернионов над полем $K_v = \mathbb{R}$, в то время как для неархимедова v можно взять максимальное неразветвленное над K_v подполе $L \subset D$. Осталось рассмотреть случай, когда $G \simeq \boldsymbol{SU}_m(f)$ над K_v, где f — невырожденная m-мерная эрмитова форма над квадратичным расширением L/K_v. Но здесь группа G является L-разложимой и поэтому обладает

максимальным K_v-определенным тором $T \subset G$, который разложим над L (лемма 6.23). Остается рассмотреть лишь группы G типа D_{2n}. Здесь в специальном исследовании нуждается лишь случай, когда $F = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ и $\mathcal{G}/\mathcal{G}(F) = \operatorname{Aut} F = S_3$. Обозначим через P подполе в $L = \bar{K}^{\mathcal{G}(F)}$, имеющее степень 3 над K. Тогда сквозное отображение

$$H^1(K, F) \xrightarrow{\text{Res}} H^1(P, F) \xrightarrow{\text{Cor}} H^1(K, F)$$

совпадает с умножением на 3 и, следовательно, тождественно на $H^1(K, F)$, ибо экспонента F равна 2. В частности, отображение Cor сюръективно. Аналогично, для любого $v \in V^K$ сквозное отображение

$$H^1(K_v, F) \xrightarrow{\alpha_v} \prod_{w|v} H^1(P_w, F) \xrightarrow{\beta_v} H^1(K_v, F),$$

где α_v индуцировано соответствующими отображениями ограничения, а β_v — отображениями коограничения, также является умножением на 3, и, следовательно, β_v сюръективно. С другой стороны, поле L является циклическим расширением P и поэтому для любого конечного подмножества $\tilde{S} \subset V^P$ отображение $H^1(P, F) \to \prod_{w \in \tilde{S}} H^1(P_w, F)$ сюръективно. Тогда из коммутативной диаграммы

$$\begin{array}{ccc} H^1(P, F) & \to & \prod\limits_{\substack{w|v \\ v \in S}} H^1(P_w, F) \\ \Big\downarrow \text{Cor} & & \Big\downarrow \beta \\ H^1(K, F) & \xrightarrow{\gamma} & \prod\limits_{v \in S} H^1(K_v, F), \end{array}$$

где $\beta = \prod_{v \in S} \beta_v$, и из сюръективности β получаем сюръективность γ. Предложение 11 полностью доказано.

Так как любая присоединенная K-группа является прямым произведением своих K-простых компонент, которые получаются конструкцией ограничения основного поля из абсолютно простых групп, то тем самым предложение 11 завершает доказательство теоремы 8.

Все предыдущие результаты носили позитивный характер, в связи с чем может сложиться впечатление, что слабая аппроксимация имеет место всегда. Это, однако, не так, причем соответствующие примеры имеются как для полупростых групп, так и для алгебраических торов.

Примеры, которые мы здесь приведем, связаны с расширением L/K, где $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$, которое обладает следующим свойством: любое $p \neq 2$ неразветвлено в L/K, а $p = 2$ вполне разветвлено, причем локальная степень относительно

$p \neq 2$ (включая $p = \infty$) есть 1 или 2, а относительно $p = 2$ равна 4. Положим теперь $T = \mathbf{R}^{(1)}_{L/K}(\boldsymbol{G}_m)$ и покажем, что группа T_K не является плотной в T_{K_v}. Для этого покажем, что включение (4) из доказательства предложения 8, которое является необходимым и достаточным для слабой аппроксимации, здесь не выполняется. С этой целью построим для нашего случая точную последовательность

$$1 \to N \to H \xrightarrow{\varphi} T \to 1,$$

где $H = \mathbf{R}_{L/K}(T)$, φ — норменное отображение (см. доказательство предложения 8). Ей отвечает точная последовательность модулей кохарактеров

$$0 \to \mathbf{X}_*(N) \to \mathbf{X}_*(H) \to \mathbf{X}_*(T) \to 0.$$

Модуль $\mathbf{X}_*(H)$ имеет вид $\mathbf{X}_*(H) = \mathbf{X}_*(T) \otimes_{\mathbb{Z}} \mathbb{Z}[\mathcal{G}]$, где $\mathcal{G} = \mathrm{Gal}(L/K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, т. е. является индуцированным. Поэтому $\hat{H}^i(L/K, \mathbf{X}_*(H)) = 0$ для любого i, а из точной когомологической последовательности

$$0 = \hat{H}^{-2}(L/K, \mathbf{X}_*(H)) \to \hat{H}^{-2}(L/K, \mathbf{X}_*(T)) \to$$
$$\to \hat{H}^{-1}(L/K, \mathbf{X}_*(N)) \to \hat{H}^{-1}(L/K, \mathbf{X}_*(H)) = 0$$

получаем существование естественного изоморфизма

$$\hat{H}^{-1}(L/K, \mathbf{X}_*(N)) \simeq \hat{H}^{-2}(L/K, \mathbf{X}_*(T)).$$

В свою очередь, $\mathbf{X}_*(T)$ входит в точную последовательность

$$0 \to \mathbf{X}_*(T) \to \mathbb{Z}[\mathcal{G}] \to \mathbb{Z} \to 1,$$

отвечающую последовательности $1 \to T \to \mathbf{R}_{L/K}(\boldsymbol{G}_m) \to \boldsymbol{G}_m \to 1$, и, рассуждая аналогично, получим, что

$$\hat{H}^{-2}(L/K, \mathbf{X}_*(T)) \simeq \hat{H}^{-3}(L/K, \mathbb{Z}).$$

Проводя те же вычисления в локальном случае, мы придем к изоморфизму

$$\hat{H}^{-1}(L_w/K_v, \mathbf{X}_*(N)) \simeq \hat{H}^{-3}(L_w/K_v, \mathbb{Z}).$$

Тогда включение (4) сводится к такому:

$$\sum_{\substack{v \in S \\ w \mid v}} \mathrm{Cor}^{\mathcal{G}}_{\mathcal{G}(w)}(\hat{H}^{-3}(L_w/K_v, \mathbb{Z})) \subset \sum_{\substack{v \notin S \\ w \mid v}} \mathrm{Cor}^{\mathcal{G}}_{\mathcal{G}(w)}(\hat{H}^{-3}(L_w/K_v, \mathbb{Z})). \qquad (8)$$

В нашем случае $S = \{2\}$, $\mathcal{G}(2) = \mathcal{G}$, так что левая часть (8) есть $\hat{H}^{-3}(\mathcal{G}, \mathbb{Z}) \simeq H^3(\mathcal{G}, \mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$. С другой стороны, все локальные (группы Галуа в правой части (8) — циклические, так что $\hat{H}^{-3}(L_w/K_v, \mathbb{Z}) \simeq H^1(L_w/K_v, \mathbb{Z}) = 0$ и правая часть (8) тривиальна. Таким образом, включение (8) не выполняется, значит,

T_K не является плотной в T_{K_2}. (Отметим, что наши рассуждения в действительности показывают, что факторгруппа $T_{K_2}/\overline{T}_K$ изоморфна $\mathbb{Z}/2\mathbb{Z}$).

Используя конструкцию тора T, проведем теперь построение конечной диагонализируемой K-группы F, для которой отображение $H^1(K, F) \to H^1(K_2, F)$ не является сюръективным. Так как $\overline{T}_K \neq T_{K_2}$, то найдется такое целое $l > 0$, что $T_{K_2} \not\subset T_K \cdot L_2^{*l}$. Положим тогда $n = 4l$, $F = \mathbf{R}_{L/K}^{(1)}(\mu_n)$, где μ_n — модуль корней степени n из единицы (отметим, что F совпадает со множеством элементов порядка, делящего n в T).

Лемма 3. *Отображение $H^1(K, F) \xrightarrow{\chi} H^1(K_2, F)$ не является сюръективным.*

Доказательство. В силу леммы 2.6 имеют место следующие изоморфизмы:

$$H^1(K, \mu_n) \simeq K^*/K^{*n},$$
$$H^1(K, \mathbf{R}_{L/K}(\mu_n)) \simeq H^1(L, \mu_n) \simeq L^*/L^{*n},$$

так что $H^1(K, F)$ входит в точную последовательность

$$H^1(K, F) \to L^*/L^{*n} \xrightarrow{\alpha} K^*/K^{*n},$$

где α индуцировано норменным отображением $N_{L/K}$. В частности, $H^1(K, F)$ сюръективно отображается на $\operatorname{Ker}\alpha$. Аналогично, группа $H^1(K_2, F)$ сюръективно отображается на ядро отображения β: $L_2^*/L_2^{*n} \to K_2^*/K_2^{*n}$, индуцированного N_{L_2/K_2}. Поэтому если χ сюръективно, то естественное отображение $\operatorname{Ker}\alpha \xrightarrow{\gamma} \operatorname{Ker}\beta$ также сюръективно. Но легко видеть, что

$$\operatorname{Ker}\alpha = T_K K^{*l} L^{*n}/L^{*n},$$
$$\operatorname{Ker}\beta = T_{K_2} K_2^{*l} L_2^{*n}/L_2^{*n},$$

поэтому сюръективность γ, в частности, означает, что $T_{K_2} \subset \subset T_K K^{*l} L_2^{*n} \subset T_K L_2^{*l}$, — противоречие. Лемма 3 доказана.

Чтобы получить теперь пример полупростой группы G, которая не обладает слабой аппроксимацией, достаточно взять группу $H = \mathbf{R}_{L/K}(\boldsymbol{SL}_n)$ и, рассмотрев естественное вложение $F \subset \mathbf{R}_{L/K}(\mu_n) = Z(H)$, положить $G = H/F$. Тогда для $S = \{\infty, 2\}$ отображение $H^1(K, F) \to \prod_{v \in S} H^1(K_v, F)$ не является сюръективным, следовательно, G не обладает слабой аппроксимацией относительно S (и даже относительно множества $\{2\}$). Отметим, что первые примеры такого рода были построены Серром, см. [АТЧ], упр. 5.

В связи с результатами о слабой аппроксимации для односвязных групп и контрпримерами Серра возникла гипотеза о справедливости слабой аппроксимации для полупростых односвязных групп над произвольным бесконечным полем K (см. Кнезер [5]). В частности, Кнезер предположил в [5], что алгебраическая группа $G = \boldsymbol{SL}_n(D)$, где D — конечномерная центральная алгебра с делением над K, всегда обладает свойством слабой аппроксимации. Здесь имеет место

Предложение 12. *Пусть $G = \boldsymbol{SL}_n(D)$, v — дискретное нормирование поля K. Тогда имеют место следующие утверждения:*

1) *$\overline{G}_K$ — нормальная подгруппа в G_{K_v} (черта означает замыкание в v-адической топологии);*

2) *$G_{K_v}/\overline{G}_K \simeq SK_1(D \otimes_K K_v)/\varphi(SK_1(D))$, где φ индуцировано вложением $D \hookrightarrow D \otimes_K K_v$.*

Доказательство. Многообразие группы $H = \boldsymbol{GL}_n(D)$ рационально над K, и поэтому H_K плотно в H_{K_v} (доказательство то же, что и в числовом случае). Так как $[H_K, H_K] \subset G_K$, то замыкание $\overline{G}_K$ группы G_K содержит $\overline{[H_K, H_K]} \supset [H_{K_v}, H_{K_v}]$, откуда следует 1). Отметим, что последнее включение является на самом деле равенством, ибо группа $[H_{K_v}, H_{K_v}]$ содержит $[H_K, H_K]$ и, согласно замечанию после теоремы 3.3, является открытой, а следовательно, и замкнутой в G_{K_v}. Из этих фактов вытекает также, что замыкание $\overline{G}_K$ совпадает с $G_K[H_{K_v}, H_{K_v}]$, и поэтому

$$G_{K_v}/\overline{G}_K = G_{K_v}/G_K[H_{K_v}, H_{K_v}] \simeq SK_1(M_n(D \otimes_K K_v))/\psi(SK_1(M_n(D))),$$

где ψ индуцировано вложением $M_n(D) \hookrightarrow M_n(D \otimes_K K_v)$. Остается заметить, что определитель Дьедонне индуцирует изоморфизм

$$SK_1(M_n(D \otimes_K K_v))/\psi(SK_1(M_n(D)) \simeq SK_1(D \otimes_K K_v)/\varphi(SK_1(D)).$$

Предложение 12 доказано.

Воспользуемся теперь следующим результатом приведенной K-теории.

Теорема 10 (Платонов [16]). *Существуют такие тела D над некоторым полем K, что группа $SK_1(D)$ конечна (и даже тривиальна), но для бесконечного множества $V = \{v_i\}$ дискретных нормирований поля K порядки групп $SK_1\left(D \otimes_K K_{v_i}\right)$ не ограничены в совокупности.*

Из теоремы 10 и предложения 12 вытекает следующий результат, дающий, в частности, отрицательный ответ на сформулированную выше гипотезу Кнезера.

Теорема 11 (Платонов [16]). *Существуют такие тела D над некоторым полем K, что порядки групп $G_{K_v}/\overline{G}_K$ (где $G = \boldsymbol{SL}_n(D)$), выражающих отклонение от слабой аппроксимации, не ограничены в совокупности для некоторого бесконечного множества $V = \{v_i\}$ дискретных нормирований поля K.*

(Унитарный аналог теоремы 11 был получен Янчевским [2].)

Несмотря на то, что большинство гипотез об алгебраических группах над произвольным полем было в последнее время опровергнуто, мы берем на себя смелость сформулировать здесь новую гипотезу. А именно, ряд примеров показывает, что в вопросах рациональности, в частности, в вопросах слабой аппроксимации, «идеально» ведут себя не односвязные группы, как предполагалось ранее, а присоединенные.

Гипотеза. *Пусть G — полупростая присоединенная группа над произвольным бесконечным полем K. Тогда многообразие G рационально над K. В частности, G обладает слабой аппроксимацией относительно любого конечного множества S нормирований поля K.*

Легко показать, что эта гипотеза выполняется для группы $G = \boldsymbol{PGL}_n(D)$. Однако проверка этого факта уже для группы $\boldsymbol{PSO}_{2n}(f)$, где $f = x_1^2 + \ldots + x_{2n}^2$ (В. И. Черноусов, неопубликовано), требует привлечения аппарата алгебраической теории квадратичных форм. Общий случай групп $\boldsymbol{PSO}_{2n}(f)$ пока не разобран.

В заключение сделаем несколько замечаний о связи между геометрическими и арифметическими свойствами линейных алгебраических групп. По-видимому, впервые точное выражение этой связи для алгебраических торов дал В. Е. Воскресенский [1], [3]. Чтобы сформулировать его результат, нужно рассмотреть K-определенное вложение $T \hookrightarrow V(T)$ в некоторое гладкое проективное многообразие (существование такого вложения легко следует из теоремы Хиронаки о разрешении особенностей) и соответствующую группу Пикара $\operatorname{Pic} V(T)$; тогда для числового поля K имеет место точная последовательность

$$0 \to A(T) \to H^1(K, \operatorname{Pic} V(T)) \to Ш(T) \to 0, \tag{9}$$

где $Ш(T)$ — группа Шафаревича — Тейта тора T, $A(T)$ — группа, выражающая отклонение от слабой аппроксимации (как заметил Сансюк [1], исходя из соображений естественности следует заменить средний член в (9) на двойственную группу). Впоследствии Сансюк [1] показал, что последовательность, аналогичная (9), имеет место для произвольной связной K-группы.

§ 7.4. Теорема о сильной аппроксимации

Цель настоящего параграфа — установить критерий сильной аппроксимации в связных группах над числовыми полями (относительно случая функциональных глобальных полей см. замечания в конце параграфа). Если $G = HR_u(G)$ — разложение Леви связной K-группы G, то в силу предложения 1 наличие сильной аппроксимации в группе G равносильно наличию сильной аппроксимации в группе H (относительно одного и того же конечного подмножества $S \subset V^K$), поэтому в дальнейшем можно считать группу G редуктивной. Тогда имеет место

Теорема 12. *Пусть G — редуктивная алгебраическая группа над полем алгебраических чисел K, $S \subset V^K$ — конечное подмножество. Тогда G обладает сильной аппроксимацией относительно S в том и только том случае, когда: 1) G односвязна (в частности, G полупроста); 2) G не содержит K-простых компонент G^i с компактной группой G^i_S. В частности, для K-простой односвязной группы G сильная аппроксимация относительно S равносильна некомпактности G_S.*

Доказательство необходимости условий 1), 2) вытекает из следующего более точного утверждения.

Предложение 13. *Пусть G — алгебраическая K-группа, $S \subset V^K$ — непустое конечное подмножество. Предположим, что выполняется одно из следующих условий:*

1) *группа G несвязна;*

2) *группа G связна, но неодносвязна;*

3) *группа G связна, и существует K-простая компонента D^i ее полупростой части D с компактной группой D^i_S.*

Тогда замыкание $\overline{G}_K$ группы G_K в G_{A_S} имеет бесконечный индекс.

Доказательство. Предположим вначале, что группа G несвязна. Пусть P — такое конечное расширение Галуа поля K, что $G = G_P G^0$. По теореме плотности Чеботарева множество $V_0 = \{v \in V_f^K \setminus S \mid P \subset K_v\}$ бесконечно. Зафиксируем целое $l > 0$ и выберем $v_1, \ldots, v_l \in V_0$. Далее, положим $T = \{v_1, \ldots, v_l\}$ и обозначим через $\overline{G}_K^{(T)}$ замыкание G_K в G_T. Поскольку $G_{A_S} = G_T \times G_{A_{S \setminus T}}$, то проекция $\overline{G}_K$ на G_T содержится в $\overline{G}_K^{(T)}$, следовательно,

$$[G_{A_S} : \overline{G}_K] \geqslant [G_T : \overline{G}_K^{(T)}]. \tag{1}$$

С другой стороны, подгруппа $G_T^0 \subset G_T$ является замкнутым нормальным делителем конечного индекса, откуда без труда вытекает, что группа $B = G_K G_T^0$ содержит $\overline{G}_K^{(T)}$. Поэтому

$$[G_T : \overline{G}_K^{(T)}] \geqslant [G_T : B] = [G_T : G_T^0]/[G_K : G_K^0] \geqslant [G : G^0]^{l-1}, \tag{2}$$

ибо $[G_T : G_T^0] = \prod_{v \in T} [G_{K_v} : G_{K_v}^0] = [G : G^0]^t$, так как по построению $G = G_{K_v} G^0$, и, значит, $[G_{K_v} : G_{K_v}^0] = [G : G^0]$. Выбирая t достаточно большим, из (1) и (2) получаем, что индекс $[G_{A_S} : \overline{G}_K]$ не может быть конечным.

Пусть теперь группа G связна. Если $G = HR_u(G)$ — разложение Леви, то ясно, что условия 2), 3) для группы G эквивалентны соответствующим условиям для группы H, причем $[G_{A_S} : \overline{G}_K] = [H_{A_S} : \overline{H}_K]$. Отсюда следует, что в дальнейшем можно считать группу G редуктивной. Положим $S_1 = S \cup V_\infty^K$ и рассмотрим открытую подгруппу $W = \prod_{v \in S \cup V_\infty^K} G_{K_v} \times \prod_{v \notin S_1} G_{\mathcal{O}_v} \subset G_{A_S}$. Тогда замыкание $\overline{\Gamma}$ группы $\Gamma = G_K \cap W$ в W совпадает с пересечением $\overline{G}_K \cap W$, поэтому если индекс $[G_{A_S} : \overline{G}_K]$ конечен, то индекс $[W : \overline{\Gamma}]$ также конечен. В частности, для любого конечного подмножества $T \subset V^K \setminus S_1$ и соответствующего замыкания $\overline{\Gamma}^{(T)}$ группы Γ в $W_T = \prod_{v \in T} G_{\mathcal{O}_v}$ индекс $[W_T : \overline{\Gamma}^{(T)}]$ ограничен сверху числом c, не зависящим от T. Предположим теперь, что группа G неодносвязна, т. е. существует K-определенное накрытие π: $H \to G$, где группа H связна, а $F = \operatorname{Ker} \pi \neq 1$. Тогда для любого $v \in V^K$ можно рассмотреть точную когомологическую последовательность

$$H_{K_v} \xrightarrow{\pi} G_{K_v} \xrightarrow{\psi_{K_v}} H^1(K_v, F),$$

где ψ_{K_v} — соответствующий кограничный морфизм. В силу открытости $\pi(H_{K_v})$ в G_{K_v} (см. следствие 1 из предложения 3.3) для любого конечного $T \subset V^K \setminus S_1$ произведение $U = \prod_{v \in T} \pi(H_{K_v})$ открыто в G_T, так что $\overline{\Gamma}^{(T)} \subset \Gamma U$. Отсюда следует, что, полагая $\psi_T = \prod_{v \in T} \psi_{K_v}$, мы будем иметь

$$\psi_T(\Gamma) = \psi_T(\overline{\Gamma}^{(T)}).$$

Но поскольку для любого T по условию $[W_T : \overline{\Gamma}^{(T)}] \leqslant c$, то в итоге

$$[\psi_T(W_T) : \psi_T(\Gamma)] \leqslant c. \tag{3}$$

Заметим теперь, что группа Γ совпадает с группой S_1-единиц $G_{\mathcal{O}(S_1)}$ и поэтому является конечно порожденной (теорема 5.11), скажем, $\Gamma = \langle \gamma_1, \ldots, \gamma_r \rangle$. Обозначим через P конечное расширение Галуа поля K, порожденное коэффициентами матриц из F и матриц $\delta_1, \ldots, \delta_r \in H_{\overline{K}}$ таких, что $\pi(\delta_i) = \gamma_i$, $i = 1, \ldots, r$.

Ясно, что в этом случае $\pi^{-1}(\Gamma) \subset H_P$, т. е. $\Gamma \subset \pi(H_P)$. Далее, согласно предложению 6.4 найдется такое конечное подмножество $S_0 \subset V_f^K$, что для $v \in V_f^K \setminus S_0$ справедливо соотношение $\psi_{K_v}(G_{\mathcal{O}_v}) = H^1(K_v^{\text{нр}}/K_v, F)$. По теореме плотности Чеботарева множество $V_0 = \{v \in V_f^K \setminus (S_1 \cup S_0) \mid P \subset K_v\}$ бесконечно, и поэтому можно выбрать конечное подмножество $T \subset V_0$ с произвольно большим числом элементов. Тогда для любого $v \in T$ по построению $\Gamma \subset \pi(G_{K_v})$, и, следовательно, $\psi_T(\Gamma) = \{1\}$. С другой стороны, в силу предложения 6.4 $\psi_{K_v}(G_{\mathcal{O}_v}) \simeq F$, ибо $F \subset G_{K_v}$, так что $\psi_T(W_T) \simeq F^l$, $l = [T]$. Тем самым $[\psi_T(W_T) : \psi_T(\Gamma)] = [F]^l$, и мы получаем противоречие с (3), взяв l достаточно большим.

Наконец, покажем, что при выполнении условия 3) индекс $[G_{A_S} : \overline{G}_K]$ также бесконечен. В силу уже доказанного можно предполагать группу G редуктивной и односвязной, в частности, полупростой. Тогда G является прямым произведением своих K-простых компонент G^i, поэтому из конечности индекса $[G_{A_S} : \overline{G}_K]$ вытекает конечность всех индексов $[G^i_{A_S} : \overline{G}^i_K]$. С другой стороны, в силу условия 3) существует компонента G^i с компактной группой G^i_S. Так как группа G^i_K дискретна в $G^i_A = G^i_{A_S} \times G^i_S$, то из компактности G^i_S вытекает дискретность G^i_K в $G^i_{A_S}$, и, следовательно, $\overline{G}^i_K = G^i_K$. Но тогда индекс $[G^i_{A_S} : \overline{G}^i_K]$, очевидно, не может быть конечным (и даже счетным). Предложение доказано.

Доказательство достаточности условий 1), 2) значительно сложнее и составляет основную часть доказательства теоремы 12. Из условия 1) вытекает, что G является прямым произведением своих K-простых компонент, и, воспользовавшись предложением 1, получаем редукцию к случаю K-простых групп. В свою очередь, K-простая группа получается конструкцией ограничения основного поля из простой группы, так что утверждение 3) предложения 2 дает редукцию к простым группам, которыми мы и будем заниматься. Нам придется неоднократно пользоваться следующим простым утверждением.

Лемма 4. *Пусть Γ подгруппа прямого произведения $B = B_1 \times B_2$ двух топологических групп B_1 и B_2, $\pi_i\colon B \to B_i$ $(i = 1, 2)$ — соответствующие проекции. Предположим, что выполняются следующие условия:*

1) *$\pi_1(\Gamma)$ плотно в B_1;*

2) *B_1 обладает базой $\mathcal{U} = \{U\}$ окрестностей единицы, состоящей из подгрупп, причем для любой подгруппы $U \in \mathcal{U}$ проекция $\pi_2(\Gamma \cap (U \times B_2))$ плотна в B_2.*

Тогда Γ плотна в B.

Доказательство почти очевидно. Если предположить, что $\overline{\Gamma} \neq B$, то существует открытое множество $W = W_1 \times W_2 \subset B$, не пересекающееся с Γ. В силу условия 1), найдется элемент $\gamma \in \Gamma$, для которого $\pi_1(\gamma) \in W_1$. Далее, в силу 2) найдется открытая подгруппа $U \subset B_1$, содержащаяся в $\pi_1(\gamma)^{-1}W_1$. Так как $\Gamma \cap W = \varnothing$ и $\gamma^{-1}W \supset U \times \pi_2(\gamma)^{-1}W_2$, то $\pi_2(\Gamma \cap U) \cap \cap \pi_2(\gamma)^{-1}W_2 = \varnothing$, что противоречит 2).

Рассмотрим вначале случай, когда S содержит все архимедовы нормирования и те неархимедовы v, для которых группа G является K_v-анизотропной (последние, как мы знаем, могут существовать лишь для групп типа A_n). В силу утверждения 2) предложения 2 нам нужно показать, что для любого конечного $S_1 \subset V^K \setminus S$ группа $\Gamma = G_{\mathcal{O}(S \cup S_1)}$ плотна в G_{S_1}. Пусть S_2 — максимальное (возможно, пустое) подмножество в S_1 такое, что Γ плотна в G_{S_2} (всюду имеется в виду диагональное вложение группы Γ). Наша цель — показать, что $S_1 = S_2$. Пусть $S_2 \neq S_1$ и $v \in S_1 \setminus S_2$. Положим $S_3 = S_2 \cup \{v\}$, представим группу G_{S_3} в виде $G_{S_3} = G_{S_2} \times G_{K_v}$ и применим лемму 3. Так как Γ не является плотной в G_{S_2}, то найдется такая открытая подгруппа $U \subset G_{S_2}$, что группа $\Delta = \Gamma \cap U$ не является плотной в G_{K_v} (при этом, уменьшая при необходимости подгруппу U, можно с самого начала считать ее компактной). Покажем, что на самом деле это не так. Поскольку Γ является дискретной подгруппой в $G_{S \cup S_1}$ и факторпространство $G_{S \cup S_1}/\Gamma$ имеет конечную меру (теорема 5.7), то Δ является дискретной подгруппой в $D = G_{(S \cup S_1) \setminus S_2} \times U$ и факторпространство D/Δ также имеет конечную меру. Представив D в виде $D = (G_{(S \cup S_1)} \setminus S_3 \times U) \times \times G_{K_v}$ и воспользовавшись с учетом некомпактности G_S леммой 3.17, получим, что Δ как подгруппа в G_{K_v} не является дискретной и факторпространство $G_{K_v}/\overline{\Delta}$ по ее замыканию имеет конечную меру. Обозначим, далее, через p отвечающее нормированию v простое число. Тогда $\mathbb{Q}_p \subset K_v$ и группу G_{K_v} можно рассматривать как p-адическую группу Ли (см. § 3.1). Ее алгебра Ли совпадает с алгеброй $L(G)_{K_v}$, рассматриваемой над полем $\mathbb{Q}_p$. В силу простоты группы G она не содержит нетривиальных идеалов. По теореме Картана (см. теорему 3.4) замыкание $\overline{\Delta}$ является подгруппой Ли в G_{K_v}, причем в силу недискретности Δ ее алгебра Ли $\mathfrak{h} \neq 0$. Далее, из утверждения теоремы 5.7 о конечности объема факторпространства $G_S/G_{\mathcal{O}(S)}$ и некомпактности G_S вытекает бесконечность $G_{\mathcal{O}(S)}$. А тогда, дословно повторяя доказательство теоремы 4.10, мы получим плотность $G_{\mathcal{O}(S)}$ в G в топологии Зарисского. Будучи открытой и компактной, группа U соизмерима с $\prod_{v \in S_2} G_{\mathcal{O}_v}$, так

что индекс $[G_{\mathcal{O}(S)} : G_{\mathcal{O}(S)} \cap U]$ конечен. Отсюда следует, что группа $G_{\mathcal{O}(S)} \cap U$ также плотна в G в топологии Зарисского. Так как, очевидно, $\Delta \supset G_{\mathcal{O}(S)} \cap U$, то, окончательно, Δ плотно в G по Зарисскому. Применяя предложение 3.4, получаем, что $\mathfrak{h}$ является идеалом в $L(G)_{K_v}$, и, следовательно, $\mathfrak{h} = L(G)_{K_v}$, ибо $\mathfrak{h} \neq 0$. Тогда из предложения 3.2 вытекает, что $\bar{\Delta}$ открыто в G_{K_v}. С другой стороны, выше мы установили, что фактор-пространство $G_{K_v}/\bar{\Delta}$ имеет конечную меру. Поэтому в действительности $\bar{\Delta}$ имеет конечный индекс в G_{K_v}, и, следовательно, $\bar{\Delta} = G_{K_v}$, ибо G_{K_v} не имеет нетривиальных подгрупп конечного индекса, что легко вытекает из теоремы 6. Полученное противоречие завершает доказательство теоремы 12 в рассматриваемом случае.

Ослабим теперь ограничения на S, сохранив лишь требование о том, чтобы S содержало все архимедовы нормирования. Положим $S_0 = \{v \in V_f^K \setminus S \mid G$ анизотропна над $K_v\}$; в силу теоремы 6.7 множество S_0 конечно. Из доказанного выше вытекает, что G обладает сильной аппроксимацией относительно $S \cup S_0$, т. е. G_K плотно в $G_{A_{S_0 \cup S}}$. С другой стороны, G обладает слабой аппроксимацией относительно S_0 (предложение 9), т. е. G_K плотно в G_{S_0}. Так как $G_{A_S} = G_{S_0} \times G_{A_{S \cup S_0}}$, то чтобы воспользоваться леммой 4, достаточно показать, что для любой открытой подгруппы $U \subset G_{S_0}$ пересечение $G_K \cap U$ плотно в $G_{A_{S \cup S_0}}$. Так как для любого $v \in S_0$ группа G_{K_v} компактна (теорема 3.1), то вся группа G_{S_0} также компактна, и, значит, U имеет в ней конечный индекс. Отсюда следует, что пересечение $G_K \cap U$ имеет конечный индекс в G_K, поэтому его замыкание имеет конечный индекс в $G_{A_{S \cup S_0}}$, и нам остается показать, что $G_{A_{S \cup S_0}}$ не имеет нетривиальных замкнутых подгрупп конечного индекса. Как мы отмечали выше, из теоремы 6 вытекает, что для любого $v \in V^K \setminus (S \cup S_0)$ группа G_{K_v} не имеет собственных нормальных делителей конечного индекса, следовательно, то же самое справедливо для любой группы G_{S_1}, где $S_1 \subset V^K \setminus (S \cup S_0)$ — конечное подмножество. Поэтому любая замкнутая подгруппа $B \subset G_{A_{S \cup S_0}}$ конечного индекса обязана содержать образы всех вложений $\delta_{S_1}: G_{S_1} \to G_{A_{S \cup S_0}}$. Однако из определения адельной топологии легко вытекает плотность в $G_{A_{S \cup S_0}}$ объединения $\bigcup \delta_{S_1}(G_{S_1})$ по всем конечным подмножествам $S_1 \subset V^K \setminus (S \cup S_0)$, что и дает требуемое.

Нам осталось избавиться от последнего ограничения: $S \supset V_\infty^K$. Положим $S_1 = V_\infty^K \setminus (S \cap V_\infty^K)$, $S_2 = S \cup S_1$; тогда

$$G_{A_S} = G_{A_{S_2}} \times G_{S_1}.$$

Согласно уже доказанному, группа G_K плотна в $G_{A_{S_2}}$. Поэтому для того чтобы воспользоваться леммой 4, достаточно удостовериться, что для любой открытой подгруппы $U \subset G_{A_{S_2}}$ группа $G_K \cap U$ плотна в G_{S_1}. Без ограничения общности группу U, можно считать компактной. Тогда она соизмерима с $G_{A_{S_2}(S_2)}$, и, следовательно, пересечение $G_K \cap U$ соизмеримо с группой $G_{\mathcal{O}(S_2)}$. С другой стороны, согласно предложению 6 группы G_{K_v} для $v \in V_\infty^K$ являются связными, так что связной будет и группа G_{S_1}. Отсюда следует, что нам в действительности достаточно установить плотность $G_{\mathcal{O}(S_2)}$ в G_{S_1}. Обозначим через Λ связную компоненту замыкания $G_{\mathcal{O}(S_2)}$ в G_{S_1}. Утверждается, что Λ является нормальным делителем в G_{S_1}. В самом деле, для любого $g \in G_K$ группы $G_{\mathcal{O}(S_2)}$ и $g^{-1}G_{\mathcal{O}(S_2)}g$ соизмеримы, поэтому их замыкания также соизмеримы, и, следовательно, связные компоненты последних совпадают, т. е. $\Lambda = g^{-1}\Lambda g$. Но в силу предложения 9 группа G обладает слабой аппроксимацией относительно S_1, откуда следует, что $\Lambda = g^{-1}\Lambda g$ для любого $g \in G_{S_1}$. Тем самым Λ является связным нормальным делителем в G_{S_1}, и поэтому $\Lambda = G_{S_3}$ для некоторого подмножества $S_3 \subset S_1$.

Предположим, что $S_4 = S_1 \setminus S_3 \neq \varnothing$, и пусть π: $G_{S_1} \to G_{S_4}$ — соответствующая проекция. Поскольку $\operatorname{Ker} \pi = G_{S_3}$ содержится в замыкании группы $G_{\mathcal{O}(S_2)}$ в G_{S_1}, то связная компонента замыкания Φ группы $G_{\mathcal{O}(S_2)}$ в G_{S_4} совпадает с $\pi(\Lambda) = \{1\}$. Рассмотрим теперь группу G_{S_4} как вещественную группу Ли. Тогда по теореме Картана Φ является подгруппой Ли, причем ее размерность равна нулю, ибо Φ вполне несвязна. Следовательно, Φ дискретна в G_{S_4}. Чтобы получить здесь противоречие, достаточно рассмотреть $G_{\mathcal{O}(S_2)}$ как дискретную подгруппу в $G_S = G_{S_2 \setminus S_4} \times G_{S_4}$, факторпространство по которой имеет конечную меру, и воспользоваться леммой 3.17 с учетом того обстоятельства, что группа $G_{S_2 \setminus S_4}$ некомпактна, ибо $S \subset S_2 \setminus S_4$ и группа G_S некомпактна. Теорема 12 полностью доказана.

Сопоставляя теорему 12 с предложением 13, мы приходим к следующему интересному наблюдению: алгебраическая K-группа G либо обладает сильной аппроксимацией относительно непустого подмножества $S \subset V^K$, либо замыкание $\bar{G}_K$ группы G_K в G_{A_S} имеет бесконечный индекс.

Проблема сильной аппроксимации в алгебраических группах имеет довольно длинную историю. Первым важным результатом здесь была теорема Эйхлера [1] о группе $\boldsymbol{SL}_n(D)$, где D — конечномерная алгебра с делением над K. Позднее различные частные случаи этой проблемы над числовым полем K исследовали Эйхлер [2], Шимура [1], Вейль [3]. Затем Кнезер [10], [11] решил проблему о сильной аппроксимации для классиче-

ских групп, дал необходимые условия для ее решения в общем случае и показал, что теорема о сильной аппроксимации для произвольных групп может быть получена при условии справедливости принципа Хассе. Полное решение проблемы о сильной аппроксимации (теорема 12) было получено Платоновым [3]—[5] на другой идейной основе. Из приведенного выше доказательства теоремы 12 видно, что ключевую роль в нем играет редукция арифметической проблемы о сильной аппроксимации к структурной гипотезе Кнезера—Титса над локальными полями, доказанной первым из авторов (теорема 6).

Теорема о сильной аппроксимации остается справедливой и для глобального поля положительной характеристики, однако ее доказательство нуждается в заметной модификации. Это относится как к доказательству необходимости условий 1) и 2) (см. Бер [2]), так еще в большей степени — к доказательству достаточности. Одна из наиболее существенных причин состоит здесь в том, что важнейшая составная часть приведенного выше рассуждения (которое близко к первоначальному варианту, изложенному в работах Платонова [4], [5]) — теория аналитических групп — неприменима в случае положительной характеристики. Прасад [1]*) усовершенствовал метод Платонова и получил полное доказательство в функциональном случае, которое использует теорему 6 и опирается на следующее утверждение, представляющее самостоятельный интерес.

Теорема 13. *Пусть G — K_v-простая K_v-изотропная алгебраическая группа. Если H — такая замкнутая недискретная подгруппа G_{K_v}, что факторпространство G_{K_v}/H имеет конечную инвариантную меру, то $H \supset G_{K_v}^+$.*

Другое доказательство теоремы 13, основанное на эргодических свойствах пространства G_{K_v}/H, было получено Маргулисом [1]. Отметим также, что в случае нулевой характеристики доказательство теоремы 13 фактически совпадает с первой частью доказательства достаточности в теореме 12.

§ 7.5. Обобщения сильной аппроксимационной теоремы

В последнее время рядом авторов (см. Матьюз и др. [1], Нори [2]) были получены результаты, в некотором смысле обобщающие сильную аппроксимационную теорему. Отправным пунктом этого обобщения служит следующее простое замечание: при доказательстве наличия сильной аппроксимации в односвязной группе G относительно конечного множества $S \supset V_\infty^K$ важную роль играет утверждение о том, что замыкание $\overline{G}_{\mathcal{O}(S)}$ группы $G_{\mathcal{O}(S)}$ в G_{A_S} открыто. В самом деле, вторая часть

*) Русский перевод этой статьи содержится в книге Хамфри [2].

доказательства достаточности в теореме 12 показывает, что можно без ограничения общности считать все нормирования $v \in V_f^K$, для которых группа G является K_v-анизотропной, включенными в S, и достаточно установить, что для любого конечного $S_1 \subset V^K \setminus S$ группа $\bar{G}_K$ содержит образ естественного вложения δ_{S_1}: $G_{S_1} \to G_{A_S}$. Из открытости $\bar{G}_K$ вытекает, что $W = \delta_{S_1}^{-1}(\operatorname{Im}\delta_{S_1} \cap \bar{G}_K)$ является открытой подгруппой в G_{S_1}, которая, очевидно, нормализуется G_K. Из свойства слабой аппроксимации для G (предложение 9) G_K плотно в G_{S_1}, и, следовательно, W нормализуется всей группой G_{S_1}, откуда $W = G_{S_1}$ в силу теоремы 6. Так мы приходим к вопросу, который исследовался в цитированных выше работах: пусть $\Gamma \subset G_K$ — конечно порожденная подгруппа; когда замыкание Γ в G_{A_S} открыто? Мы не будем здесь приводить формулировки полученных результатов в максимальной общности, а ограничимся для простоты случаем $K = \mathbb{Q}$. Тогда имеет место

Теорема 14. *Пусть G — простая односвязная $\mathbb{Q}$-определенная группа, S — конечное множество простых чисел и $\Gamma \subset G_{\mathbb{Z}(S)}$ плотная в G по Зарисскому подгруппа. Тогда замыкание Γ в G_{A_S} открыто.*

Доказательство теоремы 14 легко получается из следующего утверждения, которое представляет самостоятельный интерес:

Теорема 15. *Обозначим через π_p отображение редукции по модулю p. Тогда в условиях теоремы 14 для почти всех $p \notin S$ имеем $\pi_p(\Gamma) = \underline{G}_{F_p}^{(p)}$, где $\underline{G}^{(p)}$ — редукция G по модулю p, F_p — поле из p элементов.*

Доказательство этого факта, данное в работе Матьюза и соавторов [1], к сожалению, использует условную классификацию простых конечных групп. Наоборот, доказательство, приведенное у Нори [2], имеет априорный характер и основывается на ряде красивых наблюдений, связанных с применением экспоненциального и логарифмического отображений в характеристике $p > 0$.

Из теоремы 14 вытекает, что в любой бесконечной арифметической подгруппе Γ односвязной простой $\mathbb{Q}$-определенной алгебраической группы G имеется много подгрупп $\Phi \subset \Gamma$ бесконечного индекса, которые плотны в Γ в адельной топологии. Действительно, Маргулисом и Сойфером [2] показано, что в Γ имеется континуум максимальных подгрупп бесконечного индекса, которые и будут искомыми. С другой стороны, в ряде случаев, например, для $\Gamma = SL_n(\mathbb{Z})$ $(n \geqslant 3)$ адельная топология совпадает с проконечной (отметим, что последнее эквивалентно положительному решению для Γ конгруэнц-проблемы (см. § 9.5)), откуда получаем примеры собственных подгрупп $\Phi \subset \Gamma$, плотных в проконечной топологии. Тогда соответствующий

гомоморфизм $\widehat{\Phi} \to \widehat{\Gamma}$ проконечных пополнений сюръективен. Естественно спросить, существуют ли такие собственные подгруппы $\Phi \subset \Gamma$, для которых гомоморфизм $\widehat{\Phi} \to \widehat{\Gamma}$ является изоморфизмом? Для произвольных конечно порожденных финитно аппроксимируемых групп Γ этот вопрос был поставлен А. Гротендиком [1] в 1970 г. Как показано Платоновым и Тавгенем [1], общая проблема Гротендика имеет отрицательный ответ. Соответствующий пример существует уже в группе $\Gamma = F \times F$, где F — свободная группа с четырьмя образующими x_1, x_2, x_3, x_4. Достаточно рассмотреть нормальный делитель $N \lhd F$, порожденный элементами $x_2x_1x_2^{-1}x_1^{-2}$, $x_3x_2x_3^{-1}x_2^{-2}$, $x_4x_3x_4^{-1}x_3^{-2}$, $x_1x_4x_1^{-1}x_4^{-2}$ (отметим, что факторгруппа F/N является замечательной группой Хигмана), и взять в качестве Φ группу $(N, 1)F^{\Delta}$, где F^{Δ} — диагональ в $F \times F$. Дальнейшие результаты по проблеме Гротендика см. в работах Тавгеня [1], [2], в частности, в [1] построен соответствующий контрпример в классе разрешимых групп. Обратим внимание на тот факт, что указанная выше группа $\Gamma = F \times F$ является арифметической подгруппой в $\boldsymbol{SL}_2 \times \boldsymbol{SL}_2$, так что предположение Гротендика не выполняется и в классе арифметических групп. Тем не менее, остается открытой

Проблема. *Пусть Γ — S-арифметическая подгруппа в G, для которой конгруэнц-ядро $C^S(G)$ конечно (например, $\Gamma = SL_n(\mathbb{Z})$, $n \geqslant 3$). Существуют ли собственные подгруппы $\Phi \subset \Gamma$, для которых гомоморфизм $\widehat{\Phi} \to \widehat{\Gamma}$ проконечных пополнений является изоморфизмом?*

Эта проблема тесно связана с интересной гипотезой, которая возникла при изучении представлений конечно порожденных групп. В § 2.4, п. 7 мы определили многообразие представлений $R(\Gamma, G)$ конечно порожденной группы Γ в алгебраическую группу G. Вместо $R(\Gamma, \boldsymbol{GL}_n)$ мы будем писать $R_n(\Gamma)$ и называть $R_n(\Gamma)$ *многообразием n-мерных представлений группы* Γ. Хорошо известно (см., например, Ван дер Варден [1]), что вполне приводимое представление $\rho \in R_n(\Gamma)$ однозначно с точностью до эквивалентности определяется своим характером, т. е. функцией $\chi_\rho(g) = \operatorname{tr} \rho(g)$, $g \in \Gamma$; с другой стороны, для произвольного представления ρ существует вполне приводимое представление ρ_0 с тем же характером: $\chi_\rho = \chi_{\rho_0}$. Таким образом, возникает естественная биекция между множеством классов эквивалентности вполне приводимых n-мерных представлений группы Γ и множеством $\mathbf{X}_n(\Gamma)$ всех n-мерных характеров. Оказывается, что на $\mathbf{X}_n(\Gamma)$ также существует естественная структура алгебраического многообразия такая, что сопоставление представлению его характера является морфизмом μ многообразий. Вычисление $\mathbf{X}_n(\Gamma)$ для конкретных групп и изучение

влияния геометрии $\mathbf{X}_n(\Gamma)$ на свойства группы Γ и ее представления составляет проблематику геометрического подхода к теории представлений конечно порожденных групп, берущего начало в классических трудах А. Пуанкаре, Ф. Клейна, Фогта, Фрике. Один из первых возникающих здесь вопросов: каковы те группы Γ, для которых $\dim \mathbf{X}_n(\Gamma) = 0$ при любом n? (Последнее условие эквивалентно конечности множества $\mathbf{X}_n(\Gamma)$, и поэтому удовлетворяющие ему группы естественно называть группами конечного представленческого типа.) Ясно, что группами конечного представленческого типа являются все конечные группы, но существуют и бесконечные группы с этим свойством, например, $\Gamma = SL_m(\mathbb{Z})$, $m \geqslant 3$. Конечность представленческого типа здесь вытекает из общей теоремы Г. А. Маргулиса о почти алгебраичности конечномерных представлений неприводимых решеток в полупростых группах Ли ранга не меньшего 2 (см. Маргулис [5]). Однако доказательство Маргулиса не вскрывает связи между конечностью представленческого типа и структурой группы Γ. Поэтому мы покажем, как конечность типа группы $\Gamma = SL_m(\mathbb{Z})$, $m \geqslant 3$, выводится из результата Картера и Келлера [1] об ограниченности ширины группы Γ относительно множества элементарных матриц (см. в § 4.4).

Предложение 14. *Пусть* $\Gamma = SL_m(\mathbb{Z})$, $m \geqslant 3$. *Тогда* $\dim \mathbf{X}_n(\Gamma) = 0$ *для любого* n.

Доказательство (А. С. Рапинчук). Суть упомянутого результата Картера и Келлера состоит в доказательстве существования такой целочисленной константы $d > 0$, что любой элемент $x \in \Gamma$ допускает представление вида $x = x_1^{\alpha_1} \ldots x_d^{\alpha_d}$, где $\alpha_i \in \mathbb{Z}$, x_i совпадает с одной из элементарных матриц $e_{jk}(1)$, множество которых мы обозначим через X. Пусть теперь $\rho\colon \Gamma \to GL_n(\mathbb{C})$ — некоторое n-мерное представление. Если $U \subset \Gamma$ — подгруппа верхних унипотентных матриц, то $\rho(U)$ — нильпотентная подгруппа в $GL_n(\mathbb{C})$. По теореме Мальцева — Колчина $\rho(U)$ обладает триангулируемым нормальным делителем N конечного индекса l. Тогда, очевидно, $\rho(e_{ij}(l)) = \rho(e_{ij}(1))^l \in N$ для всех $i < j$, следовательно,

$$\rho(e_{13}(l^2)) = \rho([e_{12}(l), e_{23}(l)]) \in [N, N];$$

в частности, $\rho(e_{13}(l^2))$ — унипотентная матрица. Учитывая сопряженность всех матриц $e_{ij}(1)$ в группе Γ, получаем, что $\rho(e_{ij}(l^2))$ — унипотентная матрица для любых $i \neq j$. Другими словами,

$$(\rho(e_{ij}(1))^{l^2} - E_n)^n = 0, \tag{4}$$

где E_n — единичная матрица. Обозначим через $f(t)$ — полином $(t^{l^2} - 1)^n$ степени $\delta = l^2 n$. Тогда (4) означает, что $f(\rho(x)) = 0$ для любого $x \in X$. Обозначим через Y (конечное) множество

$\{x_1^{\alpha_1} \ldots x_d^{\alpha_d} \mid x_i \in X,\ 0 \leqslant \alpha \leqslant \delta\}$ и покажем, что $\mathbb{Q}$-оболочка $\mathbb{Q}[\rho(\Gamma)]$ совпадает с $\mathbb{Q}$-пространством, натянутым на $\rho(Y)$, в частности, $\dim_{\mathbb{Q}} \mathbb{Q}[\rho(\Gamma)] < \infty$. В самом деле, поскольку $f(\rho(x)) = 0$ для любого $x \in X$, то любая степень $\rho(x)^\alpha$ линейно выражается через $\rho(x)^\beta$, $0 \leqslant \beta \leqslant \delta$, с целыми коэффициентами. Записывая теперь произвольный элемент $z \in \Gamma$ в виде $z = x_1^{\alpha_1} \ldots x_d^{\alpha_d}$, где $x_i \in X$, $\alpha_i \in \mathbb{Z}$, и подставляя в соответствующее выражение для $\rho(z)$ уже полученные выражения для $\rho(x_i)^{\alpha_i}$, мы получим линейное выражение $\rho(z)$ через элементы множества $\rho(Y)$, что и требовалось.

Из доказанного вытекает, что для произвольного элемента $z \in \Gamma$ все степени $\rho(z)^i$ не могут быть линейно независимыми над $\mathbb{Q}$, так что $\rho(z)$ удовлетворяет некоторому полиномиальному уравнению с рациональными коэффициентами. Этому же уравнению удовлетворяют все собственные числа $\lambda_1, \ldots, \lambda_n$ матрицы $\rho(z)$ и, таким образом, являются алгебраическими числами. Поэтому алгебраическим будет и след $\operatorname{tr} \rho(z) = \sum_{i=1}^{n} \lambda_i$. Завершает доказательство предложения

Лемма 5. *Предположим, что для любого представления* $\rho \in R_n(\Gamma)$ *все следы* $\operatorname{tr} \rho(x)$ *являются алгебраическими числами. Тогда* $\dim \mathbf{X}_n(\Gamma) = 0$.

Доказательство. Пусть $\dim \mathbf{X}_n(\Gamma) > 0$. Тогда существует неприводимая кривая $C \subset R_n(\Gamma)$, определенная над некоторым конечно порожденным полем k, образ которой при отображении $\mu: R_n(\Gamma) \to \mathbf{X}_n(\Gamma)$ не сводится к точке. Обозначим через K поле рациональных функций $k(C)$ и, вложив его в $\mathbb{C}$, построим представление π: $\Gamma \to GL_n(\mathbb{C})$, определяя $\pi(x)$ для $x \in \Gamma$ как матрицу (a_{ij}), где a_{ij} — такая функция на C, что $a_{ij}(\rho) = \rho(x)_{ij}$ для $\rho \in C$. Из того что образ C в $\mathbf{X}_n(\Gamma)$ не сводится к точке, вытекает существование $x_0 \in \Gamma$, для которого $\chi_\pi(x_0) = \operatorname{tr} \pi(x_0)$ является непостоянной функцией из $k(C)$, в частности, $\chi_\pi(x_0) \notin \overline{\mathbb{Q}}$. Мы получаем противоречие с алгебраичностью следов всех представлений $\rho \in R_n(\Gamma)_{\mathbb{C}}$. Лемма 5, а вместе с тем и предложение доказаны.

В § 4.4 мы отмечали, что Тавгень [3] получил обобщение результата Картера и Келлера [1] на все группы Шевалле ранга не меньшего 2. В связи с этим укажем на то обстоятельство, что приведенное доказательство предложения 14 также распространяется на эти группы. (Более точно, если все корни имеют одинаковую длину, то наше доказательство проходит без всяких изменений. В случае же систем с корнями разной длины необходимы несложные модификации, связанные с тем, что ана-

лог равенства (4) нужно отдельно доказывать для коротких и длинных корней.)

Анализируя известные примеры групп конечного представленческого типа, В. П. Платонов [22, 23] высказал следующую гипотезу:

Гипотеза. *Пусть* Γ — *конечно порожденная линейная группа такая, что* $\dim \mathbf{X}_n(\Gamma) = 0$ *для любого* n. *Тогда* Γ *является группой арифметического типа.*

(Под группой арифметического типа здесь понимается группа, соизмеримая с прямым произведением некоторых S-арифметических подгрупп (возможно, относительно разных S), причем соизмеримость в данном случае означает наличие изоморфных подгрупп конечного индекса.)

К сожалению, эта гипотеза пока далека от своего доказательства. Однако даже ее предварительный анализ выявил на первый взгляд удивительную связь со сформулированной выше проблемой Гротендика (см. Платонов, Тавгень [2]). А именно, если, скажем, в группе $\Gamma = SL_n(\mathbb{Z})$, $n \geqslant 3$, найдется собственная подгруппа $\Phi \subset \Gamma$, для которой гомоморфизм $\widehat{\Phi} \to \widehat{\Gamma}$ проконечных пополнений является изоморфизмом, то в любой размерности представления групп Φ и Γ одни и те же. Следовательно, из предложения 14 вытекает, что Φ имеет конечный представленческий тип, причем Гротендиком фактически доказано, что Φ не может быть группой арифметического типа. Поэтому из справедливости гипотезы Платонова вытекало бы положительное решение указанной выше проблемы Гротендика для подгрупп большинства арифметических групп.

ЧИСЛА И ГРУППЫ КЛАССОВ АЛГЕБРАИЧЕСКИХ ГРУПП

Настоящая глава посвящена изучению важной арифметической характеристики алгебраической K-группы G — ее числа классов $\mathrm{cl}(G)$ (см. § 5.1). В § 8.1 мы приводим результаты, которые позволяют интерпретировать проблему вычисления $\mathrm{cl}(G)$ как проблему вычисления числа классов в роде некоторых объектов арифметического типа. В частности, будет установлено, что число классов $\mathrm{cl}(\boldsymbol{O}_n(f))$ ортогональной группы квадратичной формы f совпадает с числом классов в роде f, а число классов $\mathrm{cl}(\boldsymbol{GL}_n)$ группы $\boldsymbol{GL}_n$ $(n \geqslant 1)$ над полем K — с числом классов идеалов K. Уже эти примеры показывают, что проблема вычисления чисел классов является очень трудной, а в самой общей постановке — бесперспективной. Естественно, что мы не смогли в равной степени подробно остановиться здесь на всех аспектах этой проблемы, поставив в центр изложения исследование возможных значений числа классов $\mathrm{cl}(\varphi(G))$ алгебраической K-группы G при различных реализациях φ в зависимости от ее арифметических свойств. Наиболее законченные результаты получаются в том случае, когда G является полупростой группой некомпактного типа. Оказывается, что здесь число классов $\mathrm{cl}(G)$ совпадает с порядком некоторой конечной абелевой группы $\mathcal{G}\,\mathrm{cl}(G)$, называемой группой классов, причем экспонента $\mathcal{G}\,\mathrm{cl}(G)$ является делителем экспоненты f фундаментальной группы F группы G. В частности, если каноническое разложение f имеет вид $f = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, то число классов в любой реализации имеет вид $p_1^{\beta_1} \ldots p_r^{\beta_r}$. В § 8.2 мы доказываем теорему реализации, согласно которой любое число такого вида получается как число классов группы G в подходящей реализации. В § 8.3 исследуются числа классов полупростых групп компактного типа. Основной результат параграфа утверждает, что здесь число классов принимает значения, которые делятся на любое наперед заданное число. В § 8.4 доказывается общая теорема о неограниченности чисел классов неодносвязных групп и исследуется связь между числом классов группы и числами классов ее наиболее важных подгрупп (параболических подгрупп, максимальных торов).

Полученные результаты позволяют решить ряд классических арифметических задач. В частности, в § 8.2—8.3 рассматривают-

ся задачи о числе классов в роде квадратичной формы и числе классов в роде решетки относительно сопряженности. В § 8.5 мы исследуем проблему рода для арифметических групп и целочисленных представлений конечных групп.

§ 8.1. Числа классов алгебраических групп и числа классов в роде

Пусть K — поле алгебраических чисел. Напомним (см. § 5.1), что по определению числом классов $\mathrm{cl}(G)$ алгебраической K-группы G называется число двойных смежных классов $G_{A(\infty)}xG_K$ в разложении группы аделей G_A по подгруппам $G_{A(\infty)}$ и G_K целых и главных аделей соответственно. В § 1.2 мы видели, что для группы иделей J_K поля K (которая является группой аделей одномерного K-разложимого тора $\boldsymbol{G}_m$) индекс $[J_K: J_K^\infty K^*]$ равен числу h_K классов идеалов поля K. Ниже мы покажем, что для ортогональной группы $G = \boldsymbol{O}_n(f)$ невырожденной n-мерной квадратичной формы f над K число классов $\mathrm{cl}(G)$ совпадает с числом классов в роде формы f. Тем самым введенное определение числа классов представляет естественное обобщение классических арифметических инвариантов, восходящих к Лагранжу и Гауссу. Кроме того, мы увидим, что это определение успешно работает и в других ситуациях, где позволяет на основе универсальных методов получать новые результаты.

Необходимо сделать одно замечание, которое следует постоянно иметь в виду при работе с числами классов алгебраических групп. Если в группе иделей J_K подгруппа J_K^∞ целых иделей определена однозначно, то для произвольной алгебраической K-группы G группа целых аделей $G_{A(\infty)}$ корректно определена лишь в том случае, если фиксирована реализация G как матричной группы. В дальнейшем мы под заданием реализации группы G будем понимать задание точного K-определенного представления φ: $G \to \boldsymbol{GL}_r$ и решетки $L(\varphi) \subset K^r$. Тогда полагаем $G_{A(\infty)}^{L(\varphi)} = \varphi_A^{-1}(\varphi(G)_{A(\infty)}^{L(\varphi)})$, где

$$\varphi(G)_{A(\infty)}^{L(\varphi)} = \prod_{v \in V_\infty^K} \varphi(G)_{K_v} \times \prod_{v \in V_f^K} \varphi(G)_{\mathcal{O}_v}^{L(\varphi)_v};$$

$\varphi(G)_{\mathcal{O}_v}^{L(\varphi)_v} = \{g \in \varphi(G)_{K_v} \mid gL(\varphi)_v = L(\varphi)_v\}$ — группа целых v-адических точек относительно локализации $L(\varphi)_v$ решетки $L(\varphi)$, т. е. совокупность тех $g \in \varphi(G)_{K_v}$, которые записываются матрицей из $GL_r(\mathcal{O}_v)$ в базисе решетки $L(\varphi)_v$. Эквивалентным образом, группу $\varphi(G)_{A(\infty)}^{L(\varphi)}$ можно рассматривать как стабилизатор в $\varphi(G)_A$ решетки $L(\varphi)$ относительно действия группы $GL_r(A)$

на решетках в K^r, которое определяется следующим образом. Если $g=(g_v)\in GL_r(A)$ и $L\subset K^r$ — некоторая решетка, то для почти всех $v\in V_f^K$ имеем $g_v\in GL_r(\mathcal{O}_v)$ и $L_v=\mathcal{O}_v^r$ (см. § 1.5, п. 3), так что $g_vL_v=L_v$; поэтому согласно теореме 1.15 существует единственная решетка $M\subset K^r$ со свойством: $M_v=g_vL_v$ для всех $v\in V_f^K$, и по определению полагаем $M=gL$.

Число классов группы G, отвечающее реализации φ, мы будем обозначать через $\mathrm{cl}(\varphi(G)^{L(\varphi)})$, употребляя также обозначения $\mathrm{cl}(G^{L(\varphi)})$, $\mathrm{cl}(\varphi(G))$ или просто $\mathrm{cl}(G)$, если это не приводит к недоразумению. Отметим, что из теоремы 5.1 вытекает конечность числа $\mathrm{cl}(\varphi(G))$ для любой реализации φ. Действительно, сама теорема 5.1 утверждает конечность числа $\mathrm{cl}(\varphi(G))$ для любой реализации φ, задаваемой свободной решеткой $L(\varphi)$. С другой стороны, для произвольных двух реализаций φ_i: $G\to \boldsymbol{GL}_{r_i}$ $(i=1, 2)$ группы $G_{A(\infty)}^{L(\varphi_i)}$ соизмеримы. В самом деле, $G_{A(\infty)}^{L(\varphi_i)}=G_\infty\times G_{A_f(\infty)}^{L(\varphi_i)}$, причем архимедова часть G_∞ группы аделей не зависит от выбора реализации, а конечные части $G_{A_f(\infty)}^{L(\varphi_1)}$ и $G_{A_f(\infty)}^{L(\varphi_2)}$, будучи открытыми компактными подгруппами в G_{A_f}, соизмеримы. Отсюда следует, что числа классов $\mathrm{cl}(\varphi_1(G))$ и $\mathrm{cl}(\varphi_2(G))$ конечны (или бесконечны) одновременно. С учетом вышесказанного, из этого замечания вытекает

Теорема 1. *Для любой реализации φ алгебраической K-группы G число классов $\mathrm{cl}(\varphi(G))$ конечно.*

Как мы уже отмечали, основная цель настоящей главы — изучить, какие значения может принимать $\mathrm{cl}(\varphi(G))$ в зависимости от арифметических и структурных свойств группы G. В этой связи напомним, что согласно предложению 5.4 число классов $\mathrm{cl}(\varphi(G))$ равно единице для любой реализации φ, если G обладает свойством абсолютной сильной аппроксимации.

Выше мы видели, что число h_K классов идеалов поля K можно интерпретировать как число классов одномерного K-разложимого тора $T\simeq \boldsymbol{GL}_1$. Оказывается, что число классов полной линейной группы любой степени также равно h_K.

Предложение 1. *Пусть $G=\boldsymbol{GL}_n$ — полная линейная группа над K в естественной реализации. Тогда* $\mathrm{cl}(G)=h_K$.

Доказательство использует широко применяемый при определении чисел классов подход, суть которого состоит в том, что «некоммутативная» задача подсчета числа двойных классов редуцируется к вычислению некоторого индекса в коммутативных группах. В рассматриваемой ситуации это можно проделать при помощи гомоморфизма определителя $\det$: $G\to \boldsymbol{G}_m$, который мы

для краткости обозначим через f. Ясно, что образ $f(G_A)$ совпадает с группой иделей J_K поля K, $f(G_{A(\infty)})$ есть подгруппа целых иделей J_K^∞, а $f(G_K)$ — подгруппа главных иделей K^*. Покажем, что отображение θ: $G_{A(\infty)}\backslash G_A/G_K \to J_K^\infty\backslash J_K/K^*$, индуцируемое f, является биекцией. Тогда

$$\mathrm{cl}(G) = [J_K : J_K^\infty K^*] = h_K,$$

и требуемое доказано. С учетом вышесказанного в доказательстве нуждается лишь инъективность θ, т. е. импликация

$$J_K^\infty f(g) K^* = J_K^\infty f(h) K^* \Rightarrow G_{A(\infty)} g G_K = G_{A(\infty)} h G_K \qquad (1)$$

для g, $h \in G_A$. Если $f(g) = x f(h) y$, где $x \in J_K^\infty$, $y \in K^*$, то, выбирая $a \in G_{A(\infty)}$, $b \in G_K$ со свойством $f(a) = x$, $f(b) = y$, будем иметь $f(g) = f(ahb)$, и достаточно показать, что элементы g и $t = ahb$ определяют один и тот же двойной класс по подгруппам $G_{A(\infty)}$ и G_K. Очевидно, что $s = t^{-1}g \in H_A$, где $H = \boldsymbol{SL}_n$. Подгруппа $U = t^{-1}H_{A(\infty)}t$ является открытой в H_A, и поэтому пересечение $Us \cap H_\infty H_K$ непусто, ибо для H имеет место абсолютная сильная аппроксимация. Учитывая, что $H_\infty \subset U$, отсюда получаем существование таких $u \in H_{A(\infty)}$, $v \in H_K$, что

$$s = t^{-1}g = t^{-1}uv.$$

Тогда $g = utv$, что и требовалось. Предложение 1 доказано.

Равенство $\mathrm{cl}(G) = h_K$, где $G = \boldsymbol{GL}_n$, можно подвергнуть дальнейшей расшифровке, используя соображения, аналогичные тем, при помощи которых доказывалось равенство $h_K = [J_K : J_K^\infty K^*]$, и заменяя дробные идеалы поля K (т. е. решетки в пространстве K^1) n-мерными решетками. Для этого зафиксируем решетку $L = \mathcal{O}^n \subset K^n$ и воспользуемся действием группы G_A на решетках, которое было определено выше. Утверждается, что орбита $G_A(L)$ совпадает со множеством $\mathscr{L}$ всех n-мерных решеток. В самом деле, для любой решетки $M \subset K^n$ и почти всех $v \in V_f^K$ имеет место совпадение локализаций $L_v = M_v$. С другой стороны, любая локализация M_v является $\mathcal{O}_v$-свободной (см. § 1.5), и поэтому найдется $g_v \in G_{K_v}$ со свойством $M_v = g_v(L_v)$. Отсюда без труда вытекает существование такого аделя $g \in G_A$, что $M = g(L)$. Так как группа $G_{A(\infty)}$ является стабилизатором решетки L, то множество двойных смежных классов $\{G_{A(\infty)}\backslash G_A/G_K\}$ находится в биективном соответствии со множеством орбит $G_K\backslash\mathscr{L}$, т. е. множеством классов изоморфных решеток. Поэтому из предложения 1 вытекает, что число классов изоморфных n-мерных решеток совпадает с числом h_K классов идеалов поля K. Этот факт может быть доказан и непосредственно методами теории решеток. Для этого используем введенное в § 1.5, п. 3 понятие псевдобазиса решетки.

Напомним, что любая решетка $M \subset K^n$ обладает псевдобазисом, т. е. существует представление вида $M = \mathcal{O}x_1 \oplus \mathcal{O}x_2 \oplus \ldots \ldots \oplus \mathcal{O}x_{n-1} \oplus \mathfrak{a}x_n$, где $\mathfrak{a} \subset \mathcal{O}$ — некоторый идеал, класс которого в группе классов идеалов зависит лишь от самой решетки M. Далее показывается, что две решетки $M = \mathcal{O}x_1 \oplus \ldots \oplus \mathcal{O}x_{n-1} \oplus \oplus \mathfrak{a}x_n$ и $N = \mathcal{O}y_1 \oplus \ldots \oplus \mathcal{O}y_{n-1} \oplus \mathfrak{b}y_n$ изоморфны в том и только том случае, если классы идеалов $\mathfrak{a}$ и $\mathfrak{b}$ совпадают. Из этих фактов вытекает, что классы изоморфных n-мерных решеток находятся в биективном соответствии с классами дробных идеалов поля K, и мы опять приходим к равенствам $\mathrm{cl}(G) = [G_K \backslash \mathscr{L}] = = h_K$. Уже на этом примере видно, что адельная интерпретация позволяет достичь цели быстрее и более прямым путем. Кроме того, она позволяет сформулировать следующий критерий свободы решетки, который будет нам полезен:

Лемма 1. *Зафиксируем решетку $L = \mathcal{O}^n$ и рассмотрим произвольную решетку $M \subset K^n$. Тогда M свободна в том и только том случае, если $f(g) \in J_K^\infty K^*$, где $g \in G_A$ — такой элемент, что $M = g(L)$.*

Доказательство. Из сказанного выше вытекает, что решетка M свободна в том и только том случае, если $g \in G_K G_{A(\infty)}$, что в силу (1) сводится к условию $f(g) \in J_K^\infty K^*$.

Отсюда вытекает

Предложение 2. *Пусть K — поле алгебраических чисел с гильбертовым полем классов $\tilde{K}$, $L \subset K^n$ — некоторая свободная решетка. Тогда если решетка M обладает свойством: локализации L_v и M_v совпадают для всех неархимедовых $v \neq v_0$, а $\tilde{K} \subset \subset K_{v_0}$, то M свободна.*

Доказательство. Напомним вначале, что гильбертовым полем классов для K называется максимальное абелево расширение K, неразветвленное во всех точках. В терминах глобальной теории полей классов $\tilde{K}$ определяется как поле, отвечающее норменной подгруппе $J_K^\infty K^*/K^* \subset C_K$, так что группа Галуа $\mathrm{Gal}(\tilde{K}/K)$ изоморфна группе классов идеалов поля K. При этом включение $\tilde{K} \subset K_{v_0}$ равносильно тому, что главный класс $J_K^\infty K^*$ содержит все идели $i^{v_0}(\alpha)$, $\alpha \in K_{v_0}^*$, с компонентами

$$i_v = \begin{cases} 1, & v \neq v_0, \\ \alpha, & v = v_0 \end{cases}$$

(все отмеченные факты можно найти в [АТЧ]).

Пусть теперь M удовлетворяет условиям предложения. Тогда в качестве аделя $g \in G_A$, переводящего L в M, можно взять адель вида $g^{v_0}(a)$, $a \in G_{K_{v_0}}$, так что $f(g) = i^{v_0}(\det a) \in J_K^\infty K^*$, и согласно лемме 1 M свободна. Предложение 2 доказано.

При доказательстве теоремы об одноклассных решетках (см. § 8.2) нам понадобится одно утверждение, которое также вытекает из леммы 1.

Предложение 3. *Пусть $S \subset V^K$ — такое конечное подмножество, содержащее V_∞^K, что $J_K = J_K^S K^*$, где J_K^S — группа S-целых иделей. Тогда для любой решетки $M \subset K^n$ существует такая свободная решетка $N \subset K^n$, что $M_v = N_v$ для $v \in V^K \setminus S$. Другими словами, любую решетку можно сделать свободной, изменяя ее локализации лишь для $v \in S \setminus V_\infty^K$.*

Доказательство. Положим $L = \mathcal{O}^n$ и пусть $g \in G_A$ — такой адель, что $M = g(L)$. Тогда $f(g) \in J_K = J_K^S K^*$, и поэтому $f(g) = xyz$, где v-компоненты x_v равны 1 для $v \notin S \setminus V_\infty^K$, $y \in J_K^\infty$ и $z \in K^*$. Выберем для $v \in S \setminus V_\infty^K$ такие элементы $a_v \in G_{K_v}$, что $f(a_v) = x_v$, и построим адель h с компонентами

$$h_v = \begin{cases} 1, & v \notin S \setminus V_\infty^K, \\ a_v, & v \in S \setminus V_\infty^K. \end{cases} \tag{2}$$

Утверждается, что решетка $N = h^{-1}(M)$ будет искомой. В самом деле, $N = (h^{-1}g)(L)$ и $f(h^{-1}g) = f(h)^{-1}f(g) = x^{-1}(xyz) = yz \in J_K^\infty K^*$, так что N свободна. С другой стороны, из (2) вытекает, что $N_v = M_v$ для $v \in V^K \setminus S$. Предложение доказано.

Здесь мы завершаем обсуждение круга вопросов, связанных с вычислением числа классов группы $G = \boldsymbol{GL}_n$ в естественной реализации и различными интерпретациями равенства $\mathrm{cl}(G) = h_K$. Однако связи между числами классов алгебраических групп и классическими арифметическими инвариантами на этом не оканчиваются. В частности, мы сейчас покажем, что число классов в роде невырожденной квадратичной формы f совпадает с числом классов $\mathrm{cl}(G)$ соответствующей ортогональной группы $G = \boldsymbol{O}_n(f)$. Этот факт мы выведем из одного общего результата, который имеет и ряд других интересных приложений.

Итак, пусть G — линейная алгебраическая K-группа, действующая на аффинном K-многообразии X. Зафиксируем некоторые реализации $G \subset \boldsymbol{GL}_n$, $X \subset \mathbb{A}^m$ и будем предполагать, что относительно этих реализаций рассматриваемое действие G на X определено над кольцом целых $\mathcal{O} \subset K$, т. е. задается полиномами с коэффициентами из $\mathcal{O}$. Будем говорить, что два элемента $x, y \in X_\mathcal{O}$ эквивалентны (относительно группы $G_\mathcal{O}$), если существует такой элемент $g \in G_\mathcal{O}$, что $y = gx$. Как мы увидим на приводимых ниже примерах, это определение охватывает классические понятия эквивалентности целочисленных матриц, целочисленных квадратичных форм, целочисленных представлений конечных групп и других арифметических

объектов. Основной возникающей здесь проблемой является проблема выяснения условий, необходимых и достаточных для эквивалентности двух элементов. При этом серия очень естественных необходимых условий указывается без труда: если элементы $x, y \in X_G$ эквивалентны относительно G_G, то они эквивалентны относительно групп G_K и G_{G_v} для всех неархимедовых нормирований v поля K, т. е. существуют такие элементы $g_K \in G_K$ и $g_v \in G_{G_v} (v \in V_f^K)$, что $g_K x = y$, $g_v x = y$. Вопрос о достаточности этих условий имеет характер вопроса о справедливости в данной ситуации локально-глобального принципа. Он оказывается очень сложным и с качественной точки зрения решается отрицательно во многих случаях. Чтобы иметь возможность обсуждать его количественную сторону (т. е. характеризовать отклонение от локально-глобального принципа), введем следующее

Определение. Пусть $x \in X_G$. *Родом* $\operatorname{gen}(x)$ элемента x называется совокупность таких элементов $y \in X_G$, что x и y эквивалентны относительно групп G_K и G_{G_v} для всех $v \in V_f^K$. *Классом* $\operatorname{cl}(x)$ элемента x называется орбита $G_G x$, т. е. совокупность элементов y, которые эквивалентны x относительно группы G_G. Каждый род $\operatorname{gen}(x)$ распадается в объединение непересекающихся классов:

$$\operatorname{gen}(x) = \bigcup_{i \in I} \operatorname{cl}(x_i), \quad \operatorname{cl}(x_i) \cap \operatorname{cl}(x_j) = \varnothing \qquad (i \neq j);$$

мощность множества I называется *числом классов в роде* элемента x (относительно действия группы G) и обозначается через $f_G(x)$.

Таким образом, локально-глобальный принцип для эквивалентности справедлив тогда и только тогда, когда $f_G(x) = 1$. В общем случае $f_G(x) \neq 1$, что, естественно, порождает задачу вычисления $f_G(x)$. О полученных в этом направлении результатах мы расскажем в последующих параграфах, а сейчас укажем на имеющуюся связь с числами классов алгебраических групп.

Теорема 2 (о стабилизаторе). *Пусть $x \in X_G$ и $G(x) = \{g \in G \mid gx = x\}$ — стабилизатор элемента x. Тогда число $f_G(x)$ совпадает с числом двойных смежных классов $G(x)_{A(\infty)} g G(x)_K$ группы аделей $G(x)_A$, содержащихся в главном классе $G_{A(\infty)} G_K$. В частности, число $f_G(x)$ всегда конечно. Если для группы G имеет место абсолютная сильная аппроксимация, то $f_G(x) = \operatorname{cl}(G(x))$.*

Доказательство. Пусть $\mathfrak{g}(x)$ — фактормножество, получаемое из рода $\operatorname{gen}(x)$ отождествлением элементов, принадлежащих одному классу. Так как $f_G(x) = [\mathfrak{g}(x)]$, то для доказательства теоремы достаточно установить биекцию между множеством M

двойных смежных классов $G(x)_{A(\infty)}gG(x)_K$ группы $G(x)_A$, содержащихся в $G_{A(\infty)}G_K$, и $\mathfrak{g}(x)$.

Пусть $\bar{g}=G(x)_{A(\infty)}gG(x)_K\in M$, т. е.

$$g=g_{A(\infty)}g_K, \tag{3}$$

где $g_{A(\infty)}\in G_{A(\infty)}$, $g_K\in G_K$. Покажем, что $y=g_Kx\in\operatorname{gen}(x)$. Во-первых, заметим, что $y\in X_{\mathcal{O}}$. Действительно, по определению

$$y=g_Kx, \tag{4}$$

так что $y\in X_K$. Далее, из (3) получаем, что для любого $v\in V_f^K$ v-компонента g_v совпадает с $g_{\mathcal{O}_v}g_K$, где $g_{\mathcal{O}_v}\in G_{\mathcal{O}_v}$. Отсюда $g_K=g_{\mathcal{O}_v}^{-1}g_v$ и

$$y=g_{\mathcal{O}_v}^{-1}x, \tag{5}$$

ибо $g_v\in G(x)_{K_v}$; в частности, $y\in X_{\mathcal{O}_v}$. Поэтому $y\in X_{\mathcal{O}}$, и равенства (4), (5) показывают, что $y\in\operatorname{gen}(x)$. Определим теперь соответствие $\theta\colon M\to\mathfrak{g}(x)$, отображая $\bar{g}$ в класс, содержащий y.

Корректность определения θ. Пусть $\bar{g}=G(x)_{A(\infty)}gG(x)_K=$ $=G(x)_{A(\infty)}hG(x)_K$, т. е. $h=t_{A(\infty)}gt_K$, где $t_{A(\infty)}\in G(x)_{A(\infty)}$, $t_K\in G(x)_K$. Рассмотрим произвольное разложение $h=h_{A(\infty)}h_K$ в классе $G_{A(\infty)}G_K$. Тогда

$$h=h_{A(\infty)}h_K=(t_{A(\infty)}g_{A(\infty)})(g_Kt_K),$$

и, следовательно, $s=h_{A(\infty)}^{-1}t_{A(\infty)}g_{A(\infty)}=h_Kt_K^{-1}g_K^{-1}\in G_{A(\infty)}\cap G_K=G_{\mathcal{O}}$. Поэтому $h_K=sg_Kt_K$, и, значит,

$$\tilde{y}=h_Kx=(sg_Kt_K)x=s(g_Kx)=sy,$$

откуда следует, что $\tilde{y}$ лежит в том же классе, что и y. Корректность определения θ доказана.

Сюръективность θ. Пусть $y\in\operatorname{gen}(x)$. Тогда

$$y=g_Kx=g_vx \tag{6}$$

для некоторых $g_K\in G_K$, $g_v\in G_{\mathcal{O}_v}$ $(v\in V_f^K)$. Обозначим через h адель с компонентами

$$h_v=\begin{cases} g_K, & v\in V_\infty^K,\\ g_v, & v\in V_f^K.\end{cases} \tag{7}$$

Очевидно, $h\in G_{A(\infty)}$. Из (6) и (7) вытекает, что для любого $v\in V^K$ имеет место включение $h_v^{-1}g_K\in G(x)_{K_v}$, так что $g=h^{-1}g_K\in$ $\in G(x)_A$. При этом по построению $\bar{g}=G(x)_{A(\infty)}gG(x)_K\in M$ и при отображении θ классу $\bar{g}$ соответствует класс эквивалент-

ности в $g(x)$, содержащий y, что и доказывает сюръективность θ.

Инъективность θ. Пусть g, $h \in G(x)_A$ — такие элементы, что соответствующие классы $\bar{g}$, $\bar{h}$ лежат в M и $\theta(\bar{g}) = \theta(\bar{h})$. Выберем разложения $g = g_{A(\infty)}g_K$, $h = h_{A(\infty)}h_K$ в $G_{A(\infty)}G_K$. Тогда равенство $\theta(\bar{g}) = \theta(\bar{h})$ означает существование такого $s \in G_{\mathcal{O}}$, что

$$h_K x = s g_K x.$$

Положим $t_{A(\infty)} = h_{A(\infty)} s g_{A(\infty)}^{-1}$, $t_K = g_K^{-1} s^{-1} h_K$. Легко проверяется, что

$$t_{A(\infty)} \in G(x)_A \cap G_{A(\infty)} = G(x)_{A(\infty)},$$
$$t_K \in G(x)_A \cap G_K = G(x)_K.$$

При этом $h = t_{A(\infty)} g t_K$, т. е. $\bar{g} = \bar{h}$, и инъективность θ установлена.

Таким образом, мы доказали основную часть теоремы 2. Конечность числа $f_G(x)$ теперь непосредственно вытекает из теоремы 1. Если G обладает абсолютной сильной аппроксимацией, то $\mathrm{cl}(G) = 1$ (см. предложение 5.4), т. е. $G_A = G_{A(\infty)}G_K$, и поэтому $f_G(x) = \mathrm{cl}(G(x))$. Теорема 2 полностью доказана.

Приведем примеры использования теоремы 2.

Пример 1 (квадратичные формы). Пусть X — многообразие невырожденных симметрических $(n \times n)$-матриц, рассматриваемое как подмногообразие n^2-мерного аффинного пространства $\mathbb{A}^{n^2} \simeq \boldsymbol{M}_n$. Точки X однозначно соответствуют невырожденным n-мерным квадратичным формам, причем точкам из X_K и $X_{\mathcal{O}}$ отвечают соответственно K- и $\mathcal{O}$-определенные формы. На пространстве X естественным образом действует группа $G = \boldsymbol{GL}_n$,

$$g(F) = {}^t g F g, \quad g \in G, \quad F \in X,$$

где ${}^t g$ — транспонированная к g матрица, причем это действие, очевидно, $\mathcal{O}$-определено. Поэтому на основе данного выше определения можно ввести понятия рода и класса симметрической матрицы $F \in X_{\mathcal{O}}$, а также понятия числа классов в роде $f_G(F)$. Так как элементам из X однозначно соответствуют квадратичные формы, то все перечисленные понятия переносятся на квадратичные формы и превращаются в классические понятия теории квадратичных форм, восходящие к Лагранжу и Гауссу. Так, например, род $\mathrm{gen}(f)$ квадратичной формы f представляет собой совокупность квадратичных форм, которые эквивалентны форме f над полем K и над всеми кольцами $\mathcal{O}_v$, $v \in V_f^K$; при этом класс $\mathbf{cl}(f)$ есть совокупность форм, $\mathcal{O}$-эквивалентных форме f. Число классов в роде здесь по традиции обозначается через $c(f)$.

Если f — невырожденная $\mathcal{O}$-определенная квадратичная форма и $F \in X_{\mathcal{O}}$ — соответствующая симметрическая матрица, то стабилизатор $G(F)$ совпадает с ортогональной группой $\boldsymbol{O}_n(f)$. Покажем, что всегда $\boldsymbol{O}_n(f)_A \subset GL_n(A(\infty))GL_n(K)$. Для каждого $v \in V_f^K$ группа $GL_n(\mathcal{O}_v)$, очевидно, содержит матрицу с определителем -1, поэтому любой элемент из $\boldsymbol{O}_n(f)_A$ путем умножения на подходящий элемент из $GL_n(A(\infty))$ можно заключить в группу $SL_n(A)$. Но, как мы уже отмечали, $\mathrm{cl}(\boldsymbol{SL}_n) = 1$, т. е. $SL_n(A) = SL_n(A(\infty))SL_n(K)$, откуда следует, что $\boldsymbol{O}_n(f)_A \subset GL_n(A(\infty))GL_n(K)$. С учетом этого из теоремы 2 получаем

Предложение 4. *Число $c(f)$ классов в роде невырожденной квадратичной формы f конечно и равно числу классов $\mathrm{cl}(\boldsymbol{O}_n(f))$ соответствующей ортогональной группы.*

Здесь уместно также привести простой пример, принадлежащий Милнору, который показывает, что, вообще говоря, $c(f) \neq 1$. Рассмотрим над полем $\mathbb{Q}$ две симметрические целочисленные матрицы

$$F_1 = \begin{pmatrix} 5 & 0 \\ 0 & 11 \end{pmatrix}, \quad F_2 = \begin{pmatrix} 1 & 0 \\ 0 & 55 \end{pmatrix}.$$

Введем следующие невырожденные рациональные матрицы:

$$g_1 = \begin{pmatrix} 1/4 & -11/4 \\ 1/4 & 5/4 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1/7 & -22/7 \\ 2/7 & 5/7 \end{pmatrix}.$$

Прямое вычисление показывает, что ${}^t g_i F_1 g_i = F_2$ $(i = 1, 2)$. Так как матрицы g_i рациональны, причем $g_1 \in GL_2(\mathbb{Z}_p)$ для всех $p \neq 2$, а $g_2 \in GL_2(\mathbb{Z}_2)$, то матрицы F_1, F_2 (и соответствующие им квадратичные формы f_1, f_2) лежат в одном роде. В то же время если предположить, что F_1, F_2 лежат в одном классе, то должна найтись такая целочисленная матрица $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, что ${}^t g F_1 g = F_2$. Последнее соотношение, как легко проверить, сводится к системе

$$\begin{cases} 5a^2 + 11c^2 = 1, \\ 5ab + 11cd = 0, \\ 5b^2 + 11d^2 = 55, \end{cases}$$

уже первое уравнение которой неразрешимо в целых числах. Таким образом, $f_{\mathbb{Z}_2}(F_1) = c(f_1) > 1$.

Пример 2 (целочисленные представления). Пусть Γ — конечно порожденная группа, $X = R_n(\Gamma)$ — многообразие n-мерных представлений Γ, рассматриваемое как подмногообразие в $(\boldsymbol{GL}_n)^d$ (см. § 2.4, 7.5). Группа $G = \boldsymbol{GL}_n$ естественным образом действует на $R_n(\Gamma)$; при этом орбиты действия совпадают с классами эквивалентных представлений. Точкам из $X_{\mathbb{Z}}$ отвечают целочисленные представления $\rho\colon \Gamma \to GL_n(\mathbb{Z})$ степени n, а общие понятия рода и класса элемента приводят в данной

ситуации к понятиям рода и класса целочисленного представления, которые применяются в теории представлений (см. Кэртис, Райнер [1]). Так как над полем $\mathbb{Q}$ имеем $\mathrm{cl}(\boldsymbol{GL}_n)=1$ (предложение 1), то из теоремы 2 вытекает

Предложение 5. *Пусть* $\rho\colon \Gamma\to GL_n(\mathbb{Z})$ — *целочисленное представление конечно порожденной группы* Γ, C — *централизатор* ρ ($=$ *централизатор* $\rho(\Gamma)$). *Тогда число классов в роде представления* ρ *конечно и равно числу классов* $\mathrm{cl}(C)$ *группы* C.

Используя этот факт, мы, следуя работе Платонова [2], получим точные оценки для числа классов в роде целочисленного представления (см. § 8.5), улучшающие оценки А. В. Ройтера [1], полученные с помощью модульной техники.

Пример 3 (сопряженность целочисленных матриц). Пусть $G\subset \boldsymbol{GL}_n$ — связная алгебраическая подгруппа, определенная над полем $\mathbb{Q}$. Рассмотрим присоединенное действие группы G:

$$x(y)=xyx^{-1},\quad x,\ y\in G.$$

Род элемента $g\in G_{\mathbb{Z}}$, который в данном случае принято обозначать $[g]_G$, совпадает с совокупностью элементов из $G_{\mathbb{Z}}$, которые сопряжены с g в группах $G_{\mathbb{Q}}$ и $G_{\mathbb{Z}_p}$ для всех простых p; класс g есть его класс сопряженности в $G_{\mathbb{Z}}$. Применяя теорему 2, получаем следующее утверждение о числе $f_G(g)$ классов в роде.

Предложение 6 («теорема о централизаторе», Платонов [8]). *Число* $f_G(g)$ *классов в роде элемента* $g\in G_{\mathbb{Z}}$ *конечно и совпадает с числом двойных смежных классов* $C_{A(\infty)}xC_{\mathbb{Q}}$ *группы аделей* C_A *централизатора* $C=Z_G(g)$, *содержащихся в главном классе* $G_{A(\infty)}G_{\mathbb{Q}}$. *В частности, если* $\mathrm{cl}(G)=1$, *то* $f_G(g)=\mathrm{cl}(C)$.

В § 8.5 мы, применяя это утверждение, получим решение так называемой проблемы рода (см. Рапинчук [1]).

В заключение укажем еще на одну интерпретацию чисел классов алгебраических групп, которая в некотором смысле двойственна обсуждавшейся выше. Для этого рассмотрим алгебраическую K-группу $G\subset \boldsymbol{GL}_n$ и некоторую решетку $M\subset K^n$.

Определение. *Родом* $\mathrm{gen}(M)$ решетки M относительно группы G называется совокупность решеток $N\subset K^n$, которые локально изоморфны M относительно группы G, т. е. таких, что для каждого $v\in V_f^K$ существует $g_v\in G_{K_v}$ со свойством $g_v(M_v)=N_v$. *Класс* решетки M состоит из решеток, изоморфных M относительно G, т. е. решеток вида $g(M)$, $g\in G_K$.

Предложение 7. *Число классов в роде решетки* M *относительно группы* G *конечно и совпадает с числом классов* $\mathrm{cl}(G^M)$.

Доказательство, как обычно, заключается в установлении биекции между множеством Λ двойных смежных классов $G_K g G^M_{A(\infty)}$ группы G_A, число которых совпадает с $\mathrm{cl}(G^M)$, и множеством $\mathfrak{g}(M)$ классов в роде решетки M. Для этого рассмот-

рим действие группы G_A на решетках в пространстве K^n, которое индуцировано вложением $G_A \subset GL_n(A)$ и рассмотренным выше действием $GL_n(A)$. Утверждается, что род $\mathrm{gen}(M)$ совпадает с орбитой $G_A(M)$. Включение $G_A(M) \subset \mathrm{gen}(M)$ очевидно. Пусть теперь $N \in \mathrm{gen}(M)$, так что для каждого $v \in V_f^K$ имеется элемент $g_v \in G_{K_v}$ со свойством $g_v(M_v) = N_v$. Так как $M_v = N_v = C_v^n$ для почти всех v, то элемент $h = (h_v)$ с компонентами

$$h_v = \begin{cases} 1, & v \in V_\infty^K, \\ g_v, & v \in V_f^K, \end{cases}$$

является аделем, причем по построению $h(M) = N$. Так как стабилизатор решетки M при описанном действии совпадает с $G^M_{A(\infty)}$, а орбиты группы G_K и есть классы решеток в нашем смысле, то тем самым получаем требуемую биекцию $\Lambda \simeq \mathfrak{g}(M)$. Предложение 7 доказано.

Пример 4. Пусть $G = \boldsymbol{O}_n(f)$, где f — невырожденная квадратичная форма на пространстве K^n. Тогда род решетки $M \subset K^n$ состоит из решеток $N \subset K^n$, которые локально изометричны M, т. е. таких, что локализации M_v и N_v изометричны (другими словами, существует изометрия $\sigma_v \in \boldsymbol{O}_n(f)_{K_v}$ со свойством $\sigma_v(M_v) = N_v$) для всех $v \in V_f^K$. Класс решетки M состоит из всех изометричных ей решеток. Таким образом, в данной ситуации наши понятия рода и класса решетки полностью совпадают с теми, которые использовал О'Мира в своей книге [1] по арифметической теории квадратичных форм. Объединяя предложения 4 и 7, мы приходим к следующему утверждению:

пусть f — невырожденная квадратичная форма на пространстве K^n с коэффициентами в $\mathcal{O}$; тогда следующие три числа совпадают

1) *число $c(f)$ классов в роде формы f;*
2) *число классов $\mathrm{cl}(\boldsymbol{O}_n(f))$;*
3) *число классов в роде решетки $L = \mathcal{O}^n$ относительно действия группы $G = \boldsymbol{O}_n(f)$.*

Отметим, что в дальнейшем, имея в виду интерпретацию числа классов, содержащуюся в предложении 7, мы будем называть решетки M, для которых $\mathrm{cl}(G^M) = 1, 2, \ldots$, соответственно одноклассными, двуклассными и т. д.

§ 8.2. Числа и группы классов полупростых групп некомпактного типа. Теорема реализации

В этом параграфе мы получим полное описание значений, которые принимает число классов $\mathrm{cl}(\varphi(G))$ полупростой K-группы G некомпактного типа при различных реализациях φ.

(Напомним, что полупростая K-группа G называется группой некомпактного типа, если она не имеет K-простых сомножителей G^i с компактной архимедовой частью группы аделей G^i_∞.) Используя теорему 7.12, можно дать эквивалентное определение: G является группой некомпактного типа в том и только том случае, когда для односвязной накрывающей $\tilde{G}$ имеет место абсолютная сильная аппроксимация. Оказывается, что в рассматриваемом случае $\mathrm{cl}(\varphi(G))$ может принимать далеко не произвольные значения, и мы вначале получим соответствующие ограничения на число классов, а затем покажем, что все априори возможные значения действительно реализуются в качестве $\mathrm{cl}(\varphi(G))$.

Итак, пусть G — полупростая K-группа некомпактного типа. Рассмотрим универсальное K-определенное накрытие $\pi\colon \tilde{G} \to G$ и соответствующую точную последовательность K-групп

$$1 \to F \to \tilde{G} \to G \to 1, \tag{1}$$

где $F = \mathrm{Ker}\,\pi$ — фундаментальная группа группы G. Для любого расширения M/K можно рассмотреть отрезок точной когомологической последовательности

$$\tilde{G}_M \xrightarrow{\pi_M} G_M \xrightarrow{\psi_M} H^1(M, F),$$

где ψ_M — кограничный морфизм (см. § 1.3). Если положить $M = K_v$ $(v \in V^K)$, а затем перейти к прямым произведениям, то мы придем к точной последовательности

$$\prod_v \tilde{G}_{K_v} \xrightarrow{\Pi} \prod_v G_{K_v} \xrightarrow{\Psi} \prod_v H^1(K_v, F), \tag{2}$$

где $\Pi = \prod_v \pi_{K_v}$, $\Psi = \prod_v \psi_{K_v}$. Обозначим через π_A и ψ_A ограничения Π и Ψ на группы аделей $\tilde{G}_A$ и G_A соответственно.

Предложение 8. *Пусть G — полупростая K-группа некомпактного типа. Тогда главный класс $G_{A(\infty)}G_K$ является нормальной подгруппой в G_A, содержащей коммутант $[G_A, G_A]$, и число классов $\mathrm{cl}(G)$ совпадает с порядком конечной абелевой группы $\mathcal{G}\mathrm{cl}(G) = G_A/G_{A(\infty)}G_K$. При этом*

$$\mathcal{G}\mathrm{cl}(G) \simeq \psi_A(G_A)/\psi_A(G_{A(\infty)}G_K); \tag{3}$$

в частности,

$$\mathrm{cl}(G) = [\psi_A(G_A) : \psi_A(G_{A(\infty)}G_K)]. \tag{4}$$

Доказательство. Вначале установим точность последовательности

$$\tilde{G}_A \xrightarrow{\pi_A} G_A \xrightarrow{\psi_A} \prod_v H^1(K_v, F).$$

В силу точности (2) достаточно показать, что

$$\Big(\prod_v \pi_{K_v}(\widetilde{G}_{K_v})\Big) \cap G_A = \pi_A(G_A).$$

Последнее же эквивалентно тому, что для почти всех $v \in V_f^K$ справедливо равенство

$$\pi_{K_v}(\widetilde{G}_{K_v}) \cap G_{\mathcal{O}_v} = \pi_{K_v}(\widetilde{G}_{\mathcal{O}_v}). \tag{5}$$

В § 6.2 мы видели, что для почти всех $v \in V_f^K$ имеет место точная последовательность

$$1 \to F_{\mathcal{O}_{K_v^{\text{нр}}}} \to \widetilde{G}_{\mathcal{O}_{K_v^{\text{нр}}}} \xrightarrow{\pi} G_{\mathcal{O}_{K_v^{\text{нр}}}} \to 1,$$

причем $F_{\mathcal{O}_{K_v^{\text{нр}}}}$ для почти всех $v \in V_f^K$ совпадает с F. Тогда для $g \in G_{\mathcal{O}_{K_v^{\text{нр}}}}$ имеем $\pi^{-1}(g) \subset \widetilde{G}_{\mathcal{O}_{K_v^{\text{нр}}}}$. В частности, если $g = \pi(x) \in G_{\mathcal{O}_v}$, где $x \in \widetilde{G}_{K_v}$, то $x \in \widetilde{G}_{\mathcal{O}_{K_v^{\text{нр}}}} \cap \widetilde{G}_{K_v} = \widetilde{G}_{\mathcal{O}_v}$, откуда и следует (5).

Заметим теперь, что из свойства абсолютной сильной аппроксимации для $\widetilde{G}$ вытекает включение $\pi_A(\widetilde{G}_A) \subset G_{A(\infty)}G_K$; более того, $\pi_A(\widetilde{G}_A) \subset g^{-1}G_{A(\infty)}gG_K$ для любого $g \in G_A$. В самом деле, подгруппа $U = \pi_A^{-1}(g^{-1}G_{A(\infty)}g)$ является открытой в $\widetilde{G}_A$ и содержит $\widetilde{G}_\infty$, поэтому из плотности $\widetilde{G}_\infty\widetilde{G}_K$ в $\widetilde{G}_A$ вытекает, что $\widetilde{G}_A = UG_K$. Следовательно,

$$\pi_A(\widetilde{G}_A) = \pi_A(U\widetilde{G}_K) \subset g^{-1}G_{A(\infty)}gG_K.$$

Так как ψ_A является гомоморфизмом G_A на абелеву группу, то из доказанного вытекает, что

$$[G_A, G_A] \subset \operatorname{Ker}\psi_A = \operatorname{Im}\pi_A \subset g^{-1}G_{A(\infty)}gG_K \tag{6}$$

для любого $g \in G_A$. Теперь уже несложно завершить доказательство предложения. Для любых $g_i \in G_{A(\infty)}$, $h_i \in G_K$ $(i = 1, 2)$ и $g \in G_A$ имеем

$$\begin{gathered}(g_1h_1)(g_2h_2) = (g_1g_2)([g_2^{-1}, h_1])h_1h_2 \in G_{A(\infty)}G_K,\\ (g_1h_1)^{-1} = h_1^{-1}g_1^{-1} = g_1^{-1}[g_1, h_1^{-1}]h_1^{-1} \in G_{A(\infty)}G_K,\\ g^{-1}g_1h_1g = g_1[g_1^{-1}, g^{-1}][g^{-1}, h_1]h_1 \in G_{A(\infty)}G_K\end{gathered} \tag{7}$$

в силу включения $[G_A, G_A] \subset G_{A(\infty)}G_K$ (где $[x, y] = xyx^{-1}y^{-1}$). Включения (7) показывают, что класс $G_{A(\infty)}G_K$ является нормальной подгруппой в G_A, которая содержит коммутант $[G_A, G_A]$. Для доказательства утверждения о том, что порядок

факторгруппы $\mathscr{G}\mathrm{cl}(G) = G_A/G_{A(\infty)}G_K$ совпадает с числом классов, достаточно установить совпадение двойного класса $G_{A(\infty)}xG_K$ с обычным смежным классом $xG_{A(\infty)}G_K$ для любого $x \in G_A$. В силу (6) для любых $g, h \in G_A$ имеем включение

$$(gh)^{-1}G_{A(\infty)}(gh)G_K \subset g^{-1}G_{A(\infty)}g\,[g^{-1}G_{A(\infty)}g,\ h^{-1}]\,G_K \subset$$
$$\subset g^{-1}G_{A(\infty)}g\,[G_A,\ G_A]\,G_K = g^{-1}G_{A(\infty)}gG_K.$$

Полагая здесь $g = 1$, $h = x$, получим включение

$$x^{-1}G_{A(\infty)}xG_K \subset G_{A(\infty)}G_K,$$

а полагая $g = x$, $h = x^{-1}$, — обратное включение, что и дает требуемое. Доказательство изоморфизма (3) вытекает из стандартной теоремы о гомоморфизмах, ибо $\operatorname{Ker}\psi_A \subset G_{A(\infty)}G_K$. Предложение 8 полностью доказано.

Определение. Группа $\mathscr{G}\mathrm{cl}(G) = G_A/G_{A(\infty)}G_K$ называется *группой классов* полупростой алгебраической K-группы G некомпактного типа.

Из предложения 8 вытекает

Следствие. *Пусть G — полупростая K-группа некомпактного типа, f — показатель (т. е. минимальная экспонента) ее фундаментальной группы F. Тогда f является экспонентой группы классов $\mathscr{G}\mathrm{cl}(G)$. В частности, число классов $\mathrm{cl}(G)$ всегда имеет вид $p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, где $p_1, \ldots, p_r$ — различные простые делители порядка F.*

Цель настоящего параграфа — показать, что все числа описанного вида получаются как числа классов $\mathrm{cl}(\varphi(G))$ в подходящей реализации φ группы G. Эту задачу решает

Теорема 3 (о реализации). *Пусть G — полупростая K-группа некомпактного типа, f — показатель ядра F универсального накрытия π: $\tilde{G} \to G$. Тогда для любой конечной абелевой группы B экспоненты f существует такая K-реализация φ_B группы G, что группа классов $\mathscr{G}\mathrm{cl}(\varphi_B(G))$ изоморфна B. В частности, эффективно определяется такое n, что G имеет точное представление степени n и для любого числа вида $p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ существует такая свободная решетка $M(\alpha_1, \ldots, \alpha_r) \subset K^n$, что $\mathrm{cl}\left(G^{M(\alpha_1, \ldots, \alpha_r)}\right) = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$.*

Доказательство теоремы 3 делится на ряд этапов, первым из которых является теорема о существовании свободной одноклассной решетки.

Теорема 4. *Пусть G — полупростая K-группа некомпактного типа и степени n. Тогда существует такая свободная решетка $L_0 \subset K^n$, что $\mathrm{cl}\left(G^{L_0}\right) = 1$.*

Доказательство использует следующее простое утверждение, которое позволяет специализировать выбор системы представителей двойных смежных классов.

Лемма 2. *Пусть H — алгебраическая K-группа, обладающая слабой аппроксимацией относительно конечного подмножества $S \subset V_f^K$, $W \subset H_{A(\infty)}$ — открытая подгруппа вида $W = H_\infty \times \prod_{v \in V_f^K} W_v$, где W_v — открытая подгруппа в $H_{\mathcal{O}_v}$ и $W_v = H_{\mathcal{O}_v}$ для почти всех $v \in V_f^K$. Тогда существует такое конечное подмножество $T \subset V_f^K$, не пересекающееся с S, и такая конечная система представителей $\{h^i\}_{i=1}^r$ двойных смежных классов $W \backslash H_A / H_K$, что v-компонента h_v^i равна 1 для любого $v \notin T$ и любого $i = 1, \ldots, r$. В частности, $H_A = H_{A(T)} H_K$ для подходящего конечного T, содержащего V_∞^K и не пересекающегося с S.*

Доказательство. Подгруппа W, очевидно, имеет конечный индекс в $H_{A(\infty)}$, поэтому из теоремы 1 вытекает существование конечной системы представителей $\{x^i\}_{i=1}^r$ двойных смежных классов $W \backslash H_A / H_K$. Используя слабую аппроксимацию, выбираем для каждого $i = 1, \ldots, r$ элемент $a^i \in H_K \cap \prod_{v \in S} (W_v x_v^i)$ и положим $\bar{x}^i = x^i (a^i)^{-1}$, $y^i = (y_v^i)$, где

$$y_v^i = \begin{cases} 1, & v \notin S, \\ \bar{x}_v^i, & v \in S. \end{cases}$$

Тогда по построению $y^i \in W$ для любого $i = 1, \ldots, r$, так что адель $z^i = (y^i)^{-1} x^i (a^i)^{-1}$ определяет тот же двойной смежный класс, что и x^i. Положим $T = \{v \in V_f^K \mid z_v^i \notin W_v$ для некоторого $i = 1, \ldots, r\}$. Очевидно, T — конечное подмножество, причем поскольку $z_v^i = 1$ для $v \in S$, имеем $T \cap S = \varnothing$. Теперь ясно, что в качестве искомой системы представителей $\{h^i\}_{i=1}^r$ можно взять «усеченные» относительно T адели z^i, т. е. положить $h^i = (h_v^i)$, где

$$h_v^i = \begin{cases} 1, & v \notin T, \\ z_v^i, & v \in T. \end{cases} \tag{8}$$

Остается заметить, что построенная система $\{h^i\}_{i=1}^r$ содержит представители всех двойных смежных классов $H_{A(\infty)} \backslash H_A / H_K$, и поскольку в силу (8) $h^i \in H_{A(T \cup V_\infty^K)}$, то $H_A = \bigcup_{i=1}^r H_{A(\infty)} h^i H_K = H_{A(T \cup V_\infty^K)} H_K$. Лемма доказана.

Согласно теореме 7.7 найдется такое конечное подмножество $S_0 \subset V_f^K$, что для любого конечного $S \subset V^K$, непересекающегося с S_0, группа G обладает слабой аппроксимацией относительно S. Применяя лемму 2 к одномерному тору $H = \mathbf{G}_m$, установим существование такого конечного подмножества $S \subset V^K$, содержащего V_∞^K и не пересекающегося с S_0, что $J_K = J_K^S K^*$, где J_K^S — группа S-целых идеалей. Зафиксируем теперь некоторую решетку $L \subset K^n$ и обозначим через W подгруппу в $G_{A(\infty)}^L$ вида

$$W = G_\infty \times \prod_{v \in V_f^K \setminus S} G_{\mathcal{O}_v}^{L_v} \times \prod_{v \in S_f} \left(G_{\mathcal{O}_v}^{L_v} \cap \pi_{K_v}\left(\tilde{G}_{K_v}\right)\right),$$

где $S_f = S \setminus V_\infty^K$.

Применяя еще раз лемму 2, теперь уже к группе $H = G$ и множеству S_f (отметим, что по построению G обладает слабой аппроксимацией относительно S), мы получим такую систему представителей $\{g^i\}_{i=1}^l$ двойных смежных классов $W \backslash G_A / G_K$, что для некоторого конечного $T \subset V_f^K$, не пересекающегося с S, v-компонента g_v^i равна 1 для любого $v \notin T$ и любого $i = 1, \ldots, l$.

Искомую решетку L_0 мы построим, изменяя v-компоненты исходной решетки L для $v \in S \cup T$. Для нормирований $v \in T$ нужные нам локальные компоненты строятся на основе следующего утверждения.

Лемма 3. *Существует такая решетка $N_v \subset K_v^n$, что*

$$G_{K_v} = G_{\mathcal{O}_v}^{N_v} \pi_{K_v}\left(\tilde{G}_{K_v}\right).$$

Действительно, согласно предложению 3.18 существует такая максимальная компактная подгруппа $B \subset G_{K_v}$, что $G_{K_v} = B \times \times \pi_{K_v}(\tilde{G}_{K_v})$. С другой стороны, в силу предложения 1.12 найдется решетка $N_v \subset K_v^n$ со свойством $G_{\mathcal{O}_v}^{N_v} = B$.

Из условия $J_K = J_K^S K^*$ и предложения 2 вытекает существование таких решеток $M_v \subset K_v^n$ для $v \in S_f$, что решетка L_0 с локальными компонентами

$$(L_0)_v = \begin{cases} L_v, & v \notin S \cup T, \\ N_v, & v \in T, \\ M_v, & v \in S \end{cases}$$

является свободной, и нам остается показать, что $\mathrm{cl}(G^{L_0}) = 1$.

Пусть $g \in G_A$. Тогда существуют $h \in W$, $t \in G_K$ и число i, $1 \leqslant i \leqslant l$, такие, что $h = hg^i t$. Для $v \in T$ выберем разложение

$$h_v g_v^i = b_v s_v,$$

где $b_v \in G_{\mathcal{O}_v}^{N_v}$, $s_v \in \pi_{K_v}(\widetilde{G}_{K_v})$, и введем адели x, y с компонентами

$$x_v = \begin{cases} h_v, & v \notin S \cup T, \\ b_v, & v \in T, \\ 1, & v \in S, \end{cases} \qquad y_v = \begin{cases} 1, & v \notin S \cup T, \\ s_v, & v \in T, \\ h_v, & v \in S. \end{cases}$$

Тогда поскольку $g_v^i = 1$ для $v \notin T$, имеем $hg^i = xy$, причем по построению $x \in G_{A(\infty)}^{L_0}$, $y \in \pi_A(\widetilde{G}_A)$. Поскольку G является группой некомпактного типа, то $\pi_A(\widetilde{G}_A) \subset G_{A(\infty)}^{L_0} G_K$, следовательно, $g = hg^i t = xyt \in G_{A(\infty)}^{L_0} G_K$, что и требовалось. Теорема 4 доказана.

Если не налагать на конструируемую одноклассную решетку требования свободы, то доказательство ее существования становится совсем коротким и при этом выпукло выступает основная идея рассуждений, состоящая в использовании предложения 3.18. Доказательство же самого предложения 3.18 опирается на факт сопряженности силовских про-p-подгрупп в группе $\pi_{K_v}(\widetilde{G}_{K_v})$, и мы получаем великолепный пример применения абстрактных теоретико-групповых соображений к исследованию тонких арифметических вопросов. В связи с этим стоит отметить, что доказательство теоремы 4 для ортогональной группы неопределенной квадратичной формы методами теории решеток требует гораздо большей подготовительной работы (см. О'Мира [1]). Обратим внимание читателя также на то обстоятельство, что в теореме 4 разбирается, по-видимому, максимально общая ситуация, в которой существование одноклассных решеток является правилом, а не исключением. А именно, в работе Платонова, Бондаренко, Рапинчука [1], § 4, приведены примеры торов и полупростых групп компактного типа, которые не имеют одноклассной реализации ни в каком пространстве.

В связи с этим отметим следующий любопытный факт, который показывает, что существование одноклассной реализации определяется внутренними свойствами самой группы и не зависит от выбора точного представления.

Предложение 9. *Пусть $G \subset \boldsymbol{GL}_n$ — произвольная алгебраическая K-группа степени n. Предположим, что существует такая решетка $L \subset K^n$, что $\mathrm{cl}(G^L) = 1$. Тогда для любого точного K-определенного представления φ: $G \to \boldsymbol{GL}_r$ также существует такая решетка $L(\varphi) \subset K^r$, что $\mathrm{cl}(G^{L(\varphi)}) = 1$.*

Доказательство. Обозначим через S конечное подмножество V_f^K такое, что для $v \in V_f^K \setminus S$ выполняются следующие условия: морфизм φ определен над $\mathcal{O}_v$ и $L_v = \mathcal{O}_v^n$. Для каждого $v \in S$ группа $\varphi(G_{\mathcal{O}_v}^L)$ компактна, и поэтому существует

такая решетка $M_v \subset K_v^r$, что $\varphi\left(G_{\mathcal{O}_v}^{L_v}\right) \subset \varphi(G)_{\mathcal{O}_v}^{M_v}$. Зададим локализации искомой решетки $L(\varphi)$ следующим образом:

$$L(\varphi)_v = \begin{cases} \mathcal{O}_v^r, & v \notin S, \\ M_v, & v \in S. \end{cases}$$

Тогда из наших построений вытекает, что $\varphi\left(G_{A(\infty)}^L\right) \subset \varphi(G)_{A(\infty)}^{L(\varphi)}$, и поэтому $\varphi(G)_A = \varphi(G_A) = \varphi\left(G_{A(\infty)}^L G_K\right) \subset \varphi(G)_{A(\infty)}^{L(\varphi)} \varphi(G)_K$, т. е. $\mathrm{cl}\left(\varphi(G)^{L(\varphi)}\right) = 1$. Предложение доказано.

Возвращаемся к доказательству теоремы 3. Построение искомых решеток проводится исходя из специальной одноклассной решетки L путем изменения ее v-компонент для нормирований v из некоторого конечного подмножества $S \subset V_f^K$ таким образом, что соответствующая группа целых аделей уменьшается. В этой ситуации можно несколько уточнить описание изоморфизма (3).

Предложение 10. *Пусть G — полупростая K-группа некомпактного типа и степени n, $L \subset K^n$ — такая решетка, что $\mathrm{cl}(G^L) = 1$. Предположим, что $N \subset K^n$ — другая решетка, причем выполняются следующие условия:*

1) $\psi_A\left(G_{A(\infty)}^N\right) \subset \psi_A\left(G_{A(\infty)}^L\right)$;

2) $N_v = L_v$ *для* $v \in V_f^K \setminus S$, *где* $S \subset V_f^K$ — *некоторое конечное подмножество.*

Для любого подмножества $T \subset V^K$ обозначим через δ_T: $H^1(K, F) \to \prod_{v \in T} H^1(K_v, F)$ отображение, индуцированное ограничениями, и пусть $\delta = \delta_{V^K}$. Тогда

$$\mathcal{G}\mathrm{cl}(G^N) \simeq \prod_{v \in S} \psi_{K_v}\left(G_{\mathcal{O}_v}^{L_v}\right) / \delta_S\left(\psi_K\left(G_{\mathcal{O}}^L\right)\right) \prod_{v \in S} \psi_{K_v}\left(G_{\mathcal{O}_v}^{N_v}\right). \tag{9}$$

При этом группа $\delta_S\left(\psi_K\left(G_{\mathcal{O}}^L\right)\right)$ совпадает с образом при проекции p_S: $\prod_v H^1(K_v, F) \to \prod_{v \in S} H^1(K_v, F)$ группы $\delta\left(\psi_K\left(G_{\mathcal{O}}^L\right)\right)$, а последняя является конечной группой и может быть определена из соотношения $\delta\left(\psi_K\left(G_{\mathcal{O}}^L\right)\right) = \psi_A\left(G_{A(\infty)}^L\right) \cap \delta\left(\psi_K(G_K)\right)$.

Доказательство. Так как $\mathrm{cl}(G^L) = 1$, то $\psi_A(G_A) = \psi_A\left(G_{A(\infty)}^L G_K\right)$. Поэтому в силу изоморфизма (3) имеем

$$\mathcal{G}\mathrm{cl}(G^N) \simeq \psi_A\left(G_{A(\infty)}^L G_K\right) / \psi_A\left(G_{A(\infty)}^N G_K\right). \tag{10}$$

Используя в данной ситуации классический изоморфизм $AB/CB \simeq A/(A \cap B)C$, справедливый для произвольных подгрупп A, B, C некоторой абелевой группы таких, что $C \subset A$, будем иметь

$$\mathcal{G}\mathrm{cl}(G^N) \simeq \psi_A\left(G_{A(\infty)}^L\right) / \left(\psi_A\left(G_{A(\infty)}^L\right) \cap \psi_A(G_K)\right) \psi_A\left(G_{A(\infty)}^N\right).$$

Применяя теперь проекцию p_S и учитывая, что ядро ограничения p_S на $\psi_A(G^L_{A(\infty)})$ лежит в $\psi_A(G^N_{A(\infty)})$, из теоремы о гомоморфизмах получаем изоморфизм

$$\mathscr{G}\mathrm{cl}(G^N) \simeq \prod_{v\in S} \psi_{K_v}\left(G^{L_v}_{\mathcal{O}_v}\right)/\Gamma \prod_{v\in S} \psi_{K_v}\left(G^{N_v}_{\mathcal{O}_v}\right),$$

где Γ обозначает образ при p_S пересечения $\psi_A(G^L_{A(\infty)}) \cap \psi_A(G_K)$. Учитывая, что $\psi_A(G_K) = \delta(\psi_K(G_K))$ и $\delta_S(\psi_K(G^L_{\mathcal{O}})) = p_S(\delta(\psi_K(G^L_{\mathcal{O}})))$, мы видим, что нам достаточно убедиться в справедливости равенства

$$\psi_A(G^L_{A(\infty)}) \cap \psi_A(G_K) = \psi_A(G^L_{\mathcal{O}}).$$

Пусть $x = \psi_A(g) = \psi_A(h)$, где $g \in G^L_{A(\infty)}$, $h \in G_K$. Тогда $\psi_A(gh^{-1}) = 1$, и, значит, $y = gh^{-1} \in \operatorname{Ker}\psi_A = \operatorname{Im}\pi_A$ (см. доказательство предложения 8). Из свойства абсолютной сильной аппроксимации для $\tilde{G}$ вытекает равенство

$$\pi_A(\tilde{G}_A) = (\pi_A(\tilde{G}_A) \cap G^L_{A(\infty)})\,\pi_A(\tilde{G}_K),$$

так что $y = gh^{-1} = st$ для некоторых $s \in \pi_A(\tilde{G}_A) \cap G^L_{A(\infty)}$, $t \in \pi_A(\tilde{G}_K)$. Имеем

$$s^{-1}g = th \in G^L_{A(\infty)} \cap G_K = G^L_{\mathcal{O}},$$

откуда $x = \psi_A(h) = \psi_A(th) \in \psi_A(G^L_{\mathcal{O}})$, что и требовалось. Остается заметить, что из теоремы 4.17 вытекает наличие у группы $G^L_{\mathcal{O}}$ конечной системы образующих, поэтому группа $\psi_K(G^L_{\mathcal{O}})$ является конечно порожденной абелевой группой конечной экспоненты, и потому конечна. Предложение 10 доказано.

У нас уже есть все необходимое для доказательства теоремы 3. Однако мы ограничимся здесь полным доказательством для важного случая, когда фундаментальная группа F является циклической. При этом оказывается возможным дать явное описание получаемых реализаций, что важно с точки зрения арифметических приложений (см. теорему 6 и предложение 13). Кроме того, этот случай содержит основные технические трудности, и общий случай фактически может быть к нему редуцирован (см. Платонов, Бондаренко, Рапинчук [3]).

Теорема 5. *Пусть G — полупростая K-группа некомпактного типа с циклической фундаментальной группой F порядка $f = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$. Предположим, что существует такое точное K-определенное представление $\rho\colon G \to \mathbf{GL}_r$ и такое конечное расширение P/K, что для почти всех $v \in V_f^K$ со свойством $P \subset K_v$ найдется решетка $R_v \subset K_v^r$, для которой $\psi_{K_v}\left(G^R_{\mathcal{O}_v}\right) = 1$. Тогда для любой конечной абелевой группы B экспоненты f найдется*

такая свободная решетка $L(B) \subset K^r$, *что* $\mathcal{G}\mathrm{cl}\left(G^{L(B)}\right) \simeq B$. *В частности, для любого числа вида* $p_1^{\beta_1} \ldots p_s^{\beta_s}$ *найдется свободная решетка* $L(\beta_1, \ldots, \beta_s) \subset K^r$ *с числом классов* $\mathrm{cl}\left(G^{L(\beta_1, \ldots, \beta_s)}\right) = p_1^{\beta_1} \ldots p_s^{\beta_s}$. *Если* G *имеет степень* n *как линейная группа, то в качестве* ρ *всегда можно взять представление степени* $2n$, *задаваемое формулой* $\rho(g) = \begin{pmatrix} g & 0 \\ 0 & E_n \end{pmatrix}$.

Доказательство. Увеличивая P, будем в дальнейшем предполагать, что P является расширением Галуа поля K, содержит гильбертово поле классов $\bar{K}$ и что $F = F_P$. Зафиксируем некоторую одноклассную решетку $L \subset K^r$ и выберем разложение $B = \prod_{i=1}^{l} B_i$ группы B на циклические сомножители. Обозначим через S_1 совокупность таких $v \in V_f^K$, что $\psi_{K_v}\left(G_{\mathcal{O}_v}^{L_v}\right) \neq H^1\left(K_v^{\text{нр}}/K_v, F\right)$. Отметим, что из предложения 6.4 вытекает конечность S_1. Далее, пусть S_2 — такое конечное подмножество в V_f^K, что для любого конечного S, не пересекающегося с S_2, отображение δ_S: $H^1(K, F) \to \prod_{v \in S} H^1(K_v, F)$ сюръективно (см. следствие 2 из предложения 7.8). По теореме плотности Чеботарева можно выбрать l нормирований $\bar{v}_1, \ldots, \bar{v}_l \in V_f^K \setminus (S_1 \cup S_2)$ со свойством $P \subset K_{\bar{v}_i}$ для $i = 1, \ldots, l$. Положим $\bar{S} = \{\bar{v}_1, \ldots, \bar{v}_l\}$. Тогда имеет место

Лемма 4. *Существует такая свободная одноклассная решетка* $M \subset K^r$, *что*

$$\delta_{\bar{S}}\left(\psi_K\left(G_{\mathcal{O}}^M\right)\right) = \prod_{i=1}^{l} H^1\left(K_{\bar{v}_i}^{\text{нр}}/K_{\bar{v}_i}, F\right). \tag{11}$$

Доказательство. Используя лемму 2, выберем такое конечное подмножество $S \subset V^K$, содержащее V_∞^K и не пересекающееся с $S_2 \cup \bar{S}$, что $J_K = J_K^S K^*$. Из наших построений и предложения 7.10 вытекает наличие в группе G свойства слабой аппроксимации относительно множества $T = S \cup \bar{S}$. Рассмотрим две открытые подгруппы в G_T

$$W_1 = G_\infty \times \prod_{v \in T \setminus V_\infty^K} G_{\mathcal{O}_v},$$

$$W_2 = \prod_{v \in T} \pi_{K_v}\left(\tilde{G}_{K_v}\right).$$

Тогда из свойства слабой аппроксимации получаем, что $W_1 = (G_K \cap W_1)(W_1 \cap W_2)$ в смысле диагонального вложения G_K в G_T, следовательно, $\delta_T(\psi_K(G_K \cap W_1)) = \psi_T(W_1)$, где $\psi_T =$

$= \prod_{v \in T} \psi_{K_v}$. Поскольку все группы когомологий $H^1(K_v, F)$ конечны (теорема 6.14), то образ $\psi_T(W_1)$ также конечен, и поэтому существует такая конечно порожденная подгруппа $\Gamma \subset \subset G_K \cap W_1$, что

$$\delta_T(\psi_K(\Gamma)) = \psi_T(W_1). \tag{12}$$

Ясно, что $\Gamma \subset G^L_{\mathcal{O}(V \cup V^K_\infty)}$ для некоторого конечного подмножества $V \subset V^K_f$, не пересекающегося с T. Определим теперь искомую решетку $M \subset K^r$ ее локализациями следующим образом:

$$M_v = \begin{cases} L_v, & v \notin V \cup S, \\ N_v, & v \in V, \\ J_v, & v \in S, \end{cases} \tag{13}$$

где N_v — решетка из леммы 3, а компоненты J_v подобраны таким образом, чтобы обеспечить свободу решетки M (см. предложение 3). Покажем, что $\mathrm{cl}(G^M) = 1$. Из одноклассности L получаем равенство $\psi_A(G_A) = \psi_A(G^L_{A(\infty)} G_K)$, и поэтому в силу предложения 8 достаточно установить включение $\psi_A(G^L_{A(\infty)}) \subset \subset \psi_A(G^M_{A(\infty)} G_K)$. Так как $M_v = L_v$ для $v \notin V \cup S$ и $\psi_{K_v}\left(G^{L_v}_{\mathcal{O}_v}\right) \subset \subset \psi_{K_v}\left(G^{M_v}_{\mathcal{O}_v}\right) = \psi_{K_v}\left(G_{K_v}\right)$ для $v \in V$, то в доказательстве нуждается лишь включение $\Phi \subset \psi_A(G^M_{A(\infty)} G_K)$, где Φ есть произведение $\prod_{v \in S} \psi_{K_v}\left(G^{L_v}_{\mathcal{O}_v}\right)$, естественным образом вложенное в $\psi_A(G_A)$. Из (12) вытекает, что для любого $x \in \Phi$ найдется $\gamma \in \Gamma$ со свойством $\delta_S(\psi_K(\gamma)) = x$. Тогда из рассмотрения локальных компонент и (13) легко получается, что $x\psi_A(\gamma^{-1}) \in \psi_A(G^M_{A(\infty)})$ и, следовательно, $x = x(\psi_A(\gamma^{-1}))\psi_A(\gamma) \in \psi_A(G^M_{A(\infty)} G_K)$, что и требовалось. Чтобы вычислить $\delta_{\overline{S}}(\psi_K(G^M_{\mathcal{O}}))$, нужно, согласно предложению 10, взять образ при проекции $p_{\overline{S}}$ группы $\psi_A(G^M_{\mathcal{O}}) = = \psi_A(G_K) \cap \psi_A(G^M_{A(\infty)})$. Если обозначить через Δ ядро ограничения δ_S на $\psi_K(\Gamma)$, то из (12) вытекает, что

$$\delta_{\overline{S}}(\Delta) = \prod_{v \in \overline{S}} \psi_{K_v}\left(G^{L_v}_{\mathcal{O}_v}\right) = \prod_{v \in \overline{S}} H^1\left(K_v^{\text{нр}}/K_v, F\right).$$

С другой стороны, используя (13), получаем, что $\delta(\Delta) \subset \psi_A(G_K) \cap \cap \psi_A\left(G^M_{A(\infty)}\right)$, откуда $\delta_{\overline{S}}\left(\psi_K\left(G^M_{\mathcal{O}}\right)\right) \supset \prod_{v \in \overline{S}} H^1\left(K_v^{\text{нр}}/K_v, F\right)$. Обратное включение очевидно, ибо $G^M_{\mathcal{O}} \subset G^{M_v}_{\mathcal{O}_v} = G^{L_v}_{\mathcal{O}_v}$ для всех $v \in \overline{S}$. Лемма 4 доказана.

Отметим, что до сих пор мы нигде не пользовались цикличностью фундаментальной группы F, поэтому все построения и результаты остаются справедливыми и в общем случае.

Продолжаем доказательство теоремы 5. Поскольку $F = F_P$, то $H^1(P, F) = \mathrm{Hom}(\mathrm{Gal}(\bar{P}/P), F)$, и мы имеем возможность рассмотреть сквозное отображение

$$\theta\colon H^1(K, F) \to H^1(P, F) = \mathrm{Hom}(\mathrm{Gal}(\bar{P}/P), F).$$

Обозначим через H пересечение ядер всех гомоморфизмов $\chi \in \theta(\psi_K(G_{\mathfrak{O}}^M))$. Поскольку группа $E = \psi_K(G_{\mathfrak{O}}^M)$ конечна (предложение 10), то H — замкнутый нормальный делитель в $\mathrm{Gal}(\bar{P}/P)$ конечного индекса. Утверждается, что H на самом деле является нормальным делителем в $\mathrm{Gal}(\bar{K}/K)$. Действительно, если $\chi \in \theta(\psi_K(G_{\mathfrak{O}}^M))$, $h \in \mathrm{Ker}\,\chi$ и $g \in \mathrm{Gal}(\bar{K}/K)$, то

$$\chi(g^{-1}hg) = \chi(g^{-1})\, g^{-1}(\chi(hg)) = \chi(g^{-1})\, g^{-1}(\chi(h)\, h\chi(g)) = \\ = \chi(g^{-1})\, g^{-1}(\chi(g)) = \chi(gg^{-1}) = 1,$$

ибо χ является коциклом на всей группе $\mathrm{Gal}(\bar{K}/K)$, и h, будучи элементом из $\mathrm{Gal}(\bar{P}/P)$, действует тривиально на F. Обозначим через C конечное расширение Галуа поля K, отвечающее H. (Его можно охарактеризовать как минимальное расширение Галуа поля K, содержащее P и такое, что $E \subset H^1(C/K, F)$.) Таким образом, гомоморфизм $\delta_{\bar{S}}\colon E \to \prod_{i=1}^{l} H^1(K_{\bar{v}_i}, F)$ пропускается через группу $H^1(C/K, F)$. Из (11) теперь вытекает неразветвленность всех расширений $C_{\bar{v}_i}/K_{\bar{v}_i}$, $i = 1, \ldots, l$. Кроме того, по построению $F = F_P$ и $P \subset K_{\bar{v}_i}$, откуда

$$H^1\left(K_{\bar{v}_i}^{\text{нр}}/K_{\bar{v}_i}, F\right) = \mathrm{Hom}(\hat{\mathbb{Z}}, F) \simeq F,$$

причем сквозное отображение

$$\alpha\colon H^1(C/K, F) \to \prod_{i=1}^{l} H^1(C_{\bar{v}_i}/K_{\bar{v}_i}, F) \to \prod_{i=1}^{l} H^1\left(K_{\bar{v}_i}^{\text{нр}}/K_{\bar{v}_i}, F\right) \simeq F^l$$

задается формулой

$$\chi \xrightarrow{\alpha} (\chi(\sigma_1), \ldots, \chi(\sigma_l)),$$

где σ_i — автоморфизм Фробениуса расширения $C_{\bar{v}_i}/K_{\bar{v}_i}$, рассматриваемый как элемент группы $\mathrm{Gal}(C/K)$ (см. § 1.1). По теореме плотности Чеботарева можно вне любого конечного множества нормирований найти такие $v_1, \ldots, v_l \in V_f^K$, что расширение C_{v_i}/K_{v_i} неразветвлено и автоморфизм Фробениуса $\mathrm{Fr}(C_{v_i}/K_{v_i})$ есть $\tau_i = \sigma_i^{f/[B_i]}$ для $i = 1, \ldots, l$ (отметим, что $[B_i]$ делит f,

ибо по условию экспонента B есть f). В частности, можно считать, что $\psi_{K_{v_i}}\left(G_{\mathcal{O}_{v_i}}^{M_{v_i}}\right)=H^1\left(K_{v_i}^{\text{нр}}/K_{v_i},\ F\right)$ для любого i, и в пространстве $K_{v_i}^r$ имеется решетка R_{v_i} со свойством, указанным в формулировке теоремы 5. (Отметим, что по построению $P\subset K_{\bar{v}_i}$, и поэтому σ_i имеет тривиальное ограничение на P; следовательно, ограничение τ_i на P также тривиально, и значит, $P\subset K_{v_i}$.) Решетку $L(B)$ определим следующим образом:

$$L(B)_v=\begin{cases} M_v, & v\notin\{v_1,\ \ldots,\ v_l\},\\ R_v, & v\in\{v_1,\ \ldots,\ v_l\}.\end{cases}$$

Поскольку для любого i пополнение K_{v_i} содержит гильбертово поле классов K и решетка M свободна, то решетка $L(B)$ также свободна (предложение 3).

Лемма 5. $\mathcal{G}\mathrm{cl}\,(G^{L(B)})\simeq B$.

Доказательство. Воспользуемся предложением 10. В нашей ситуации установленный там изоморфизм (9) принимает вид

$$\mathcal{G}\mathrm{cl}\,(G^{L(B)})\simeq\prod_{i=1}^{l}\psi_{K_{v_i}}\left(G_{\mathcal{O}_{v_i}}^{M_{v_i}}\right)\Big/\delta_S(E),$$

где $S=\{v_1,\ \ldots,\ v_l\}$. $\left(\text{Напомним, что по условию } \psi_{K_{v_i}}\left(G_{\mathcal{O}_{v_i}}^{R_{v_i}}\right)=1.\right)$ По построению $\psi_{K_{v_i}}\left(G_{\mathcal{O}_{v_i}}^{M_{v_i}}\right)=H^1\left(K_{v_i}^{\text{нр}}/K_{v_i},F\right)$, причем гомоморфизм $\delta_S\colon E\to\prod_{i=1}^{l}H^1(K_{v_i},F)$ пропускается через группу $H^1(C/K,\ F)$, а сквозной гомоморфизм

$$\beta\colon\ H^1(C/K,\ F)\to\prod_{i=1}^{l}H^1\left(K_{v_i}^{\text{нр}}/K_{v_i},\ F\right)\simeq F^l$$

задается формулой

$$\chi\overset{\beta}{\longmapsto}(\chi(\tau_1),\ \ldots,\ \chi(\tau_l)).$$

Поскольку $\alpha(E)=F^l$ и $\tau_i=\sigma_i^{f/[B_i]}$, то

$$\delta_S(E)=\beta(E)=\langle h^{f/[B_1]}\rangle\times\ \ldots\ \times\langle h^{f/[B_l]}\rangle,$$

где h — образующая группы F (учесть, что σ_i действует тривиально на F, и, следовательно, ограничение $\chi|_{\langle\sigma_i\rangle}$ является гомоморфизмом). Отсюда $\mathcal{G}\mathrm{cl}\,(G^{L(B)})\simeq\prod_{i=1}^{l}B_i=B$, что и требовалось.

Утверждение о том, что на решетках $L\subset K^r$ в качестве чисел классов реализуются все числа вида $m=p_1^{\beta_1}\ \ldots\ p_s^{\beta_s}$, вытекает из уже доказанного факта о реализуемости в качестве

группы классов любой конечной абелевой группы экспоненты f и того замечания, что всегда можно найти группу порядка m и экспоненты f. Таким образом, нам осталось показать, что если G является линейной группой степени n, то в размерности $r=2n$ для почти всех $v \in V_f^K$ существует решетка $R_v \subset K_v^r$ со свойством $\psi_{K_v}\left(G_{\mathcal{O}_v}^{R_v}\right)=1$. Для этого используется

Предложение 11. *Пусть $H=\boldsymbol{GL}_n$ и $\varphi\colon H \to \boldsymbol{GL}_{2n}$ — представление, определяемое соответствием*

$$\varphi\colon g \mapsto \begin{bmatrix} g & 0 \\ 0 & E_n \end{bmatrix}.$$

Тогда для любого неархимедова $v \in V_f^K$ и любого целого $t>0$ существует такая решетка $L_v(t) \subset K_v^{2n}$, что $H_{\mathcal{O}_v}^{L_v(t)}=\varphi\left(GL_n\left(\mathcal{O}_v, \mathfrak{p}_v^t\right)\right)$.

Доказательство полностью аналогично доказательству предложения 4.3.

Таким образом, если G — линейная группа степени n, то для любого $v \in V_f^K$ в пространстве K_v^{2n} всегда существует такая решетка L_v, что $G_{\mathcal{O}_v}^{L_v}=G_{\mathcal{O}_v}(\mathfrak{p}_v)$. Поэтому завершает доказательство теоремы 5 следующая

Лемма 6. *Если $v([F])=0$, то $\psi_{K_v}\left(G_{\mathcal{O}_v}(\mathfrak{p}_v)\right)=1$.*

Доказательство. Ядро гомоморфизма $\psi_{K_v}\colon G_{K_v} \to H^1(K_v, F)$ совпадает с $\pi_{K_v}\left(\widetilde{G}_{K_v}\right)$, т. е. является открытой подгруппой. Поэтому ψ_{K_v} оказывается непрерывным, если наделить $H^1(K_v, F)$ дискретной топологией. Отсюда следует, что $\Gamma=\psi_{K_v}\left(G_{\mathcal{O}_v}(\mathfrak{p}_v)\right)$ является дискретной про-p-группой, т. е. конечной p-группой. С другой стороны, $\Gamma \subset H^1(K_v, F)$, а последняя группа является группой экспоненты $f=[F]$. Так как $v(f)=0$, то $(p, f)=1$, и, значит, $\Gamma=\{1\}$, что и требовалось.

Теорема 5 гарантирует, что все априори возможные числа классов полупростой K-группы G некомпактного типа и степени n с циклической фундаментальной группой F реализуются уже на решетках в пространстве K^{2n}. Однако в ряде случаев удается построить искомые решетки уже в размерности n, что приводит к интересным арифметическим приложениям теоремы реализации, одним из которых является

Теорема 6 (Кнезер [1]). *Пусть f — неопределенная квадратичная форма от $n \geqslant 3$ переменных над кольцом целых $\mathcal{O}$ поля алгебраических чисел K. Тогда число $c(f)$ классов в роде формы f имеет вид 2^d, d — целое $\geqslant 0$. Обратно, для любого целого $d \geqslant 0$ найдется такая квадратичная форма f_d, K-эквивалентная f, что $c(f_d)=2^d$.*

Отметим, что неопределенность формы f над K означает существование такого нормирования $v \in V_\infty^K$, что f представляет нуль в пространстве K_v^n. Последнее условие эквивалентно K_v-изотропности группы $H = \boldsymbol{SO}_n(f)$ (предложение 2.14), и, следовательно, некомпактности группы $\boldsymbol{SO}_n(f)_{K_v}$. Отсюда легко получить, что при $n \geqslant 3$ форма f является неопределенной в том и только том случае, если группа H имеет некомпактный тип. Далее, с учетом предложения 4 утверждение теоремы 6 можно переформулировать следующим образом: в условиях теоремы для любой решетки $L \subset K^n$ число классов $\mathrm{cl}(G^L)$, где $G = \boldsymbol{O}_n(f)$, имеет вид 2^d, и для любого целого $d \geqslant 0$ найдется такая свободная решетка $L(d)$, что $\mathrm{cl}(G^{L(d)}) = 2^d$. К сожалению, группа G не является связной, и к ней нельзя непосредственно применить теорему 5. Поэтому здесь мы докажем аналогичное утверждение для группы $H = \boldsymbol{SO}_n(f)$. Случай группы $G = \boldsymbol{O}_n(f)$ разбирается по той же схеме с использованием того факта, что универсальное накрытие $\pi\colon \tilde{H} \to H$ группы H продолжается до накрытия группы $\tilde{G}$, т. е. существует такая группа $\tilde{G}$ и морфизм $\varphi\colon \tilde{G} \to G$, что следующая диаграмма

$$\begin{array}{ccccccccc} 1 & \to & F & \to & \tilde{H} & \xrightarrow{\pi} & H & \to & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \to & F & \to & \tilde{G} & \xrightarrow{\varphi} & G & \to & 1 \end{array} \tag{14}$$

коммутативна и имеет точные строки. Детали рассуждений мы оставляем читателю в качестве упражнения (см. ниже).

Итак, исследуем числа классов группы $H = \boldsymbol{SO}_n(f)$. Поскольку универсальное накрытие группы H в данном случае имеет вид $\pi\colon \tilde{H} = \boldsymbol{Spin}_n(f) \to \boldsymbol{SO}_n(f) = H$, и, значит, фундаментальной группой F является $\{\pm 1\}$, то число классов $\mathrm{cl}(H)$ всегда имеет вид 2^d (следствие из предложения 8). Чтобы получить все степени двойки в качестве чисел классов, воспользуемся следующей конструкцией решеток в квадратичном пространстве.

Предложение 12. *Пусть форма f имеет в базисе $e = (e_1, \ldots, e_n)$ пространства K^n вид $f = \mathfrak{f}_1 x_1^2 + \ldots + \mathfrak{f}_n x_n^2$. Для $v \in V_f^K$ обозначим через M_v $\mathcal{O}_v$-решетку с базисом $e_1, \pi_v e_2, \ldots, \pi_v^{n-1} e_n$, где π_v — униформизующий элемент. Тогда если $v(\mathfrak{f}_i) = 0$ для всех $i = 1, \ldots, n$, то*

$$G_{\mathcal{O}_v}^{M_v} = \Gamma B,$$

где

$$\Gamma = \Gamma(e) = \{x \in G \mid x(e_i) = \pm e_i,\ i = 1, \ldots, n\},$$
$$B = \{x = (x_{ij}) \in G_{\mathcal{O}_v}(\mathfrak{p}_v) \mid x_{ij} \in \mathfrak{p}_v^{|i-j|},\ i, j = 1, \ldots, n\}.$$

(*Матричная запись рассматривается относительно базиса* e.) *Если дополнительно* $v(2)=0$, *то* $H_{\mathcal{O}_v}^{M_v}=(\Gamma\cap H)(B\cap H)$.

Доказательство. Пусть $x\in G_{\mathcal{O}_v}^{M_v}$ и $x=(x_{ij})$ в базисе $e_1,\ldots,e_n$. Тогда

$$x(\pi_v^{j-1}e_j)=\sum_{i=1}^{n}\pi_v^{j-i}x_{ij}(\pi_v^{i-1}e_i) \tag{15}$$

для всех $j=1,\ldots,n$. Поэтому $x_{ij}\in\mathfrak{p}_v^{i-j}$ при $i\geqslant j$. Но $x\in G$, т. е. ${}^txFx=F$, где $F=\operatorname{diag}(f_1,\ldots,f_n)$ — матрица формы f. Отсюда получаем матричное соотношение ${}^tx=Fx^{-1}F^{-1}$, которое означает, что $x_{ij}=f_if_j^{-1}y_{ij}$, где $y=(y_{ij})=x^{-1}$. Так как $y\in G_{\mathcal{O}_v}^{M_v}$ и, следовательно, $y_{ij}\in\mathfrak{p}_v^{i-j}$ при $i\geqslant j$, то из условия $v(f_i)=0$, $i=1,\ldots,n$, вытекает, что $x_{ij}\in\mathfrak{p}_v^{|i-j|}$ для всех i, j. Далее, еще раз используя соотношение ${}^txFx=F$, получаем, что $\sum_{i=1}^{n}f_ix_{ij}^2=f_j$ для любого $j=1,\ldots,n$, откуда $x_{jj}^2\equiv 1\pmod{\mathfrak{p}_v}$, или $x_{jj}\equiv\pm 1\pmod{\mathfrak{p}_v}$. Тем самым мы доказали включение $G_{\mathcal{O}_v}^{M_v}\subset\Gamma B$. Обратное включение вытекает из формулы (15), выражающей действие x на элементы базиса $\pi_v^{j-1}e_j$. Пусть теперь $x\in H_{\mathcal{O}_v}^{M_v}$ и $x=yz$, где $y\in\Gamma$, $z\in B$. Тогда $1=\det x=\det y\det z$, причем $\det y=\pm 1$ и $\det z\equiv 1\pmod{\mathfrak{p}_v}$. Если $v(2)=0$, то $-1\not\equiv 1\pmod{\mathfrak{p}_v}$, и, следовательно, $\det y=1$, т. е. $y\in\Gamma\cap H$, $z\in B\cap H$. Предложение 12 доказано.

Будем обозначать через ϕ кограничный морфизм, отвечающий универсальному накрытию $\pi\colon\tilde{H}\to H$ группы H. Пусть P — такое конечное расширение Галуа поля K, что группа $\psi_K(\Gamma\cap H)$ лежит в $H^1(P/K,F)$. Тогда если $P\subset K_v$ и $v(2)=v(f_1)=\ldots=v(f_n)=0$, то для построенной в предложении 12 решетки имеем $\psi_{K_v}\left(H_{\mathcal{O}_v}^{M_v}\right)=\psi_{K_v}(\Gamma\cap H)\,\psi_{K_v}(B\cap H)=1$ в силу леммы 6, ибо $B\cap H\subset H_{\mathcal{O}_v}(\mathfrak{p}_v)$. Тем самым выполняются условия теоремы 5, и поэтому для любого целого $d\geqslant 0$ найдется свободная решетка $L(d)\subset K^n$ со свойством $\operatorname{cl}(H^{L(d)})=2^d$.

Упражнения. Пусть f — невырожденная неопределенная квадратичная форма над K от $n\geqslant 3$ переменных, $G=\boldsymbol{O}_n(f)$, $H=\boldsymbol{SO}_n(f)$.

1) Используя тот факт, что для любого расширения L/K коммутанты групп H_L и G_L совпадают (см. Дьедонне [2], с. 85), и сильную аппроксимационную теорему для H, показать, что главный класс $G_{A(\infty)}G_K$ является подгруппой в G_A и число классов $\operatorname{cl}(G)$ совпадает с индексом $[G_A:G_{A(\infty)}G_K]$. Далее, показать, что если θ — кограничный морфизм, отвечающий накры-

тию φ в (14) (который есть не что иное, как спинорная норма), и θ_A есть ограничение $\prod_v \theta_{K_v}$ на G_A, то $\mathrm{cl}(G) = [\theta_A(G_A) : \theta_A(G_{A(\infty)}G_K)]$. (Имитировать доказательство предложения 8.) Отсюда следует, что $\mathrm{cl}(G)$ всегда имеет вид 2^d.

2) Доказать, что существует эквивалентная f над K форма g с числом классов $c(g) = 1$; другими словами, существует решетка $L \subset K^n$, для которой $\mathrm{cl}(G^L) = 1$. С этой целью установить равенство

$$G_A^L = G_{A(\infty)}^L H_A^L,$$

справедливое для любой решетки $L \subset K^n$, откуда непосредственно вытекает неравенство $\mathrm{cl}(G^L) \leqslant \mathrm{cl}(H^L)$; далее воспользоваться теоремой 4.

3) Имитируя доказательство теоремы 5, доказать теорему 6 (отметим, что в данной ситуации (и вообще, когда $[F] = p$ — простое число) этап доказательства, заключенный в лемме 4 и связанный с построением специальной одноклассной решетки, можно опустить и начинать дальнейшие построения с произвольной одноклассной решетки.)

4) Установить следующую связь между $\mathrm{cl}(G^L)$ и $\mathrm{cl}(H^L)$:

$$\mathrm{cl}(G^L) = \mathrm{cl}(H^L)\,[G_O^L : H_O^L]/2.$$

Отсюда следует, что $\mathrm{cl}(G^L)$ есть $\mathrm{cl}(H^L)$ либо $\mathrm{cl}(H^L)/2$, причем если $[G_O^L : H_O^L] = 2$ (в частности, если n нечетно), то $\mathrm{cl}(G^L) = \mathrm{cl}(H^L)$. Построить для любого целого $d \geqslant 0$ такую решетку $L(d) \subset K^n$, что $\mathrm{cl}(H^{L(d)}) = 2^d$ и $[G_O^{L(d)} : H_O^{L(d)}] = 2$, и тем самым дать другое доказательство теоремы Кнезера.

Приведем еще один пример ситуации классического типа, в которой применение теоремы 5 позволяет получать полное описание возникающих чисел классов. Это задача о вычислении **числа классов в роде решеток на полной матричной алгебре** относительно сопряженности. Две решетки $L_1, L_2 \subset M_n(K)$ называются принадлежащими одному роду, если их локализации L_{1v} и L_{2v} сопряжены при помощи матрицы из $GL_n(K_v)$ для всех неархимедовых нормирований поля K, и одному классу, если они сопряжены при помощи матрицы из $GL_n(K)$. Каким может быть число $c(L)$ классов в роде произвольной решетки $L \subset M_n(K)$? Исчерпывающий ответ на этот вопрос дает

Предложение 13. *Пусть $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ — каноническое разложение числа n. Тогда для любой решетки $L \subset M_n(K)$ число $c(L)$ имеет вид $p_1^{\beta_1} \ldots p_r^{\beta_r}$, и обратно, для любого числа $p_1^{\beta_1} \ldots p_r^{\beta_r}$ существует такая решетка $L(\beta_1, \ldots, \beta_r) \subset M_n(K)$, что $c(L(\beta_1, \ldots, \beta_r)) = p_1^{\beta_1} \ldots p_r^{\beta_r}$.*

Доказательство. Действие $\boldsymbol{GL}_n$ на $W=\boldsymbol{M}_n$ посредством сопряжения индуцирует точное представление группы $G=\boldsymbol{PSL}_n$ в $\boldsymbol{GL}(W)=\boldsymbol{GL}_{n^2}$. Обозначим через φ: $\boldsymbol{GL}_n\to G$ возникающий при этом морфизм алгебраических групп. Так как $\operatorname{Ker}\varphi\simeq\boldsymbol{G}_m$, то для любого расширения P/K из точной последовательности $GL_n(P)\xrightarrow{\varphi}G_P\to H^1(P,\operatorname{Ker}\varphi)=1$ получаем, что $\varphi(GL_n(P))=G_P$; другими словами, преобразования из G_P реализуются как сопряжение при помощи матриц из $GL_n(P)$. Применяя теперь предложение 7, получаем, что в данной ситуации $c(L)=\operatorname{cl}(G^L)$ для любой решетки $L\subset M_n(K)$. Таким образом, задача вычисления $c(L)$ свелась к подсчету числа классов для проективной группы. Универсальное накрытие π группы G получается ограничением φ на группу $\boldsymbol{SL}_n$, поэтому $\operatorname{Ker}\pi$ — циклическая группа порядка n, и можно воспользоваться теоремой 8.5. Для ее применения нужно указать конструкцию решеток $R_v\subset M_n(K_v)$ со свойством $\psi_{K_v}\left(G_{\mathcal{O}_v}^{R_v}\right)=1$, где ψ — когранничный морфизм, отвечающий накрытию π. С учетом леммы 6 требуемую конструкцию дает

Лемма 7. *Существует такое конечное подмножество $S\subset V_f^K$, что для $v\in V_f^K\setminus S$ найдется решетка $R_v\subset W_{K_v}$ со свойством: $G_{\mathcal{O}_v}^{R_v}\subset G_{\mathcal{O}_v}^{L_v}(\mathfrak{p}_v)$, где L — решетка, натянутая на стандартный базис e_{ij} матричной алгебры.*

Доказательство. Рассмотрим квадратичную форму f на W, задаваемую формулой $f(x)=\operatorname{tr}(x^2)$, где tr обозначает след матрицы. Нетрудно видеть, что соответствующая билинейная форма имеет вид $b(x,y)=\operatorname{tr}(xy)$, причем для $x=(x_{ij})$ имеем $b(x,e_{ij})=x_{ij}$. Последнее равенство показывает, что форма f является невырожденной. Обозначим через W_0 подпространство в W, состоящее из матриц со следом 0, W_1 — подпространство скалярных матриц. Тогда, очевидно, W является ортогональной прямой суммой пространств W_0 и W_1. Отсюда следует, что ограничение f_0 формы f на W_0 также невырожденно. Пусть $w_1, w_2, \ldots, w_m$ $(m=n^2-1)$ — базис пространства W_{0K}, в котором форма f_0 имеет канонический вид $f_0=a_1x_1^2+\ldots+a_mx_m^2$, и пусть w_{m+1} — ненулевой вектор из W_{1K}. Обозначим через M решетку с базисом $w_1, w_2, \ldots, w_{m+1}$ и возьмем в качестве исключительного подмножества S объединение $S_1\cup S_2$, где $S_1=\{v\in V_f^K\mid L_v\neq M_v\}$, $S_2=\{v\in V_f^K\mid v(a_i)\neq 0$ для некоторого $i=1,\ldots,m\}$.

Предположим теперь, что $v\in V_f^K\setminus S$. Тогда $L_v=M_v$, так что $G_{\mathcal{O}_v}^{L_v}=G_{\mathcal{O}_v}^{M_v}$ и $G_{\mathcal{O}_v}^{L_v}(\mathfrak{p}_v)=G_{\mathcal{O}_v}^{M_v}(\mathfrak{p}_v)$. Покажем, что в качестве искомой решетки R_v можно взять $\mathcal{O}_v$-решетку с базисом w_1+

$+\pi_v^{-m}w_{m+1}, \ldots, \pi_v^{(j-1)}w_j + \pi_v^{(j-m-1)}w_{m+1}, \ldots, \pi_v^{(m-1)}w_m + \pi_v^{-1}w_{m+1}$, w_{m+1}, где π_v — униформизующий элемент. Пусть $x \in G_{\mathcal{O}_v}^{R_v}$ и $x = (x_{ij})$ в базисе $w_1, w_2, \ldots, w_{m+1}$. В силу инвариантности следа при сопряжении, пространство W_0 и форма f_0 инвариантны относительно G; кроме того, на W_1 группа G действует тривиально. Отсюда следует, что матрица x имеет вид $x = \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix}$, где $y = (y_{ij})$ — матрица степени m, ортогональная относительно формы f, и достаточно показать, что $y \in GL_m(\mathcal{O}_v, \mathfrak{p}_v)$ в базисе $w_1, \ldots, w_m$. Имеем

$$x\left(\pi_v^{(j-1)}w_j + \pi_v^{(j-m-1)}w_{m+1}\right) = \pi_v^{(j-1)}\sum_{i=1}^{m} y_{ij}w_i + \pi_v^{(j-m-1)}w_{m+1} =$$

$$= \sum_{i=1}^{m} \alpha_{ij}\left(\pi_v^{(i-1)}w_i + \pi_v^{(i-m-1)}w_{m+1}\right) + \alpha_{m+1,\,j}w_{m+1},$$

откуда

$$y_{ij} = \pi_v^{(i-j)}\alpha_{ij}, \tag{16}$$

$$y_{jj} = 1 - \pi_v^{(m+1-j)}\alpha_{m+1,\,j} - \sum_{i \neq j} y_{ij} \qquad (i, j = 1, \ldots, m). \tag{17}$$

Поскольку $\alpha_{ij} \in \mathcal{O}_v$, то из (16), ортогональности матрицы y относительно формы f_0 и условия $v \notin S_2$, как и при доказательстве предложения 12, получаем, что $y_{ij} \in \mathfrak{p}_v^{|i-j|}$ для всех i, j. Тогда, обращаясь к (17), находим, что $y_{jj} \equiv 1 \pmod{\mathfrak{p}_v}$. Доказательство леммы 7 и предложения 13 завершено.

Задача о числе классов в роде решетки в полной матричной алгебре относительно сопряженности допускает следующее естественное обобщение. Пусть G — простая алгебраическая K-группа присоединенного типа. Тогда присоединенное действие группы G на своей алгебре Ли $\mathfrak{g}$ индуцирует точное K-определенное представление $G \to \mathbf{GL}(\mathfrak{g})$ и можно задать вопрос, какие значения принимает число классов $\mathrm{cl}(G^L)$ на всевозможных решетках $L \subset \mathfrak{g}_K$? (Поясним, что исследованная нами выше задача является частным случаем этого вопроса применительно к группе $G = \boldsymbol{PSL}_n$, ибо введенное при доказательстве леммы 7 пространство W_0 в действительности совпадает с алгеброй Ли $L(G)$.) Развитые нами методы позволяют ответить и на этот вопрос.

Предложение 14. *Пусть G — простая присоединенная алгебраическая K-группа некомпактного типа, отличная от D_{2n}. Предположим, что G реализована как группа внутренних автоморфизмов своей алгебры Ли $\mathfrak{g}$, и пусть $f = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$ — показатель соответствующей фундаментальной группы F. Тогда для любой конечной абелевой группы B экспоненты f найдется*

такая решетка $L(B)\subset\mathfrak{g}_K$, *что* $\mathcal{G}\mathrm{cl}\left(G^{L(B)}\right)\simeq B$. *В частности, для любого числа вида* $p_1^{\beta_1}\ldots p_s^{\beta_s}$ *найдется решетка* $L(\beta_1,\ldots,\beta_s)\subset\mathfrak{g}_K$ *с числом классов* $\mathrm{cl}\left(G^{L(\beta_1,\ldots,\beta_s)}\right)=p_1^{\beta_1}\ldots p_s^{\beta_s}$.

Доказательство. У всех простых алгебраических групп типа, отличного от D_{2n}, фундаментальная группа F является циклической, поэтому в силу теоремы 5 нам достаточно указать конструкцию решеток $R_v\subset\mathfrak{g}_{K_v}$, для которых $\psi_{K_v}\left(G_{\mathcal{O}_v}^{R_v}\right)=1$. С этой целью рассмотрим форму Киллинга h на $\mathfrak{g}$, которая является невырожденной K-определенной квадратичной формой на $\mathfrak{g}$, инвариантной относительно действия группы G. Тогда можно воспользоваться следующим утверждением.

Лемма 8. *Пусть* $G\subset\boldsymbol{GL}_n$ — *K-определенная алгебраическая группа такая, что* $G\subset\boldsymbol{O}_n(h)$ *для подходящей невырожденной K-определенной квадратичной формы h. Предположим, что в базисе* $e=(e_1,\ldots,e_n)$ *пространства* K^n *форма h имеет канонический вид* $h=h_1x_1^2+\ldots+h_nx_n^2$, *и для любого* $v\in V_f^K$ *обозначим через* R_v $\mathcal{O}_v$*-решетку с базисом* $e_1,\pi_ve_2,\ldots,\pi_v^{n-1}e_n$, *где* π_v — *униформизующий элемент. Тогда для почти всех* $v\in V_f^K$ *имеем*

$$G_{\mathcal{O}_v}^{R_v}=\Phi C, \tag{18}$$

где

$$\Phi=\{x\in G\mid x(e_i)=\pm e_i,\quad i=1,\ldots,n\},$$
$$C=\left\{x=(x_{ij})\in G_{\mathcal{O}_v}(\mathfrak{p}_v)\mid x_{ij}\in\mathfrak{p}_v^{|i-j|},\quad i,j=1,\ldots,n\right\}.$$

Доказательство. Имеем $G_{\mathcal{O}_v}^{R_v}=G\cap\boldsymbol{O}_n(h)_{\mathcal{O}_v}^{R_v}$, причем $\boldsymbol{O}_n(h)_{\mathcal{O}_v}^{R_v}=\Gamma B$ для почти всех v в обозначениях предложения 12. Легко видеть, что $\Phi=G\cap\Gamma$, $C=G\cap B$, и поэтому для доказательства (18) нам надо убедиться в справедливости равенства

$$G\cap(\Gamma B)=(G\cap\Gamma)(G\cap B) \tag{19}$$

для почти всех $v\in V_f^K$. Положим $\Delta=\Gamma\setminus\Phi$. Тогда замкнутые по Зарисскому множества G и Δ не пересекаются, поэтому для почти всех v не пересекаются их редукции по модулю v (лемма 3.12), т. е.

$$G_{\mathcal{O}_v}GL_n(\mathcal{O}_v,\mathfrak{p}_v)\cap\Delta GL_n(\mathcal{O}_v,\mathfrak{p}_v)=\varnothing.$$

В частности, группа G не может пересекаться с ΔB, что и дает (19). Лемма 8 доказана.

Доказательство предложения 14 завершается уже стандартным для нас образом. Рассмотрим такое конечное расширение Галуа P/K, что $\psi_K(\Phi)\subset H^1(P/K,F)$. Тогда для почти всех v

со свойством $P \subset K_v$ в силу лемм 6 и 8 имеем

$$\psi_{K_v}\left(G^{R_v}_{G_v}\right) = \psi_{K_v}(\Phi)\,\psi_{K_v}(C) = 1,$$

что и требовалось.

Утверждение предложения 14 сохраняет силу и для групп типа D_{2n}, что легко получается из доказательства общего случая теоремы 3 о реализации (см. Платонов, Бондаренко, Рапинчук [3]).

Характерной особенностью доказательства теоремы 3 является то, что приводимые в нем вычисления чисел классов носят общий характер, в том смысле, что они не связаны со специально сконструированным представлением φ: $G \to \boldsymbol{GL}_d$ и применимы всякий раз, когда в пространстве представления имеются соответствующие решетки. С другой стороны, вопрос о построении таких решеток для произвольного точного представления остается пока открытым. Таким образом, возникает

Проблема. *Пусть* φ: $G \to \boldsymbol{GL}_d$ — *произвольное* K-*определенное представление полупростой* K-*определенной группы* G *некомпактного типа. Верно ли, что любая конечная абелева группа* B *экспоненты* f, *где* f — *показатель фундаментальной группы* F *группы* G, *может быть получена как группа классов* $\mathcal{G}\mathrm{cl}\,(G^{L(B)})$ *для подходящей решетки* $L(B) \subset K^d$?

Выше мы показали, что утвердительный ответ имеет место для присоединенных реализаций групп присоединенного типа. Если G — простая присоединенная группа типа B_l, то ответ утвердителен для любой реализации G (доказательство проводится аналогично доказательству предложения 13 с учетом того обстоятельства, что для любого представления ρ: $G \to \boldsymbol{GL}_d$ существует невырожденная G-инвариантная квадратичная форма, см. Бурбаки [4]). По обсуждаемой проблеме практически больше ничего не известно, и ее решение, по-видимому, потребует развития принципиально новых методов построения решеток при помощи теории представлений алгебраических групп. Определенный оптимизм здесь связан со следующим утверждением, которое показывает, что всегда существуют решетки с «малыми» стабилизаторами.

Предложение 15 (Рапинчук). *Пусть* $G \subset \boldsymbol{GL}_n$ — *редуктивная* K-*определенная алгебраическая группа, не являющаяся нормальным делителем в* $\boldsymbol{GL}_n$. *Тогда для любого* $v \in V_f^K$ *существует такая последовательность решеток* $L(i) \subset K_v^n$, *что* $\mu_v\left(G^{L(i)}_{\sigma_v}\right) \xrightarrow[i\to\infty]{} 0$, *где* μ_v — *мера Хаара на группе* G_{K_v}.

Доказательство. Если предположить противное, то найдется такая константа $c > 0$, что $\mu_v\left(G^{L}_{\sigma_v}\right) \geqslant c$ для любой решетки $L \subset K_v^n$. Зафиксируем некоторый базис $e_1, \ldots, e_n$ пространства K^n.

Тогда для решетки $L = x(\mathcal{O}_v e_1 + \ldots + \mathcal{O}_v e_n)$, где $x \in GL_n(K_v)$, имеем $G^L_{\mathcal{O}_v} = x(x^{-1}Gx)_{\mathcal{O}_v} x^{-1}$ (целые точки берутся относительно базиса $e_1, \ldots, e_n$). Покажем, что в нашей ситуации подгруппы $H(x) = x(x^{-1}Gx)_{\mathcal{O}_v} x^{-1}$ $(x \in GL_n(K_v))$ образуют конечное число классов сопряженности относительно G_{K_v}. Действительно, согласно предложению 3.16 любая компактная подгруппа в G_{K_v} содержится в некоторой максимальной компактной подгруппе. С другой стороны, в силу результатов § 3.4 максимальные компактные подгруппы группы G_{K_v} распадаются в конечное число классов сопряженности; пусть $H_1, H_2, \ldots, H_d$ — полная система представителей классов сопряженности максимальных компактных подгрупп в G_{K_v}. Таким образом, для любого $x \in GL_n(K_v)$ найдутся $g \in G_{K_v}$ и индекс $j = 1, \ldots, d$ со свойством $gH(x)g^{-1} \subset H_j$. При этом в силу очевидной оценки $[H_j : gH(x)g^{-1}] = \frac{\mu_v(H_j)}{\mu_v(H(x))} \leqslant \frac{\mu_v(H_j)}{c}$ индекс $[H_j : gH(x)g^{-1}]$ ограничен сверху. Тем самым нам достаточно показать, что H_j имеет лишь конечное число подгрупп данного фиксированного индекса t. Если $[H_j : D] = t$, то $D \supset \varphi_s(H_j)$, где $s = t!$, $\varphi_s(x) = x^s$. Но из предложения 3.3 легко вытекает открытость отображения φ_s в единице; в частности, подгруппа (очевидно, нормальная) $N \subset H_j$, порожденная $\varphi_s(H_j)$, открыта. Отсюда следует, что число подгрупп индекса t в H_j совпадает с числом подгрупп индекса t факторгруппы H_j/N. Остается заметить, что в силу компактности H_j последняя факторгруппа конечна. Зафиксируем такой конечный набор элементов $x_1, \ldots, x_r \in GL_n(K_v)$, что любая подгруппа $H(x)$ сопряжена в G_{K_v} одной из $H(x_i)$, $i = 1, \ldots, r$. Обозначим, далее, через Z централизатор G в $\boldsymbol{GL}_n$ и через P редуктивную подгруппу $ZG \subset \boldsymbol{GL}_n$. Покажем, что факторпространство $GL_n(K_v)/P_{K_v}$ компактно. Для этого достаточно найти такое компактное подмножество $D \subset GL_n(K_v)$, что $GL_n(K_v) = Z_{K_v} G_{K_v} D$. Положим $B_i = \{x \in GL_n(K_v) \mid H(x) = H(x_i)\}$. Тогда, поскольку для $g \in G_{K_v}$ имеем $H(gx) = gH(x)g^{-1}$, то $GL_n(K_v) = \bigcup_{i=1}^{r} G_{K_v} B_i$, и достаточно найти компакты C_i такие, что $B_i \subset Z_{K_v} C_i$. Если $x \in B_i$, то, полагая $y = x^{-1}x_i$, будем иметь

$$y(x_i^{-1}Gx_i)_{\mathcal{O}_v} y^{-1} = (x^{-1}Gx)_{\mathcal{O}_v},$$

т. е. $B_i \subset x_i Y_i^{-1}$, где

$$Y_i = \{y \in GL_n(K_v) \mid y(x_i^{-1}Gx_i)_{\mathcal{O}_v} y^{-1} \subset GL_n(\mathcal{O}_v)\}.$$

Мы покажем, что Y_i имеет вид $Y_i = D_i Z_{\boldsymbol{GL}_n}(x_i^{-1}Gx_i)_{K_v}$ с компактным D_i. Тогда

$$B \subset x_i Y_i^{-1} = x_i x_i^{-1} Z_{K_v} x_i D_i^{-1} = Z_{K_v}(x_i D_i^{-1}),$$

что и требовалось.

Пусть $a_1, \ldots, a_d$ — конечная система топологических образующих группы $(x_i^{-1}Gx_i)_{\mathcal{O}_v}$. Рассмотрим отображение φ: $\boldsymbol{GL}_n \to W = \underbrace{\boldsymbol{GL}_n \times \ldots \times \boldsymbol{GL}_n}_{d}$, $\varphi(g) = (ga_1g^{-1}, \ldots, ga_dg^{-1})$. Тогда, очевидно, $Y_i = \varphi^{-1}(W_{\mathcal{O}_v}) \cap GL_n(K_v)$. Заметим теперь, что, в силу плотности $(x_i^{-1}Gx_i)_{\mathcal{O}_v}$ в $x_i^{-1}Gx_i$ в топологии Зарисского (лемма 3.2), замыкание по Зарисскому подгруппы, порожденной $a_1, \ldots, a_d$, совпадает с $x_iGx_i^{-1}$. В частности, слои отображения φ совпадают со смежными классами по централизатору $Z_i = Z_{\boldsymbol{GL}_n}(x_i^{-1}Gx_i)$. Но, очевидно, Z_i совпадает с алгебраической группой, определяемой мультипликативной группой централизатора в $M_n(K_v)$ K_v-оболочки $K_v\left[(x_i^{-1}Gx_i)_{K_v}\right]$, которая в силу редуктивности G является полупростой K_v-алгеброй. Отсюда вытекает, что $H^1(K_v, Z_i) = 1$, и, следовательно, для $x \in \operatorname{Im}\varphi \cap W_{K_v}$ всегда $\varphi^{-1}(x)_{K_v} \neq \varnothing$. Поэтому $\varphi(Y_i) = \operatorname{Im}\varphi \cap W_{\mathcal{O}_v}$. В силу теоремы 2.16 образ $\operatorname{Im}\varphi$ замкнут в топологии Зарисского, так что $\varphi(Y_i)$ — компакт. Тогда $\varphi(Y_i) = \varphi(D_i)$ для подходящего компакта $D_i \subset GL_n(K_v)$ и $Y_i = D_i(Z_i)_{K_v}$, что и требовалось.

Теперь уже несложно завершить доказательство предложения. Из компактности пространства $GL_n(K_v)/P_{K_v}$ вытекает, что P содержит борелевскую подгруппу B группы $\boldsymbol{GL}_n$ (теорема 3.1), которая, естественно, будет борелевской подгруппой и в P. В силу редуктивности P в ней имеется противоположная B борелевская подгруппа B^-. Ясно, что B^- является противоположной B и относительно группы $\boldsymbol{GL}_n$. Но в силу разложения Брюа произведение B^-B содержит открытое по Зарисскому подмножество в $\boldsymbol{GL}_n$, и, следовательно, B и B^- порождают $\boldsymbol{GL}_n$. Тем самым $P = \boldsymbol{GL}_n$. Вспоминая, что $P = ZG$, где Z — централизатор G, мы видим, что G является нормальным делителем в группе $\boldsymbol{GL}_n$ (т. е. либо содержится в ее центре, либо содержит группу $\boldsymbol{SL}_n$). Полученное противоречие и доказывает предложение.

§ 8.3. Числа классов алгебраических групп компактного типа

Теорема 3 из предыдущего параграфа дает полное описание значений, которые может принимать число классов $\mathrm{cl}(G)$ полупростой K-группы G некомпактного типа. В настоящем

параграфе мы разберем противоположный случай. Наиболее законченные результаты будут получены в ситуации, когда G имеет компактный тип (см. теорему 8), т. е. компактна архимедова часть G_∞ группы аделей. Этот случай наиболее важен с точки зрения приложений, ибо к данному типу относятся ортогональные группы положительно определенных квадратичных форм, и, следовательно, мы получаем результаты о соответствующих числах классов в роде. Однако если не ограничивать степени используемых реализаций, то аналогичные результаты удастся получить для более широкого класса полупростых K-групп G так называемого смешанного типа, что означает наличие K-простой компоненты $G^i \subset G$ с компактной группой G^i_∞.

Теорема 7. *Пусть G — полупростая алгебраическая K-группа смешанного типа и степени n. Тогда для любого натурального r существует такая свободная решетка $M(r) \subset K^{2n}$, что $\mathrm{cl}(G^{M(r)})$ делится на r.*

Доказательство. Зафиксируем некоторую свободную решетку $L \subset K^n$ и в дальнейшем группу $G^L_{A(\infty)}$ будем обозначать просто через $G_{A(\infty)}$. Для любого $v_0 \in V^K_f$ и любой открытой подгруппы $U \subset G_{\mathcal{O}_{v_0}}$ положим

$$G_{A(\infty)}(v_0, U) = \prod_{v \in V^K_\infty} G_{K_v} \times \prod_{\substack{v \in V^K_f \\ v \neq v_0}} G_{\mathcal{O}_v} \times U,$$

и

$$G_{A(\infty)}(v_0) = G_{A(\infty)}\left(v_0, G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})\right),$$

где $G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})$ есть, как обычно, конгруэнц-подгруппа уровня $\mathfrak{p}_{v_0}$. Обозначим через $c(G, v_0, U)$ (соответственно $c(G, v_0)$) число двойных смежных классов $G_{A(\infty)}(v_0, U)\backslash G_A/G_K$ (соответственно $G_{A(\infty)}(v_0)\backslash G_A/G_K$). Вместо теоремы 7 нами будет доказан следующий несколько более точный результат: для любого натурального r существует такое $v_0 \in V^K_f$, что $\tilde{K} \subset K_{v_0}$ и $c(G, v_0)$ делится на r. Теорема 8 очевидным образом вытекает из этого утверждения. В самом деле, из предложения 11 вытекает существование такой решетки $N \subset K^{2n}$, что $N_v = L_v$ для $v \neq v_0$ и $G^{N_{v_0}}_{\mathcal{O}_{v_0}} = G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})$. Тогда, очевидно, $G^N_{A(\infty)} = G_{A(\infty)}(v_0)$; в частности, $\mathrm{cl}(G^N) = c(G, v_0)$ делится на r. С другой стороны, в силу предложения 2 и условия $\tilde{K} \subset K_{v_0}$ решетка N свободна.

Пусть $G_A = \bigcup_{i=1}^{m} G_{A(\infty)} z_i G_K$ — разложение G_A в объединение попарно не пересекающихся двойных смежных классов. Без ограничения общности можно считать, что существует конечное подмножество $S_0 \subset V^K_f$ со свойством: v-компонента $(z_i)_v$ равна 1 для всех $v \notin S_0$ и всех $i = 1, \ldots, m$. Обозначим через $G^{(i)}_{\mathcal{O}}$

пересечение $z_i^{-1}G_{A(\infty)}z_i \cap G_K$. Пусть также $c_i(G, v_0, U)$ (соответственно $c_i(G, v_0)$) — число смежных классов по подгруппам $G_{A(\infty)}(v_0, U)$ (соответственно $G_{A(\infty)}(v_0)$) и G_K, на которые распадается класс $G_{A(\infty)}z_iG_K$.

Лемма 9. *Имеем*

$$c(G, v_0, U) = \sum_{i=1}^{m} c_i(G, v_0, U), \tag{1}$$

причем при $v_0 \in V_f^K \setminus S_0$ *число* $c_i(G, v_0, U)$ *совпадает с числом двойных смежных классов* $U \backslash G_{\mathcal{O}_{v_0}} / G_{\mathcal{O}}^{(i)}$. *В частности, число* $c_i(G, v_0)$ *вычисляется по формуле*

$$c_i(G, v_0) = \left[G_{\mathcal{O}_{v_0}} : G_{\mathcal{O}}^{(i)} G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})\right]. \tag{2}$$

Доказательство. Формула (1) очевидна, поэтому установим справедливость остальных утверждений. Для $\alpha \in G_{\mathcal{O}_{v_0}}$ обозначим через $x^{v_0}(\alpha)$ адель с компонентами

$$x_v = \begin{cases} 1, & v \neq v_0, \\ \alpha, & v = v_0. \end{cases} \tag{3}$$

Тогда

$$G_{A(\infty)}z_iG_K = \bigcup_{\alpha} G_{A(\infty)}(v_0, U)\, x^{v_0}(\alpha)\, z_iG_K,$$

где объединение берется по всем $\alpha \in G_{\mathcal{O}_{v_0}}$. Покажем теперь, что условия

$$G_{A(\infty)}(v_0, U)\, x^{v_0}(\alpha)\, z_iG_K = G_{A(\infty)}(v_0, U)\, x^{v_0}(\beta)\, z_iG_K \tag{4}$$

и

$$U\alpha G_{\mathcal{O}}^{(i)} = U\beta G_{\mathcal{O}}^{(i)} \tag{5}$$

равносильны. Если выполняется (4), то

$$x^{v_0}(\alpha)\, z_i = a x^{v_0}(\beta)\, z_i b \tag{6}$$

для некоторых $a \in G_{A(\infty)}(v_0, U)$, $b \in G_K$. Тогда, очевидно, $b = z_i^{-1}x^{v_0}(\beta^{-1})\, a^{-1}x^{v_0}(\alpha)\, z_i \in z_i^{-1}G_{A(\infty)}z_i$, откуда $b \in G_{\mathcal{O}}^{(i)}$. Проектируя (6) на v_0-компоненту и учитывая, что по построению $(z_i)_{v_0} = 1$, получим $\alpha = a_{v_0}\beta b$, где $a_{v_0} \in U$, т. е. (5). Обратно, если выполнено равенство (5), то $\alpha = c\beta d$, где $c \in U$, $d \in G_{\mathcal{O}}^{(i)}$. Положив $a = x^{v_0}(\alpha)\, z_i d^{-1} z_i^{-1} x^{v_0}(\beta^{-1})$, $b = d$, мы обеспечим выполнение (6), и достаточно установить, что $a \in G(v_0, U)$. Поскольку $d \in G_{\mathcal{O}}^{(i)}$, то по построению $z_i d^{-1} z_i^{-1} \in G_{A(\infty)}$, и, следовательно, $a \in G_{A(\infty)}$. Остается вычислить v_0-компоненту a_{v_0}. Имеем

$$a_{v_0} = \alpha d^{-1}\beta^{-1} = c \in U,$$

ибо $(z_i)_{v_0} = 1$, и требуемое доказано.

Установленная нами равносильность условий (4) и (5), очевидно, дает равенство $c_i(G, U, v_0) = [U \backslash G_{\mathcal{O}_{v_0}} / G_{\mathcal{O}}^{(i)}]$. Для доказательства (2) теперь остается заметить, что в силу нормальности $U = G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})$ в $G_{\mathcal{O}_{v_0}}$ двойной смежный класс $UxG_{\mathcal{O}}^{(i)}$ $(x \in G_{\mathcal{O}_{v_0}})$ совпадает с обычным смежным классом xW по подгруппе $W = G_{\mathcal{O}}^{(i)} G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})$, так что число $c_i(G, v_0)$ совпадает с индексом $[G_{\mathcal{O}_{v_0}} : W]$.

Лемма 9 доказана.

Предложение 16. *Пусть G — полупростая алгебраическая K-группа смешанного типа. Тогда для любого натурального r найдется такое $v_0 \in V_f^K$, что $\tilde{K} \subset K_{v_0}$ и все числа $c_i(G, v_0)$ $(i = 1, \ldots, m)$ делятся на r. В частности, $c(G, v_0)$ делится на r.*

Доказательство. Из определения групп смешанного типа вытекает, что G является почти прямым произведением полупростых групп F и H, причем H имеет компактный тип. Положим $D = G/F$ и обозначим через π: $G \to D$ соответствующий факторморфизм. В силу предложения 6.5 найдется такое конечное подмножество $S_1 \subset V_f^K$, что для $v \in V_f^K \setminus S_1$ морфизм π определен над $\mathcal{O}_v$ и $\pi(G_{\mathcal{O}_v}) = D_{\mathcal{O}_v}$. Тогда $\pi(G_{\mathcal{O}_v}(\mathfrak{p}_v)) \subset D_{\mathcal{O}_v}(\mathfrak{p}_v)$. Поэтому для $v_0 \notin S_0 \cup S_1$ число $c_i(G, v_0)$ делится на индекс $[\pi(G_{\mathcal{O}_{v_0}}) : \pi(G_{\mathcal{O}}^{(i)}) \pi(G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0}))]$, а, значит, и на $[D_{\mathcal{O}_{v_0}} : \pi(G_{\mathcal{O}}^{(i)}) D_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})]$.

Установим теперь конечность всех групп $\pi(G_{\mathcal{O}}^{(i)})$. Из определений вытекает, что

$$\pi(G_{\mathcal{O}}^{(i)}) \subset \pi(z_i)^{-1} \pi(G_{A(\infty)}) \pi(z_i) \cap D_K. \tag{7}$$

Но группа D, будучи изогенной H, имеет компактный тип, откуда без труда вытекает компактность подгруппы $\pi(G_{A(\infty)}) \subset D_A$. С другой стороны, подгруппа $D_K \subset D_A$ дискретна. Поэтому пересечение в (7), будучи одновременно компактным и дискретным, конечно. Обозначим через l наименьшее общее кратное порядков всех групп $\pi(G_{\mathcal{O}}^{(i)})$. Тогда из доказанного вытекает, что для любого $i = 1, \ldots, m$ число $c_i(G, v_0)$ имеет вид $\frac{d_i}{l}[D_{\mathcal{O}_{v_0}} : D_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})]$ с некоторым целым d_i.

Поэтому завершает доказательство предложения 16, а вместе с тем и теоремы 7 следующая

Лемма 10. *Пусть D — нетривиальная редуктивная K-группа, F/K — некоторое конечное расширение. Тогда для любого натурального r существует бесконечное множество таких $v \in V_f^K$, что $F \subset K_v$ и индекс $[D_{\mathcal{O}_v} : D_{\mathcal{O}_v}(\mathfrak{p}_v)]$ делится на r.*

Доказательство. Легко видеть, что группа точек $D_{\bar{K}}$ над алгебраическим замыканием K содержит конечную подгруппу C

порядка r. (Такую подгруппу можно найти, например, рассмотрев произвольный (нетривиальный) тор $T \subset D$ и воспользовавшись изоморфизмом $T_{\overline{K}} \simeq (\overline{K}^*)^{\dim T}$.) Обозначим через P конечное расширение Галуа поля K, содержащее F и такое, что $C \subset G_P$. Из теоремы плотности Чеботарева вытекает бесконечность множества $S = \{v \in V_f^K \mid P \subset K_v\}$, и поэтому найдется бесконечно много таких $v_0 \in S$, что $C \subset D_{\mathcal{O}_{v_0}}$, и ограничение на C отображения редукции по модулю $\mathfrak{p}_{v_0}$ инъективно. В этом случае факторгруппа $D_{\mathcal{O}_{v_0}}/D_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})$ содержит изоморфный образ C, так что индекс $\left[D_{\mathcal{O}_{v_0}} : D_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})\right]$ делится на r. Лемма 10 доказана.

Теорема 7 наглядно показывает, что, в отличие от полупростых групп некомпактного типа, для групп смешанного типа число классов может принимать весьма разнообразные значения. Получить их точное описание представляется малореальным, поэтому в дальнейшем мы сосредоточим внимание не на детализации самой теоремы 7, а на получении ее арифметических приложений. Речь идет об исследовании чисел классов в исходном представлении, что позволяет получить, например, характеризацию чисел классов в роде положительно определенных квадратичных форм. К настоящему времени удалось показать, что утверждение, аналогичное теореме 7, выполняется в исходной размерности n для групп компактного типа.

Теорема 8. *Пусть G — связная линейная алгебраическая K-группа компактного типа и степени n. Тогда для любого натурального r существует такая свободная решетка $L(r) \subset K^n$, что число классов $\mathrm{cl}(G^{L(r)})$ делится на r.*

Для невырожденной n-мерной квадратичной формы f группа $G = \boldsymbol{SO}_n(f)$ относится к компактному типу в том и только том случае, если f для каждого $v \in V_\infty^K$ является K_v-анизотропной (в частности, поле должно быть вполне вещественным). Таким образом, если форма f является положительно определенной над всеми K_v, $v \in V_\infty^K$ (в этом случае говорят, что f просто является положительно определенной), то теорема 8 применима к группе $G = \boldsymbol{SO}_n(f)$. Доказательство теоремы 8 в этом случае без каких-либо изменений проходит и для группы $G = \boldsymbol{O}_n(f)$, так что, учитывая предложение 4, получаем следующий результат (ср. с теоремой 6).

Теорема 9. *Пусть f — положительно определенная квадратичная форма степени $n \geqslant 2$ с коэффициентами из кольца целых $\mathcal{O}$ вполне вещественного поля алгебраических чисел K. Тогда для любого натурального r существует такая форма f_r с коэффициентами из $\mathcal{O}$, которая K-эквивалентна форме f и для которой число $c(f_r)$ классов в роде делится на r.*

Построение локальных компонент искомой решетки $L(r)$ в теореме 8 проводится при помощи леммы 8, возможность применения которой вытекает из следующего утверждения:

Предложение 17. *Пусть G — связная алгебраическая K-группа степени n компактного типа. Тогда существует такая положительно определенная квадратичная форма f с коэффициентами из K от n переменных, что $G \subset \boldsymbol{SO}_n(f)$.*

Доказательство. Пусть W — пространство всех квадратичных форм от n переменных, которое можно отождествить с пространством симметрических $(n \times n)$-матриц $A \in M_n$. Обозначим через $\tilde{W}$ K-определенное подпространство в W, состоящее из матриц, инвариантных относительно группы G_K, т. е. $\tilde{W} = \{A \in W \mid {}^t gAg = A \forall g \in G_K\}$. По условию для любого $v \in V_\infty^K$ группа G_{K_v} компактна, и поэтому каждое пространство $\tilde{W}_{K_v}$ обязательно содержит положительно определенную матрицу (см. § 3.2). Отсюда следует, что подмножество положительно определенных матриц в $\tilde{W}_{K_v}$ является непустым и открытым. Поэтому, используя свойство слабой аппроксимации для $\tilde{W}$, мы можем найти матрицу $F \in \tilde{W}_K$, которая положительно определена относительно любого $v \in V_\infty^K$. Пусть f — соответствующая ей квадратичная форма. Тогда $G_K \subset \boldsymbol{O}_n(f)$. Ввиду связности G, множество G_K плотно в G в топологии Зарисского (теорема 2.2), так что $G \subset \boldsymbol{O}_n(f)$, откуда и следует требуемое утверждение. Предложение 17 доказано.

Опишем схему доказательства теоремы 8. Используя предложение 17, выберем n-мерную положительно определенную G-инвариантную квадратичную форму f. Предположим, что в базисе $e = (e_1, \ldots, e_n)$ пространства K^n форма f имеет канонический вид $f = f_1 x_1^2 + \ldots + f_n x_n^2$. Если для $v_0 \in V_f^K$ имеем $\tilde{K} \subset K_{v_0}$, то существует униформизующий элемент $\pi_{v_0} \in \mathcal{O}$ такой, что $\pi_{v_0} \in U_v$ для $v \neq v_0$, и можно рассмотреть решетку $L(v_0)$ с базисом $e_1, \pi_{v_0} e_2, \ldots, \pi_{v_0}^{(n-1)} e_n$. Тогда для $v \neq v_0$ имеем $L(v_0)_v = L_v$, где L — решетка с базисом $e_1, \ldots, e_n$, а для почти всех v_0 стабилизатор $B(v_0) = G_{\mathcal{O}_{v_0}}^{L(v_0)_{v_0}}$ описывается следующим образом (лемма 8):

$$B(v_0) = \Phi C, \tag{8}$$

где $\Phi = \{x \in G \mid x(e_i) = \pm e_i, \quad i = 1, \ldots, n\}$, $C = \{x = (x_{ij}) \in G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0}) \mid x_{ij} \in \mathfrak{p}_{v_0}^{|i-j|}, i, j = 1, \ldots, n\}$ (матричная запись берется относительно базиса e). Зафиксируем некоторое разложение

$$G_A = \bigcup_{i=1}^{m} G_{A(\infty)}^L z_i G_K, \tag{9}$$

обладающее тем свойством, что $(z_i)_v = 1$ для всех $i = 1, \ldots, m$ и всех v, лежащих вне некоторого конечного подмножества $S_0 \subset V_f^K$. Тогда, используя лемму 9, мы для $v_0 \notin S_0$ получаем следующую формулу для подсчета $\mathrm{cl}\,(G^{L(v_0)})$:

$$\mathrm{cl}\,(G^{L(v_0)}) = \sum_{i=1}^{m} d_i(v_0),$$

где

$$d_i(v_0) = \left[B(v_0)\backslash G^{L_{v_0}}_{\mathcal{O}_{v_0}}/G^{(i)}_{\mathcal{O}}\right], \quad G^{(i)}_{\mathcal{O}} = z_i^{-1} G_{A(\infty)} z_i \cap G_K.$$

До сих пор рассуждения вполне аналогичны доказательству теоремы 7, однако начиная с этого места, начинают проявляться дополнительные сложности. А именно, вычисляя при доказательстве теоремы 7 числа $c_i(G, v_0) = \left[G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})\backslash G_{\mathcal{O}_{v_0}}/G^{(i)}_{\mathcal{O}}\right]$, мы воспользовались нормальностью конгруэнц-подгруппы и свели вычисление числа двойных смежных классов к подсчету некоторого группового индекса. В нашей же ситуации группа $B(v_0)$, вообще говоря, не является нормальной в $G_{\mathcal{O}_{v_0}}$, и поэтому приходится привлекать другие соображения. Один прием состоит в специальном выборе базиса e и разложения (9) таким образом, чтобы соответствующие группы $G^{(i)}_{\mathcal{O}}$ содержались в $\{\pm E_n\}$; тогда снова $d_i(v_0) = \left[G^{L_{v_0}}_{\mathcal{O}_{v_0}} : G^{(i)}_{\mathcal{O}} B(v_0)\right]$, и рассуждения из доказательства теоремы 7 переносятся без каких-либо изменений. Оказывается, этот прием применим всякий раз, когда G — собственная подгруппа в $\boldsymbol{SO}_n(f)$.

Предложение 18. *Пусть G — собственная связная K-определенная подгруппа группы $H = \boldsymbol{SO}_n(f)$. Тогда существует такой ортогональный относительно формы f базис $e = (e_1, \ldots, e_n)$ пространства K^n, что $G \cap \Gamma(e) \subset \{\pm E_n\}$, где*

$$\Gamma(e) = \{x \in \boldsymbol{GL}_n \mid x(e_i) = \pm e_i, \quad i = 1, \ldots, n\}.$$

Доказательство. При $n = 2$ группа H является одномерным тором, так что группа G тривиальна и доказывать нечего. Поэтому в дальнейшем будем считать, что $n > 2$. Зафиксируем некоторый ортогональный относительно f базис $e^0 = (e_1^0, \ldots, e_n^0)$ пространства K^n и положим $\Gamma_0 = \Gamma(e^0)$. Если $h \in H_K$, то для базиса $h(e^0) = (h(e_1^0), \ldots, h(e_n^0))$ имеем $\Gamma(h(e^0)) = h\Gamma_0 h^{-1}$, поэтому для доказательства предложения достаточно установить существование такого $h \in H_K$, что $G \cap (h\Gamma_0 h^{-1}) \subset \{\pm E_n\}$. Предположим, что это невозможно; тогда

$$H_K \subset \bigcup_{\gamma \in \Delta} C(\gamma), \tag{10}$$

где $C(\gamma) = \{h \in H \mid h^{-1}\gamma h \in G\}$, $\Delta = \Gamma_0 \setminus \{\pm E_n\}$. Ясно, что $C(\gamma)$ является замкнутым по Зарисскому подмножеством в H, так

что из (10) и плотности H_K в H (теорема 2.2) вытекает равенство $H = \bigcup_{\gamma \in \Delta} C(\gamma)$. Поэтому в силу связности H имеем $H = C(\gamma)$ для некоторого $\gamma \in \Delta$, т. е. G содержит класс сопряженности $\{h^{-1}\gamma h \mid h \in H\}$. Поэтому требуемое вытекает из следующего утверждения.

Лемма 11. *При $n > 2$ нормальный делитель в H, порожденный любым элементом $\gamma \in \Gamma_0 \setminus \{\pm E_n\}$, совпадает с H.*

Действительно, при $n \neq 4$ любой собственный нормальный делитель H лежит в $\{\pm E_n\}$, поэтому в рассмотрении нуждается лишь случай $n = 4$. Здесь $H = H_1 H_2$ — почти прямое произведение двух групп, изоморфных $\boldsymbol{SL}_2$, с отождествленными центрами. Если предположить, что нормальный делитель N в H, порожденный $\gamma \in \Gamma_0 \setminus \{\pm E_n\}$, является собственным, то либо $N = H_1$, либо $N = H_2$. При изоморфизме $H_i \simeq \boldsymbol{SL}_2$ элемент γ перейдет в $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ (это единственный элемент порядка 2 в $\boldsymbol{SL}_2$!). Но тогда $\gamma = -E_4$ — противоречие. Доказательство леммы 11 и предложения 18 завершено.

Предложение 19. *Пусть G — собственная K-определенная подгруппа группы $\boldsymbol{SO}_n(f)$, где f — положительно определенная квадратичная форма. Существует такой ортогональный относительно f базис $e_1, \ldots, e_n$ пространства K^n и такое разложение*

$$G_A = \bigcup_{i=1}^{n} G^L_{A(\infty)} z_i G_K$$

(L — решетка с базисом $e_1, \ldots, e_n$), что $(z_i)_v = 1$ для всех v вне некоторого конечного подмножества $S_0 \subset V_f^K$ и все группы $G_{\mathcal{O}}^{(i)} = z_i^{-1} G_{A(\infty)} z_i \cap G_K$ лежат в $\{\pm E_n\}$.

Доказательство. Пусть $u = (u_1, \ldots, u_n)$ — ортогональный базис пространства K^n, построенный в предложении 18, M — решетка с базисом u. Зафиксируем некоторое разложение

$$G_A = \bigcup_{j=1}^{r} G^M_{A(\infty)} t_j G_K,$$

в котором $(t_j)_v = 1$ для всех $j = 1, \ldots, r$ и для всех v, лежащих вне некоторого конечного подмножества $S \subset V_f^K$. В силу положительной определенности формы f группа G_∞ компактна, откуда следует конечность всех групп $\overline{G}_{\mathcal{O}}^{(j)} = t_j^{-1} G^M_{A(\infty)} t_j \cap G_K$. Положим $R = \left(\bigcup_{j=1}^{r} \overline{G}_{\mathcal{O}}^{(j)}\right) \setminus \{\pm E_n\}$ и найдем такое конечное подмножество $S_1 \subset V_f^K$, что для $v \in V_f^K \setminus S_1$

$$R \cap \left(\pm G_{\mathcal{O}_v}(\mathfrak{p}_v)\right) = \varnothing.$$

Выберем, далее, $v_0 \in V_f^K \setminus (S \cup S_1)$, обладающее свойствами: $\widetilde{K} \subset K_{v_0}$ и стабилизатор $B(v_0)$ решетки с базисом $u_1, \pi_{v_0}u_2, \ldots, \pi_{v_0}^{(n-1)}u_n$ описывается формулой (8) ($\pi_{v_0} \in \mathcal{O}$ — такой униформизующий элемент, что $\pi_{v_0} \in U_v$ при $v \neq v_0$). Наша цель — показать, что базис $e_1 = u_1$, $e_2 = \pi_{v_0}u_2, \ldots, e_n = \pi_{v_0}^{(n-1)}u_n$ является искомым. Пусть L — решетка с базисом $e_1, \ldots, e_n$. Тогда по построению $L_v = M_v$ для $v \neq v_0$ и $G_{\mathcal{O}_{v_0}}^{L_{v_0}} \subset G_{\mathcal{O}_{v_0}}^{M_{v_0}}$, так что представители всех смежных классов $G_{A(\infty)}^{L} \backslash G_A / G_K$ можно выбрать среди аделей вида $z(j, \alpha) = x^{v_0}(\alpha) t_j$, $\alpha \in G_{\mathcal{O}_{v_0}}^{M_{v_0}}$ (обозначения см. в лемме 9). Отметим, что $(z(j, \alpha))_v = 1$ для $v \notin S_0 = S \cup \{v_0\}$. Поэтому достаточно показать, что для любых j и α справедливо включение

$$G_{\mathcal{O}}^{(j,\alpha)} = z(j, \alpha)^{-1} G_{A(\infty)}^{L} z(j, \alpha) \cap G_K \subset \{\pm E_n\}.$$

Имеем

$$G_{\mathcal{O}}^{(j,\alpha)} = z(j, \alpha)^{-1} G_{A(\infty)}^{L} z(j, \alpha) \cap G_K \subset t_j^{-1} G_{A(\infty)}^{M} t_j \cap G_K = \overline{G}_{\mathcal{O}}^{(j)}.$$

С другой стороны, беря проекцию на v_0-компоненту, получим

$$G_{\mathcal{O}}^{(j,\alpha)} \subset \alpha^{-1} G_{\mathcal{O}_{v_0}}^{L_{v_0}} \alpha,$$

т. е. окончательно

$$G_{\mathcal{O}}^{(j,\alpha)} \subset \overline{G}_{\mathcal{O}}^{(j)} \cap \alpha^{-1} B(v_0) \alpha,$$

где, как мы условились выше, $B(v_0) = G_{\mathcal{O}_{v_0}}^{L_{v_0}}$. По построению $B(v_0)$ описывается формулой (8), причем $\Gamma(e) \cap G = \{\pm E_n\}$. Отсюда следует, что для любого $\alpha \in G_{\mathcal{O}_{v_0}}^{M_{v_0}}$ выполняется включение

$$\alpha^{-1} B(v_0) \alpha \subset \pm G_{\mathcal{O}_{v_0}}^{L_{v_0}}(\mathfrak{p}_{v_0}).$$

Таким образом,

$$G_{\mathcal{O}}^{(j,\alpha)} \setminus \{\pm E_n\} \subset R \cap \left(\pm G_{\mathcal{O}_{v_0}}^{L_{v_0}}(\mathfrak{p}_{v_0})\right) = \varnothing$$

в силу того, что $R \cap (\pm G_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})) = \varnothing$. Предложение 19 доказано.

Доказательство теоремы 8 в случае $G \subsetneq SO_n(f)$. Пусть $e = (e_1, \ldots, e_n)$ — ортогональный базис, построенный в предложении 19, L — порожденная им решетка. Тогда, как мы убедились выше, для почти всех $v_0 \in V_f^K$ со свойством $\widetilde{K} \subset K$ будем иметь

$$\mathrm{cl}\left(G^{L(v_0)}\right) = \sum_{i=1}^{m} d_i(v_0),$$

где $d_i(v_0)=\left[B(v_0)\backslash G_{\mathcal{O}_{v_0}}^{L_{v_0}}/G_{\mathcal{O}}^{(i)}\right]$, $B(v_0)=G_{\mathcal{O}_{v_0}}^{L(v_0)_{v_0}}$, $G_{\mathcal{O}}^{(i)}=z_i^{-1}G_{A(\infty)}^{L}z_i\cap$ $\cap G_K$ во введенных выше обозначениях. Так как по построению $G_{\mathcal{O}}^{(i)}\subset\{\pm E_n\}$ для любого $i=1,\ldots,m$, то $d_i(v_0)=\left[G_{\mathcal{O}_{v_0}}^{L_{v_0}}:G_{\mathcal{O}}^{(i)}B(v_0)\right]$. Но $B(v_0)\subset\pm G_{\mathcal{O}_{v_0}}^{L_{v_0}}(\mathfrak{p}_{v_0})$, откуда следует, что если $\left[G_{\mathcal{O}_{v_0}}^{L_{v_0}}:G_{\mathcal{O}_{v_0}}^{L_{v_0}}(\mathfrak{p}_{v_0})\right]$ делится на $2r$, то каждое из чисел $d_i(v_0)$ делится на r, и, значит, $\mathrm{cl}(G^{L(v_0)})$ также делится на r. Таким образом, доказательство завершается применением леммы 11.

Нам осталось доказать теорему 8 для группы $\boldsymbol{SO}_n(f)$, где f — положительно определенная квадратичная форма. Рассуждения здесь технически сложнее, чем для случая собственных подгрупп в $\boldsymbol{SO}_n(f)$. Но, как мы уже отмечали, они в равной мере годятся как для $\boldsymbol{SO}_n(f)$, так и для $\boldsymbol{O}_n(f)$. Поскольку $\mathrm{cl}(\boldsymbol{O}_n(f))$ совпадает с числом $c(f)$ классов в роде формы f и, следовательно, представляет с арифметической точки зрения основной интерес, мы установим справедливость утверждения, аналогичного теореме 8 для группы $G=\boldsymbol{O}_n(f)$, что даст нам доказательство теоремы 9.

Прежде всего доказывается следующий аналог предложения 19.

Предложение 20. *Существует такой ортогональный относительно f базис $e_1,\ldots,e_n$ пространства K^n и такое разложение*

$$G_A=\bigcup_{i=1}^{m}G_{A(\infty)}^{L}z_iG_K \tag{11}$$

(L — решетка с базисом $e_1,\ldots,e_n$), что $(z_i)_v=1$ для всех v вне некоторого конечного подмножества $S_0\subset V_f^K$ и все группы $G_{\mathcal{O}}^{(i)}=z_i^{-1}G_{A(\infty)}^{L}z_i\cap G_K$ сопряжены в группе $G_{\overline{K}}$ подгруппе группы $\Gamma=\{x\in G\mid x(e_i)=\pm e_i,\ i=1,\ldots,n\}$.

Доказательство. Пусть в базисе $u_1,\ldots,u_n$ пространства K^n форма f имеет диагональный вид $f=a_1x_1^2+\ldots+a_nx_n^2$. Обозначим через M решетку с базисом $u_1,\ldots,u_n$ и зафиксируем некоторое разложение

$$G_A=\bigcup_{j=1}^{n}G_{A(\infty)}^{M}t_jG_K,$$

в котором $(t_j)_v=1$ для всех $j=1,\ldots,r$ и всех v, лежащих вне некоторого конечного подмножества $S_1\subset V_f^K$. Как и при доказательстве предложения 19, заключаем, что все группы $\overline{G}_{\mathcal{O}}^{(j)}=$ $=t_j^{-1}G_{A(\infty)}^{M}t_j\cap G_K$ являются конечными. Положим $R=\bigcup_{j=1}^{r}\overline{G}_{\mathcal{O}}^{(j)}$ и найдем такое конечное подмножество $S_2\subset V_f^K$, что для $v\in$ $\in V_f^K\setminus S_2$ имеем

$$R\cap G_{\mathcal{O}_v}^{M_v}(\mathfrak{p}_v)=\{E_n\}.$$

Выберем $v_0 \in V_f^K \setminus (S_1 \cup S_2)$ таким образом, что $\widetilde{K} \subset K_{v_0}$ и $v_0(a_i) = 0$ для всех $i = 1, \ldots, n$. Выберем, далее, такой униформизующий элемент $\pi_{v_0} \in \mathcal{O}$, что $\pi_{v_0} \in U_v$ для $v \neq v_0$, и покажем, что базис $e_1 = u_1$, $e_2 = \pi_{v_0} u_2, \ldots, e_n = \pi_{v_0}^{(n-1)} u_n$ искомый. Пусть L — решетка с базисом $e_1, \ldots, e_n$. Тогда $L_v = M_v$ для $v \neq v_0$, а стабилизатор $C = G_{\mathcal{O}_{v_0}}^{L_{v_0}}$ описан в предложении 12. Тогда, как и выше, замечаем, что представители всех смежных классов $G_{A(\infty)}^L \backslash G_A / G_K$ можно выбрать среди аделей $z(j, \alpha)$, $j = 1, \ldots, r$, $\alpha \in G_{\mathcal{O}_{v_0}}^{M_{v_0}}$ (см. доказательство предложения 19). При этом $z(j, \alpha)_v = E_n$ для $v \notin S_0 = S_1 \cup \{v_0\}$ и

$$G_{\mathcal{O}}^{(j, \alpha)} = z(j, \alpha)^{-1} G_{A(\infty)}^L z(j, \alpha) \cap G_K \subset \overline{G}_{\mathcal{O}}^{(j)} \cap \alpha^{-1} C \alpha.$$

Так как $C = \Gamma B$, где $B \subset G_{\mathcal{O}_{v_0}}^{M_{v_0}}(\mathfrak{p}_{v_0})$, $\Gamma = \{x \in G \mid x(u_i) = \pm u_i, i = 1, \ldots, n\}$, то для любого $x \in G_{\mathcal{O}}^{(j, \alpha)}$ имеем $x^2 \in \overline{G}_{\mathcal{O}}^{(j)} \cap \alpha^{-1} B \alpha = \{E_n\}$, т. е. $x^2 = E_n$. Таким образом, доказательство предложения 20 завершает

Лемма 12. *Пусть $\Theta \subset G_{\overline{K}}$ — подгруппа экспоненты 2. Тогда Θ сопряжена в $G_{\overline{K}}$ подгруппе группы Γ.*

Доказательство оставляется читателю в качестве упражнения.

Зафиксируем базис $e = (e_1, \ldots, e_n)$, построенный в предложении 20, решетку L, натянутую на этот базис, и соответствующее разложение (11). Будем считать, что в базисе e форма f имеет вид $f = f_1 x_1^2 + \ldots + f_n x_n^2$. Введем также в рассмотрение такие элементы $g_i \in G_{\overline{K}}$ $(i = 1, \ldots, m)$, что

$$g_i^{-1} G_{\mathcal{O}}^{(i)} g_i \subset \Gamma.$$

Пусть P — конечное расширение Галуа поля K, содержащее $\overline{K}$, коэффициенты матриц g_i и $\sqrt{-1}$, $\sqrt{f_1}, \ldots, \sqrt{f_n}$. Обозначим через T одномерный K-определенный подтор $\boldsymbol{SO}_2(h) \subset \boldsymbol{SO}_n(f)$, где h — ограничение f на подпространство, натянутое на векторы e_1, e_2. Для заданного r из леммы 10 вытекает существование такого $v_0 \in V_f^K \setminus S_0$, что

1) $P \subset K_{v_0}$,
2) индекс $\left[T_{\mathcal{O}_{v_0}}^{L_{v_0}} : T_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})\right]$ делится на $2^{2n} r$,
3) $v(2) = v(f_1) = \ldots = v(f_n) = 0$,
4) $g_i \in G_{\mathcal{O}_{v_0}}^{L_{v_0}}$.

Лемма 13. *Существует такой ортогональный базис u_1, u_2 решетки $\mathcal{O}_{v_0} e_1 \oplus \mathcal{O}_{v_0} e_2$, что $f(u_i) = a f_i$, $i = 1, 2$, где $a \in U_{v_0}$ — единица, не являющаяся квадратом.*

Доказательство. Из наших построений вытекает, что форма $h = f_1x_2^2 + f_2x_2^2$ эквивалентна над $\mathcal{O}_{v_0}$ форме x_1x_2, для которой требуемое утверждение легко проверяется непосредственно.

Для $i > 2$ положим $u_i = e_i$ и обозначим через N_{v_0} $\mathcal{O}_{v_0}$-решетку с базисом $u_1, \pi_{v_0}u_2, \ldots, \pi_{v_0}^{(n-1)}u_n$, где π_{v_0} — униформизующий элемент. Определим решетку $L(r)$ следующим образом:

$$L(r)_v = \begin{cases} L_v, & v \neq v_0, \\ N_{v_0}, & v = v_0. \end{cases}$$

Из предложения 2 вытекает, что решетка $L(r)$ свободна. Покажем, что число классов $\mathrm{cl}(G^{L(r)})$ делится на r. Так как $L(r)_v = L_v$ при $v \neq v_0$, а для $v = v_0$ согласно предложению 12 имеем $C = G^{L(r)_{v_0}}_{\mathcal{O}_{v_0}} = \Delta B$, где $\Delta = \{x \in G \mid x(u_i) = \pm u_i,\ i = 1, \ldots, n\}$, $B \subset G^{L_{v_0}}_{\mathcal{O}_{v_0}}(\mathfrak{p}_{v_0})$, то из леммы 9 получаем

$$\mathrm{cl}(G^{L(r)}) = \sum_{i=1}^{m} c_i, \quad \text{где} \quad c_i = \left[C \backslash G^{L_{v_0}}_{\mathcal{O}_{v_0}} / G^{(i)}_{\mathcal{O}}\right].$$

Из выбора нормирования v_0 вытекает, что для любого $i = 1, \ldots, m$ группа $G^{(i)}_{\mathcal{O}}$ сопряжена в $G^{L_{v_0}}_{\mathcal{O}_{v_0}}$ подгруппе группы Γ. Поэтому делимость всех c_i, а значит и $\mathrm{cl}(G^{L(r)})$, на число r вытекает из следующего утверждения:

Предложение 21. *Пусть H — такая конечная подгруппа в $G^{L_{v_0}}_{\mathcal{O}_{v_0}}$, что $g^{-1}Hg \subset \Gamma$ для некоторого $g \in G^{L_{v_0}}_{\mathcal{O}_{v_0}}$. Тогда число двойных классов $\left[C \backslash G^{L_{v_0}}_{\mathcal{O}_{v_0}} / H\right]$ делится на r.*

Доказательство. Обозначим через $\mathcal{H}$ множество всех подгрупп группы H и для $H' \in \mathcal{H}$ положим

$$D(H') = \left\{x \in G^{L_{v_0}}_{\mathcal{O}_{v_0}} \,\middle|\, H \cap x^{-1}Cx = H'\right\},$$

$$i(H') = [H : H'].$$

Лемма 14. *Имеет место следующая формула:*

$$\left[C \backslash G^{L_{v_0}}_{\mathcal{O}_{v_0}} / H\right] = \sum_{H' \in \mathcal{H}} 2^{-(n+i(H'))} [B \backslash D(H')]$$

в приведенных выше обозначениях.

Доказательство. Легко видеть, что $CD(H')H = D(H')$, т. е. $D(H')$ является объединением некоторого семейства смежных классов CxH. Поэтому $\left[C \backslash G^{L_{v_0}}_{\mathcal{O}_{v_0}} / H\right] = \sum_{H' \in \mathcal{H}} [C \backslash D(H')/H]$, и достаточно показать, что

$$[C \backslash D(H')/H] = 2^{-(n+i(H'))} [B \backslash D(H')].$$

Для этого мы установим, что любой двойной смежный класс CxH, $x \in D(H')$, состоит в точности из $2^{(n+i(H'))}$ обычных смежных классов By, $y \in D(H')$. Имеем

$$CxH = \bigcup_{h \in H} Cxh, \tag{12}$$

причем $Cxh_1 = Cxh_2 \Leftrightarrow h_2 h_1^{-1} \in H \cap x^{-1}Cx = H'$. Тем самым число непересекающихся классов в (12) равно $i(H')$. В то же время для любого $y \in G_{\mathcal{O}_{v_0}}^{L_{v_0}}$

$$Cy = \bigcup_{\delta \in \Delta} B\delta y, \tag{13}$$

и все классы в (13) различны, ибо $\Delta \cap B = \{1\}$. Лемма 14 доказана.

Поскольку $i(H') \leqslant n$, то для доказательства предложения достаточно показать, что число $[B \backslash D(H')]$ делится на $2^{2n}r$ для любой подгруппы $H' \in \mathscr{H}$. Положим $\mathscr{H}(H') = \{H'' \in \mathscr{H} \mid H'' \supsetneqq H'\}$, $\tilde{D}(H') = \left\{x \in G_{\mathcal{O}_{v_0}}^{L_{v_0}} \middle| H' \subset x^{-1}Cx\right\}$. Тогда

$$D(H') = \tilde{D}(H') \Big\backslash \bigcup_{H'' \in \mathscr{H}(H')} D(H''),$$

откуда следует, что

$$[B \backslash D(H')] = [B \backslash \tilde{D}(H')] - \Big[B \Big\backslash \bigcup_{H'' \in \mathscr{H}(H')} \tilde{D}(H'')\Big].$$

Для подсчета числа элементов в объединении воспользуемся следующей общеизвестной формулой: если $A_1, \ldots, A_m$ — конечные множества, то

$$[A_1 \cup \ldots \cup A_m] = \sum_{i=1}^{m} (-1)^{i+1} \sum_{1 \leqslant i_1 \leqslant \ldots \leqslant i_l \leqslant m} [A_{i_1} \cap \ldots \cap A_{i_l}].$$

Так как $\tilde{D}(H_1'') \cap \tilde{D}(H_2'') = \tilde{D}(H_1''H_2'')$, то из этого факта вытекает существование таких целых $b_{H''}$ $(H'' \in \mathscr{H}(H'))$, что

$$\Big[B \Big\backslash \bigcup_{H'' \in \mathscr{H}(H')} \tilde{D}(H'')\Big] = \sum_{H'' \in \mathscr{H}(H')} b_{H''} [B \backslash \tilde{D}(H'')].$$

Поэтому доказательство предложения 23 и теоремы 9 завершает

Лемма 15. *Для любой подгруппы $H' \in \mathscr{H}$ число $[B \backslash \tilde{D}(H')]$ делится на $2^{2n}r$.*

Доказательство. Покажем, что если $\tilde{D}(H') \neq \varnothing$, то для подходящего $x \in G_{\mathcal{O}_{v_0}}^{L_{v_0}}$ группа $Z = xT_{\mathcal{O}_{v_0}}^{L_{v_0}}x^{-1}$ централизует H'. Тогда $\tilde{D}(H')Z = \tilde{D}(H')$, так что число $[B \backslash \tilde{D}(H')]$ выражается в виде суммы $\sum_{ByZ} [\{Bz \mid Bz \subset ByZ\}]$, где сумма берется по всем двойным смежным классам ByZ, а каждое слагаемое есть число обычных смежных классов Bz, содержащихся в двой-

ном классе ByZ. Легко видеть, что последнее число равно $[Z : Z \cap (y^{-1}By)] = \left[T_{\mathcal{O}_{v_0}}^{L_{v_0}} : T_{\mathcal{O}_{v_0}}^{L_{v_0}} \cap ((yx)^{-1} B (yx))\right]$. Так как $B \subset \subset G_{\mathcal{O}_{v_0}}^{L_{v_0}}(\mathfrak{p}_{v_0})$, то по построению последний индекс кратен $2^{2n}r$, и, следовательно, общее число смежных классов $B\backslash\bar{D}(H')$ также кратно $2^{2n}r$.

Итак, пусть $d \in \bar{D}(H')$, т. е. $H' \subset d^{-1}Cd$. Так как H является 2-группой, а Δ — силовской 2-подгруппой в $C = \Delta B$, то в силу теоремы о сопряженности силовских подгрупп в прконечных группах $bdH'd^{-1}b^{-1} \subset \Delta$ для подходящего $b \in B$. Покажем, что элемент $x = bd$ удовлетворяет нашим требованиям. Для этого достаточно установить, что $xH'x^{-1} \subset \Delta_0$, где $\Delta_0 = \{\delta \in \Delta \mid \delta(u_1) = = u_1,\ \delta(u_2) = u_2$ или $\delta(u_1) = -u_1,\ \delta(u_2) = -u_2\}$. Пусть для $h \in H'$ элемент $\delta = xhx^{-1} \notin \Delta_0$. Положим $W(\delta) = \{w \in \in K_{v_0}^n \mid \delta(w) = w\}$. Тогда $W(\delta)$ содержит в точности один из элементов u_1, u_2, скажем, u_1, и поэтому обладает базисом вида $u_1, u_{i_1}, \ldots, u_{i_l}$, где $i_j > 2$. В частности, дискриминант $d(W(\delta))$ равен $af_1f_{i_1} \ldots f_{i_l}$, и следовательно, $d(W(\delta)) \notin K_{v_0}^{*2}$. С другой стороны, по условию $g^{-1}Hg \subset \Gamma$, так что аналогичное пространство $W(\gamma) = \{w \in K_{v_0}^n \mid \gamma(w) = w\}$ для элемента $\gamma = g^{-1}hg$ обладает базисом вида $e_{j_1}, \ldots, e_{j_m}$, откуда $d(W(\gamma)) = f_{j_1} \ldots f_{j_m} \in \in K_{v_0}^{*2}$. Но $\gamma = (xg)^{-1}\delta(xg)$, поэтому $W(\delta) = (xg)W(\gamma)$, т. е. пространства $W(\delta)$ и $W(\gamma)$ должны быть изометричными, в частности, иметь одинаковые дискриминанты. Полученное противоречие и доказывает требуемое. Таким образом, доказательство всех теорем этого параграфа завершено.

Отметим, что было бы интересно получить аналог теоремы 8 для групп смешанного типа.

§ 8.4. Оценки чисел классов редуктивных групп

Результаты предыдущих параграфов показывают, что значения, которые может принимать число классов $\mathrm{cl}(\varphi(G))$ полупростой K-группы G, зависят от арифметических свойств группы. Поэтому для того чтобы получить их характеризацию, нужно обладать дополнительной информацией о группе G. Возникает вопрос: что можно сказать о $\mathrm{cl}(\varphi(G))$ в самой общей ситуации? Здесь, конечно, нужно исключить из рассмотрения случай, когда группа G обладает свойством абсолютной сильной аппроксимации, ибо тогда $\mathrm{cl}(\varphi(G)) = 1$ для любой реализации φ. Оказывается, что в остальных случаях числа классов $\mathrm{cl}(\varphi(G))$ при различных реализациях φ не ограничены в совокупности.

Теорема 10. *Пусть G — линейная алгебраическая K-группа степени n, не обладающая свойством абсолютной сильной аппроксимации. Тогда для любого числа r существует такая решетка $M(r) \subset K^{2n}$, то* $\mathrm{cl}(G^{M(r)}) > r$.

Доказательство. Зафиксируем решетку $L \subset K^n$, для любой открытой подгруппы $U \subset G^L_{A_f(\infty)}$ будем обозначать через $c(U)$ число двойных смежных классов $(G_\infty \times U)\backslash G_A/G_K$.

Лемма 16. *Для любого натурального r найдется такая открытая подгруппа U, что $c(U) > r$.*

Доказательство. Предположим противное. Тогда для некоторой открытой подгруппы $U_0 \subset G^L_{A_f(\infty)}$ число $c(U_0)$ принимает максимальное значение d. Зафиксируем разложение

$$G_A = \bigcup_{i=1}^{d} (G_\infty \times U_0)\, z_i G_K \tag{1}$$

на непересекающиеся двойные смежные классы. Из предположения о максимальности $c(U_0)$ вытекает, что для любой подгруппы $U \subset U_0$ имеем $c(U) = c(U_0)$, откуда

$$(G_\infty \times U_0)\, z_i G_K = (G_0 \times U)\, z_i G_K$$

для всех $i = 1, 2, \ldots, d$. Переходя к проекциям на G_{A_f} и обозначая через $\tilde{z}_i$ соответствующую проекцию z_i, получим

$$U_0 \tilde{z}_i G_K = U \tilde{z}_i G_K,$$

и, следовательно,

$$U_0 \tilde{z}_i G_K = \bigcap U \tilde{z}_i G_K, \tag{2}$$

где пересечение берется по всем открытым подгруппам $U \subset U_0$. Воспользуемся теперь следующим простым фактом из теории топологических групп: если топологическая группа H обладает фундаментальной системой окрестностей единицы $\mathfrak{U} = \{U\}$, состоящей из подгрупп, то замыкание любого подмножества $\Gamma \subset H$ описывается следующим образом: $\overline{\Gamma} = \bigcap\limits_{U \in \mathfrak{U}} U\Gamma$. Из этого факта получается, что правая часть (2) совпадает с замыканием $\tilde{z}_i G_K$ в G_{A_f}, т. е. с $\tilde{z}_i \overline{G}_K$, где $\overline{G}_K$ — замыкание G_K. Из разложения (1) получаем, что

$$G_{A_f} = \bigcup_{i=1}^{d} U_0 \tilde{z}_i G_K = \bigcup_{i=1}^{d} \tilde{z}_i \overline{G}_K,$$

т. е. $\overline{G}_K$ имеет конечный индекс в G_{A_f}. Но это невозможно, ибо из отсутствия абсолютной сильной аппроксимации у группы G и из теоремы 7.12 вытекает, что выполняется одно из условий предложения 7.13, согласно которому индекс $\overline{G}_K$ в G_{A_f} бесконечен. Лемма доказана.

Продолжаем доказательство теоремы 10. В силу леммы 16 можно найти такую открытую подгруппу $U \subset G^L_{A_f(\infty)}$, что $c(U) > r$, а нам достаточно найти решетку $M \subset K^{2n}$ со свойством $G^M_{A_f(\infty)} \subset U$. Но, будучи открытой, U содержит подгруппу вида $W = \prod_{v \in T} G^{L_v}_{\mathcal{O}_v}(\mathfrak{p}_v^{m_v}) \times \prod_{v \in V_f^K \setminus T} G^{L_v}_{\mathcal{O}_v}$, где $T \subset V_f^K$ — некоторое конечное подмножество, m_v $(v \in T)$ — подходящие натуральные числа. Согласно предложению 11 для каждого $v \in T$ существует решетка $L_v(m_v) \subset K_v^{2n}$ такая, что $G^{L_v(m_v)}_{\mathcal{O}_v} = G^{L_v}_{\mathcal{O}_v}(\mathfrak{p}_v^{m_v})$. Определим решетку $M \subset K^{2n}$, задав ее локализации следующим образом

$$M_v = \begin{cases} L_v(m_v), & v \in T, \\ L_v \oplus \mathcal{O}_v^n, & v \notin T. \end{cases}$$

Тогда группа $G^M_{A_f(\infty)}$, очевидно, совпадает с W, так что решетка M — искомая. Теорема 10 доказана.

Из теоремы 10 вытекает следующее любопытное замечание: если число классов $\mathrm{cl}(\varphi(G))$ произвольной алгебраической K-группы G принимает хотя бы одно неединичное значение, то изменяя реализацию φ, мы получим бесконечное множество различных значений.

Было бы интересно получить аналог теоремы 10 в исходной размерности n (предполагая, естественно, что G не является нормальным делителем в $\boldsymbol{GL}_n$). По-видимому, это можно сделать, модифицируя подходящим образом доказательство предложения 15. Отметим, что для торов в $\boldsymbol{GL}_n$, отличных от скалярного, это вытекает из предложения 25, которое мы докажем в следующем параграфе в связи с изучением так называемой проблемы рода в арифметических группах.

Переходим к изложению результатов о связи между числом классов алгебраической группы и числами классов ее замечательных подгрупп (параболических подгрупп, максимальных торов). Одна из наиболее существенных мотивировок изучения этой связи состоит в гипотетической возможности получить таким образом оценки чисел классов, скажем, максимальных торов группы, что может оказаться полезным при изучении методами теории алгебраических групп чисел классов идеалов полей алгебраических чисел. В настоящее время это направление находится в стадии разработки, причем имеющиеся в нашем распоряжении результаты носят предварительный характер. По этой причине мы приводим следующие теоремы без доказательства.

Теорема 11 (Бондаренко, Рапинчук [1]). *Пусть G — редуктивная алгебраическая K-группа, P — произвольная K-определенная параболическая подгруппа группы G. Тогда* $\mathrm{cl}(G) \leqslant \mathrm{cl}(P)$.

Следствие 1. *Пусть G — редуктивная K-разложимая алгебраическая группа, T — произвольный максимальный K-разложимый тор в G. Тогда* $\mathrm{cl}(G) \leqslant \mathrm{cl}(T)$.

Действительно, пусть $B = TU$ — подгруппа Бореля группы G, содержащая тор T. Тогда согласно теореме 11 $\mathrm{cl}(G) \leqslant \mathrm{cl}(B)$. С другой стороны, в силу предложения 5.4 $\mathrm{cl}(B) \leqslant \mathrm{cl}(T)$, ибо для U имеет место абсолютная сильная аппроксимация.

Следствие 1 позволяет дать «эффективный» вариант теоремы 4 об одноклассных решетках для разложимых групп над одноклассным полем.

Следствие 2. *Пусть G — редуктивная разложимая группа над одноклассным полем K. Тогда* $\mathrm{cl}(G) = 1$ *в любой K-реализации G, в которой G содержит максимальный K-разложимый тор в диагональном виде. (Более точно, если $G \subset \boldsymbol{GL}_n$ и в базисе $e_1, \ldots, e_n$ пространства K^n некоторый максимальный тор группы G записывается диагональными матрицами, то* $\mathrm{cl}(G^L) = 1$, *где L — решетка с базисом $e_1, \ldots, e_n$.)*

Пусть T — максимальный K-разложимый тор группы G такой, что $T \subset D_n$. Так как $\mathrm{cl}(G) \leqslant \mathrm{cl}(T)$ (следствие 1), то достаточно показать, что $\mathrm{cl}(T) = 1$. Пусть $r = \dim T$ и $\varphi\colon D_r \simeq T$ — определенный над K изоморфизм. В силу одноклассности поля K мы имеем $\mathrm{cl}(D_r) = 1$, и поэтому достаточно проверить, что $\varphi(D_{r\,A(\infty)}) \subset T_{A(\infty)}$. Но в координатном выражении для φ

$$\varphi\colon (x_1, \ldots, x_r) \mapsto (\varphi_1(x_1, \ldots, x_r), \ldots, \varphi_n(x_1, \ldots, x_r))$$

рациональные функции φ_i должны быть мультипликативными, и поэтому имеют вид $\varphi_i(x_1, \ldots, x_r) = \prod_{j=1}^{r} x_j^{a_{ij}}$ для подходящих целых α_{ij}, откуда и следует требуемое.

Как мы увидим на приводимых ниже примерах, зависимость между $\mathrm{cl}(G)$ и $\mathrm{cl}(T)$, где T — произвольный K-определенный тор алгебраической K-группы G, может быть самого разного характера. Поэтому следующий результат, в котором разбирается случай полупростых групп некомпактного типа, по-видимому, не допускает распространения на более широкий класс групп:

Теорема 12 (Платонов, Бондаренко, Рапинчук [2]). *Пусть G — полупростая K-группа некомпактного типа, $\pi\colon \tilde{G} \to G$ — универсальное K-определенное накрытие. Тогда для любого K-определенного максимального тора T*

$$\mathrm{cl}(T) \geqslant \frac{\mathrm{cl}(G)}{[Ш(T)]\,[H^1(\mathcal{G}, \mathbf{X}(\tilde{T}))]},$$

где $\mathbf{X}(\tilde{T})$ — группа характеров тора $\tilde{T} = \pi^{-1}(T)$, $\mathcal{G}$ — группа Галуа над K поля разложения L торов T и $\tilde{T}$.

Отметим, что если $T \subset G$ — максимальный тор, разложимый над K, то $Ш(T) = H^1(\mathcal{G}, \mathbf{X}(\tilde{T})) = 1$, и мы приходим к оценке

$\mathrm{cl}(T) \geqslant \mathrm{cl}(G)$, которая была получена в следствии 1 из теоремы 11 другим способом.

Следствие 3. *Пусть G — полупростая K-группа некомпактного типа. Существует такая константа $M > 0$, зависящая только от G, что для любой реализации φ*

$$\min_T \mathrm{cl}(\varphi(T)) \geqslant \frac{1}{M} \mathrm{cl}(\varphi(G)), \tag{3}$$

где минимум берется по всем максимальным K-определенным торам группы G.

Приведем два любопытных примера, иллюстрирующих многообразие зависимостей между $\min_T \mathrm{cl}(T)$ и $\mathrm{cl}(G)$.

Пример 1. Пусть $G = \boldsymbol{SL}_2$ над полем рациональных чисел $\mathbb{Q}$. Покажем, что для любого $m > 0$ существует такая решетка $L(m) \subset \mathbb{Q}^4$, что для любого максимального $\mathbb{Q}$-определенного тора $T \subset G$ имеет место неравенство $\mathrm{cl}(T^{L(m)}) > m$, в то время как $\mathrm{cl}(G^{L(m)}) = 1$.

Зафиксируем решетку $L \subset \mathbb{Q}^2$ и для каждого простого p обозначим через $M_p \subset \mathbb{Q}_p^4$ такую решетку, что $G_{\mathbb{Z}_p}^{M_p} = G_{\mathbb{Z}_p}^{M_p}(p)$ (см. предложение 12). Пусть $S(m) = \{p_1, \ldots, p_m\}$ — набор, состоящий из m нечетных простых чисел. Зададим решетку $L(m) \subset \mathbb{Q}^4$ следующим образом:

$$L(m)_p = \begin{cases} L_p \oplus \mathbb{Z}_p^2, & p \notin S(m), \\ M_p, & p \in S(m), \end{cases}$$

и покажем, что $\mathrm{cl}(T^{L(m)}) \geqslant 2^{m-2}$ для любого максимального $\mathbb{Q}$-тора $T \subset G$; это очевидно, и дает требуемое.

Имеем

$$\mathrm{cl}(T^{L(m)}) = [T_A : T_{A(\infty)}^{L(m)} T_{\mathbb{Q}}] =$$
$$= [T_A : T_{A(\infty)}^{L} T_{\mathbb{Q}}] [T_{A(\infty)}^{L} T_{\mathbb{Q}} : T_{A(\infty)}^{L(m)} T_{\mathbb{Q}}] = \mathrm{cl}(T^L) [T_{A(\infty)}^{L} : T_{A(\infty)}^{L(m)} T_{\mathbb{Z}}^{L}] =$$
$$= \mathrm{cl}(T^L) \Big[\prod_{p \in S(m)} T_{\mathbb{Z}_p}^{L_p} : \tau_{S(m)}(T_{\mathbb{Z}}^{L}) \prod_{p \in S(m)} T_{\mathbb{Z}_p}^{L_p}(p) \Big],$$

где $\tau_{S(m)}\colon T_{\mathbb{Q}} \to \prod_{p \in S(m)} T_{\mathbb{Q}_p}$ — диагональное вложение. Матрица $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ принадлежит всем группам $T_{\mathbb{Z}_p}^{L_p}$, но не принадлежит ни одной из групп $T_{\mathbb{Z}_p}^{L_p}(p)$ из-за нечетности p. Поэтому в разложении абелевой группы $\prod_{p \in S(m)} T_{\mathbb{Z}_p}^{L_p} / T_{\mathbb{Z}_p}^{L_p}(p)$ на циклические встретится не менее m циклических 2-примарных сомножителей. С другой стороны, в силу следствия 1 из теоремы 4.11 группа $T_{\mathbb{Z}}^{L}$ является прямым произведением конечной группы Φ и свободной абелевой группы Γ ранга $\leqslant 1$. Поскольку $\dim T =$

$=1$, имеет место изоморфизм $T \simeq \mathbf{G}_m$, и, следовательно, группа Φ циклична, таким образом, группа $T^L_{\mathbf{Z}}$ имеет самое большее два циклических сомножителя, и, значит, факторгруппа

$$D = \prod_{p \in S(m)} T^{L_p}_{\mathbf{Z}_p} \Big/ \Big(\tau_{S(m)}\big(T^L_{\mathbf{Z}}\big) \prod_{p \in S(m)} T^{L_p}_{\mathbf{Z}_p}(p)\Big)$$

имеет не менее $(m-2)$ 2-примарных циклических сомножителей. В частности, $[D] \geqslant 2^{m-2}$, и тем более $\mathrm{cl}(T^{L(m)}) = \mathrm{cl}(T^L)\,[D] \geqslant 2^{m-2}$. Утверждение о том, что $\mathrm{cl}(G^{L(m)}) = 1$, следует из сильной аппроксимационной теоремы.

Пример 1 показывает, что разность между левой и правой частью в оценке (3) может быть как угодно большой. В то же время оценки типа $M\,\mathrm{cl}(G) \geqslant \min\limits_T \mathrm{cl}(T)$, где M — константа, зависящая только от бирациональных свойств G, но не от ее конкретной реализации, не существует.

Пример 2. Пусть $f = x^2 + y^2 + z^2$ в базисе e_1, e_2, e_3 пространства $\mathbb{Q}^3$, $G = \boldsymbol{SO}_3(f)$. Тогда $T = \boldsymbol{SO}_2(g)$, где $g = x^2 + y^2$, является максимальным тором в G.

Зафиксируем нечетное простое число p и для целого числа $n > 0$ обозначим через $L(n)$ решетку с базисом $e_1, e_2, p^n e_3$. Наша цель — показать, что $\mathrm{cl}\,(G^{L(n)}) \xrightarrow[n\to\infty]{} +\infty$, в то время как $\mathrm{cl}\,(T^{L(n)}) = 1$. Положим $D_n = G^{L(n)}_{\mathbf{Z}_p}$. Тогда, дословно повторяя доказательство предложения 12, можно показать, что $D(n) = \{x = (x_{ij}) \in G_{\mathbf{Z}_p} \mid x_{ij} \equiv \pm\delta_{ij} \pmod{p^n}$, если i либо j равно 3$\}$ (матричная запись берется относительно базиса e_1, e_2, e_3; δ_{ij} — символ Кронекера). Поэтому $D(1) \supset D(2) \supset D(3) \supset \ldots$, причем

$$\bigcap_{n>0} D(n) = \{1, \gamma\}\, T_{\mathbf{Z}_p},$$

где $\gamma = \mathrm{diag}\,(1, 1, -1)$. Поскольку индекс $T_{\mathbf{Z}_p}$ в $G_{\mathbf{Z}_p}$ бесконечен, то $[G_{\mathbf{Z}_p} : D(n)] \xrightarrow[n\to\infty]{} +\infty$, а следовательно, и $i(n) = [D(n)\backslash G_{\mathbf{Z}_p}/G_{\mathbf{Z}}] \xrightarrow[n\to\infty]{} +\infty$, ибо группа $G_{\mathbf{Z}}$ конечна в силу положительной определенности f. С другой стороны, рассуждая как и при доказательстве леммы 9, легко показать, что $i(n)$ совпадает с числом двойных смежных классов $G^{L(n)}_{A(\infty)} x G_{\mathbf{Z}}$, содержащихся в главном классе $G_{A(\infty)} G_{\mathbb{Q}}$; в частности, $\mathrm{cl}(G^{L(n)}) \geqslant i(n)$ и $\mathrm{cl}\,(G^{L(n)}) \xrightarrow[n\to\infty]{} +\infty$.

Осталось установить, что $\mathrm{cl}\,(T^{L(n)}) = 1$ для любого n. Так как T действует на e_3 тривиально, то $\mathrm{cl}\,(T^{L(n)}) = \mathrm{cl}\,(\boldsymbol{SO}_2(g))$ для всех n. Но хорошо известно, (см. например, Боревич, Шафаревич [1]), что форма g одноклассна, и поэтому, в силу предложе-

ния 4, $\mathrm{cl}(\boldsymbol{O}_2(g))=1$. Так как $\boldsymbol{O}_2(g)_{\mathbb{Z}}$ содержит матрицу с определителем (-1), то отсюда легко получить, что $\mathrm{cl}(\boldsymbol{SO}_2(g))=1$, что и требовалось.

Упражнение. Дать другое доказательство равенства $\mathrm{cl}(T^L)=1$ в примере 2, используя одноклассность поля $K=\mathbb{Q}(\sqrt{-1})$ (последняя является следствием существования алгоритма Евклида в кольце целых гауссовых чисел $\mathcal{O}=\mathbb{Z}[i]$). А именно, рассмотреть естественную реализацию тора $S=\mathbf{R}_{K/\mathbb{Q}}(\mathbf{G}_m)$, определяемую регулярным представлением K в некотором базисе $\mathcal{O}/\mathbb{Z}$. Тогда из равенства $h_K=1$ следует, что $\mathrm{cl}(S)=1$. Используя отождествление $T\simeq\mathbf{R}^{(1)}_{K/\mathbb{Q}}(\mathbf{G}_m)$, с помощью теоремы 90 Гильберта построить сюръективный морфизм $\theta\colon S\to T$ с ядром $\mathrm{Ker}\,\theta=\boldsymbol{G}_m$. Показать, что $\theta_A(S_A)=T_A$, $\theta(S_{A(\infty)})\subset T_{A(\infty)}$, и вывести отсюда, что $\mathrm{cl}(T)=1$.

Пример 2 показывает, что утверждение теоремы 12 (и даже следствия из нее) не допускает распространения на группы компактного типа.

Проблема изучения связи между числами классов группы и ее максимальных торов, несомненно, заслуживает дальнейшей разработки. Использованные до сих пор чисто алгебраические методы, по-видимому, следует дополнить применением аналитических соображений, что в итоге должно привести к прояснению «усредненной» картины изменения чисел классов торов и, в частности, к ответу на вопрос, конечно или бесконечно множество торов алгебраической группы с данным фиксированным числом классов (современный вариант знаменитой проблемы Гаусса).

В заключение этого параграфа остановимся бегло еще на одном круге вопросов. Речь идет об изменении числа классов алгебраической группы при изменении поля определения. Более точно, пусть G — K-определенная алгебраическая группа, E/K — конечное расширение. Как связано число классов $\mathrm{cl}(G)$ с числом классов $\mathrm{cl}_E(G)$ той же группы G, рассматриваемой как группа над E? (Здесь и далее имеется в виду, что реализация группы G задается некоторой решеткой $L\subset K^n$; тогда число классов $\mathrm{cl}_E(G)$ и соответствующие группы целых точек берутся относительно решетки $L\otimes_{\mathcal{O}}\mathcal{O}_E\subset E^n$, где $\mathcal{O}_E$ — кольцо целых поля E.) Различные аспекты этой проблемы исследовались в работах Бартельса [1, 2], Эрнеста, Сия [1, 2]. Мы ограничимся указанием на существующую связь с локально-глобальным принципом для когомологий арифметических подгрупп. Для точной формулировки условимся считать отмеченным элементом множества двойных смежных классов $G_{A_E(\infty)}\backslash G_{A_E}/G_E$ главный класс $G_{A_E(\infty)}G_E$.

Теорема 13 (Рольфс [1]). *Предположим, что E/K — расширение Галуа и для G над E выполняется принцип Хассе* (*т. е. отображение $H^1(E/K, G_E) \to \prod_v H^1(E_w/K_v, G_{E_w})$ имеет тривиальное ядро*). *Тогда имеет место точная последовательность множеств с отмеченными элементами*

$$1 \to \operatorname{Ker}\left(G_{A(\infty)}\backslash G_A/G_K \to G_{A_E(\infty)}\backslash G_{A_E}/G_E\right) \xrightarrow{\alpha}$$
$$\xrightarrow{\alpha} H^1(E/K, G_{\mathcal{O}_E}) \xrightarrow{\beta} \prod_v H^1\left(E_w/K_v, G_{\mathcal{O}_{E_w}}\right)$$

(*для каждого $v \in V^K$ мы выбираем одно продолжение $w \in V^E$ и считаем, что $\mathcal{O}_{E_w} = E_w$ для $w \in V_\infty^E$*).

Доказательство разбивается на несколько этапов.

Конструкция α. Пусть $x \in G_A$ и $x = yz$, где $y \in G_{A_E(\infty)}$, $z \in G_E$. Тогда для любого $\sigma \in \mathcal{G} = \operatorname{Gal}(E/K)$ имеем

$$a_\sigma = y^{-1}y^\sigma = (xz^{-1})^{-1}(xz^{-1})^\sigma = z(z^{-1})^\sigma \in G_{A_E(\infty)} \cap G_E = G_{\mathcal{O}_E}, \quad (4)$$

так что $a = \{a_\sigma\}$ определяет коцикл в $H^1(E/K, G_{\mathcal{O}_E})$. Любое другое разложение $x = y'z'$ связано с разложением $x = yz$ следующим образом: $y' = yt$, $z' = t^{-1}z$, где $t \in G_{\mathcal{O}_E}$, поэтому соответствующий коцикл

$$a'_\sigma = (y')^{-1}(y')^\sigma = t^{-1}y^{-1}y^\sigma t^\sigma = t^{-1}a_\sigma t^\sigma$$

эквивалентен коциклу $\{a_\sigma\}$. Кроме того, если $x_1 = gxh$ для $g \in G_{A(\infty)}$, $h \in G_K$, то $x_1 = (gy)(zh)$ и $(gy)^{-1}(gy)^\sigma = y^{-1}y^\sigma$, поэтому коцикл a зависит только от смежного класса $G_{A(\infty)}xG_K$. Тем самым мы построили корректно определенное отображение α.

Равенство $\operatorname{Ker}\alpha = \{1\}$. Предположим, что коцикл $a = \{a_\sigma\}$, отвечающий элементу x, тривиален в $H^1(E/K, G_{\mathcal{O}_E})$, т. е. $a_\sigma = t^{-1}t^\sigma$ для некоторого $t \in G_{\mathcal{O}_E}$. Тогда из (4) получаем

$$y^{-1}y^\sigma = z(z^{-1})^\sigma = t^{-1}t^\sigma \quad \text{для всех} \quad \sigma \in \mathcal{G}.$$

Поэтому $(yt^{-1})^\sigma = yt^{-1}$, $(tz)^\sigma = tz$, т. е. $y' = yt^{-1} \in G_{A_E(\infty)} \cap G_A = G_{A(\infty)}$, $z' = tz \in G_E \cap G_A = G_K$. Тогда $x = yz = y'z'$ принадлежит главному классу $G_{A(\infty)}G_K$, что и требовалось.

Точность в члене $H^1(E/K, G_{\mathcal{O}_E})$. По построению $a_\sigma = y^{-1}y^\sigma$, $y \in G_{A_E(\infty)}$, т. е. коцикл a становится тривиальным в группе $H^1(E/K, G_{A_E(\infty)}) = \prod_v H^1\left(E/K, \prod_{w|v} G_{\mathcal{O}_{E_w}}\right) = \prod_v H^1\left(E_w/K_v, G_{\mathcal{O}_{E_w}}\right)$.

Тем самым $\operatorname{Im}\alpha \subset \operatorname{Ker}\beta$. Обратно, если коцикл $a=\{a_\sigma\} \in H^1(E/K, G_{\mathcal{O}_E})$ лежит в $\operatorname{Ker}\beta$, то $a_\sigma = y^{-1}y^\sigma$ для некоторого $y \in G_{A_E(\infty)}$. Отсюда также вытекает, что образ a в $H^1(E/K, G_E)$ становится тривиальным элементом в $H^1(E_w/K_v, G_{E_w})$ для всех нормирований $v \in V^K$, поэтому из справедливости для G принципа Хассе вытекает тривиальность a в $H^1(E/K, G_E)$, т. е. существование такого $z \in G_E$, что $a_\sigma = z(z^{-1})^\sigma$. Положим $x = yz$. Тогда для любого $\sigma \in \mathcal{G}$ имеем

$$x^\sigma = y^\sigma z^\sigma = (ya_\sigma)(a_\sigma^{-1}z) = yz = x,$$

так что $x \in G_A$. Кроме того по построению $x \in G_{A_E(\infty)}G_E$. Таким образом, класс $G_{A(\infty)}xG_K$ лежит в $\operatorname{Ker}(G_{A(\infty)}\backslash G_A/G_K \to G_{A_E(\infty)}\backslash G_{A_E}/G_K)$, причем из конструкции α вытекает, что $\alpha(G_{A(\infty)}xG_K) = a$. Теорема 13 полностью доказана.

Следствие 4 (принцип Хассе для когомологий арифметических подгрупп односвязных групп). *Пусть G — полупростая односвязная K-определенная группа некомпактного типа. Тогда для любого расширения Галуа E/K отображение*

$$H^1(E/K, G_{\mathcal{O}_E}) \to \prod_v H^1(E_w/K_v, G_{\mathcal{O}_{E_w}})$$

имеет тривиальное ядро.

Действительно, для когомологий групп рациональных точек односвязных групп принцип Хассе выполняется всегда (теорема 6.6). С другой стороны, из свойства сильной аппроксимации для G (теорема 7.12) получаем, что $\operatorname{cl}(G) = 1$, и наше утверждение вытекает из точной последовательности теоремы.

Для групп компактного типа интересный результат получается, если рассуждать в обратном направлении: вначале получить принцип Хассе для когомологий, и в качестве следствия получить тривиальность

$$\operatorname{Ker}(G_{A(\infty)}\backslash G_A/G_K \to G_{A_E(\infty)}\backslash G_{A_E}/G_E).$$

Следствие 5. *Пусть G — определенная над $\mathbb{Q}$ алгебраическая группа с компактной группой $\mathbb{R}$-точек, $K/\mathbb{Q}$ — вполне вещественное расширение Галуа. Предположим, что $G_{\mathcal{O}_K} = G_{\mathbb{Z}}$ (см. § 4.8) и для G над K выполняется принцип Хассе. Тогда естественное отображение*

$$G_{A_{\mathbb{Q}}(\infty)}\backslash G_{A_{\mathbb{Q}}}/G_{\mathbb{Q}} \to G_{A_K(\infty)}\backslash G_{A_K}/G_K$$

имеет тривиальное ядро.

Учитывая, что двойные классы $G_{A(\infty)}\backslash G_A/G_K$ для ортогональной группы $G = \boldsymbol{O}_n(f)$ квадратичной формы f взаимно однозначно соответствуют классам в роде f (предложение 4), причем

главный класс $G_{\Delta(\infty)}G_K$ отвечает классу, содержащему f, из следствия 5 получаем

Следствие 6. *Пусть f — положительно определенная квадратичная форма с целыми коэффициентами, $K/\mathbb{Q}$ — вполне вещественное расширение Галуа. Предположим, что $\boldsymbol{O}_n(f)_{\mathcal{O}_K} = \boldsymbol{O}_n(f)_{\mathbb{Z}}$ (это всегда имеет место, если форма f диагональная, см. § 4.8). Тогда если целочисленная форма g лежит в роде f и эквивалентна форме f над $\mathcal{O}_K$, то она эквивалентна f над $\mathbb{Z}$.*

Доказательство следствия 5 вытекает из точной последовательности теоремы и следующего утверждения, представляющего независимый интерес.

Теорема 14 (Бартельс [2]). *Пусть G — $\mathbb{Q}$-определенная алгебраическая группа, $K/\mathbb{Q}$ — вполне вещественное расширение Галуа. Предположим, что $G_{\mathcal{O}_K} = G_{\mathbb{Z}}$. Тогда естественное отображение*

$$H^1(K/\mathbb{Q},\ G_{\mathcal{O}_K}) \xrightarrow{\rho} \prod_{v \in V} H^1\left(K_w/\mathbb{Q}_v,\ G_{\mathcal{O}_{K_w}}\right) \tag{5}$$

имеет тривиальное ядро.

Доказательство. Поскольку группа Галуа $\mathcal{G} = \mathrm{Gal}(K/\mathbb{Q})$ действует на $G_{\mathcal{O}_K} = G_{\mathbb{Z}}$ тривиально, то 1-коциклы на $\mathcal{G}$ со значениями в $G_{\mathcal{O}_K}$ являются гомоморфизмами $\varphi\colon \mathcal{G} \to G_{\mathcal{O}_K}$, причем тривиальный класс в $Z^1(K/\mathbb{Q},\ G_{\mathcal{O}_K})$ состоит в точности из единичного гомоморфизма. Пусть теперь $\varphi \in \mathrm{Ker}\,\rho$. Наша цель — показать, что $\varphi = 1$. Для любого нормирования $w \in V_f^K$ обозначим через $\mathcal{G}_w^{(1)}$ соответствующую группу инерции. Естественные отображения $G_{\mathcal{O}_K} \to G_{\mathcal{O}_{K_w}} \to \Gamma = G_{\mathcal{O}_{K_w}} / G_{\mathcal{O}_{K_w}}(\mathfrak{P}_w)$ и включения $\mathcal{G}_w^{(1)} \subset \mathcal{G}_w = \mathrm{Gal}(K_w/\mathbb{Q}_v) \subset \mathcal{G}$ индуцируют отображения когомологий

$$H^1(K/\mathbb{Q},\ G_{\mathcal{O}_K}) \xrightarrow{\rho_w} H^1\left(K_w/\mathbb{Q}_v,\ G_{\mathcal{O}_{K_w}}\right) \xrightarrow{\theta_w} H^1\left(\mathcal{G}_w^{(1)},\ \Gamma\right).$$

Поскольку $\varphi \in \mathrm{Ker}\,\rho$, то $\theta_w \circ \rho_w(\varphi) = 1$. Но группа $\mathcal{G}_w^{(1)}$ действует на Γ тривиально, так что последнее равносильно тривиальности гомоморфизма, который получается композицией ограничения φ на $\mathcal{G}_w^{(1)}$ и гомоморфизма $G_{\mathcal{O}_K} \to \Gamma$. Другими словами, $\varphi(\mathcal{G}_w^{(1)}) \subset G_{\mathcal{O}_K}(\mathfrak{P}_w) = G_{\mathbb{Z}}(p_w)$, где p_w — отвечающее w простое число. Из леммы Минковского (см. § 4.8) вытекает, что группа $G_{\mathbb{Z}}(p_w)$ тривиальна для нечетных p_w. Рассуждая аналогично, легко показать, что для $p_w = 2$ группа $G_{\mathbb{Z}}(p_w)$ является группой экспоненты 2. Поэтому, учитывая порождаемость $\mathcal{G}$ всеми группами $\mathcal{G}_w^{(1)}$, что является следствием теоремы Эрмита (см. § 1.1), получаем, что $\varphi(\mathcal{G}) \subset G_{\mathbb{Z}}(2)$, и, следовательно, $\varphi(\mathcal{G}) \simeq (\mathbb{Z}/2\mathbb{Z})^l$,

для подходящего l. Обозначим через L подполе в K, отвечающее $\operatorname{Ker}\varphi$. Поскольку $\mathcal{G}_w^{(1)} \subset \operatorname{Ker}\varphi$, если p_w нечетно, то в расширении $L/\mathbb{Q}$ может ветвиться только двойка. С другой стороны, из того, что $\operatorname{Gal}(L/\mathbb{Q}) = \operatorname{Im}\varphi \simeq (\mathbb{Z}/2\mathbb{Z})^l$, вытекает, что L является композитом квадратичных расширений $\mathbb{Q}$. Так как единственным вещественным квадратичным расширением $\mathbb{Q}$, ветвящимся лишь в двойке, является расширение $\mathbb{Q}(\sqrt{2})$, то либо $l=0$, что давало бы требуемое, либо $L=\mathbb{Q}(\sqrt{2})$, в частности, $l=1$.

Имеем следующую коммутативную диаграмму с точными строками:

$$\begin{tikzcd} 1 \arrow[r] & H^1(L/\mathbb{Q},\ G_{\mathcal{O}_L}) \arrow[r, "a"] \arrow[d, "\delta"] & H^1(K/\mathbb{Q},\ G_{\mathcal{O}_K}) \arrow[d, "\rho"] \\ 1 \arrow[r] & \prod\limits_v H^1\left(L_w/\mathbb{Q}_v,\ G_{\mathcal{O}_{L_w}}\right) \arrow[r] & \prod\limits_v H^1\left(K_w/\mathbb{Q}_v,\ G_{\mathcal{O}_{K_w}}\right) \end{tikzcd} \tag{6}$$

Пусть $\operatorname{Gal}(L/\mathbb{Q}) = \{1, \sigma\}$ и $\varphi(\sigma) = a$. Из диаграммы (6) вытекает, что $\varphi \in \operatorname{Ker}\delta$, поэтому, рассуждая как и выше, получим, что $a \in G_{\mathbb{Z}}(2)$. Воспользуемся далее следующим простым фактом.

Лемма 17 (Минковский). *Пусть $a \in GL_n(\mathbb{Z}, 2)$ и $a^2 = E_n$. Тогда существует такая матрица $c \in GL_n(\mathbb{Z})$, что $cac^{-1} = \operatorname{diag}(\varepsilon_1, \ldots, \varepsilon_n)$, где $\varepsilon_i = \pm 1$.*

Действительно, положим $a_1 = \frac{1}{2}(E_n - a)$, $a_2 = \frac{1}{2}(E_n + a)$. Тогда $a_i \in M_n(\mathbb{Z})$, $aa_1 = -a_1$, $aa_2 = a_2$, $a_1 + a_2 = E_n$. Отсюда следует, что любой элемент $z \in \mathbb{Z}^n$ имеет представление $z = z_1 + z_2$, где $z_i = a_i(z) \in \mathbb{Z}^n$. Так что, полагая $M_i = a_i(\mathbb{Z}^n)$, получим разложение $\mathbb{Z}^n = M_1 + M_2$. При этом если $z_i \in M_i$, то $a(z_i) = (-1)^i z_i$, поэтому данное разложение прямое, и в базисе решетки $\mathbb{Z}^n$, который является объединением базисов решеток M_1 и M_2, матрица a имеет требуемый вид.

Итак, пусть матрица $c \in GL_n(\mathbb{Z})$ выбрана таким образом, что $d = cac^{-1}$ имеет вид $\operatorname{diag}(\varepsilon_1, \ldots, \varepsilon_n)$, $\varepsilon_i = \pm 1$. Кроме того, поскольку $\varphi \in \operatorname{Ker}\delta$, можно выбрать такую матрицу $b \in G_{\mathcal{O}_{L_2}}$, что $a = b\sigma(b)^{-1}$. Тогда для матрицы $t = (t_{ij}) = c\sigma(b) \in \mathrm{GL}_n(\mathcal{O}_{L_2})$ имеем

$$\sigma(t) = \sigma(c\sigma(b)) = cb = ca\sigma(b) = dt,$$

т. е. $\sigma(t_{ij}) = \varepsilon_i t_{ij}$. Поэтому если $\varepsilon_i = -1$, то $t_{ij} \in \sqrt{2}\,\mathcal{O}_{L_2}$ для всех j. Но тогда $\det t \in \sqrt{2}\,\mathcal{O}_{L_2}$, что невозможно. Таким образом, все $\varepsilon_i = 1$, т. е. $a = E_n$. Мы показали, что гомоморфизм φ тривиален, и тем самым теорема 14 доказана.

В связи со следствием 1 из теоремы 13 и теоремой 14 было бы интересно выяснить, всегда ли для когомологий арифметических подгрупп односвязных групп выполняется принцип Хассе (в том смысле, как указано в следствии 1).

§ 8.5. Проблема рода

В § 8.1 мы дали общее определение рода и класса целочисленного элемента алгебраического многообразия относительно действия алгебраической группы и показали, что нахождение чисел классов в роде сводится к подсчету некоторых двойных классов. В настоящем параграфе, используя развитые методы вычисления чисел классов алгебраических групп, мы дадим оценки и характеризации чисел классов в роде в конкретных ситуациях.

Рассмотрим так называемую *проблему рода в арифметических группах*, исследование которой было начато Платоновым [8]. Пусть G — линейная алгебраическая группа, определенная над полем рациональных чисел $\mathbb{Q}$. Напомним (см. § 8.1), что два элемента $a, b \in G_{\mathbb{Z}}$ принадлежат одному роду, если они сопряжены в группах $G_{\mathbb{Q}}$ и $G_{\mathbb{Z}_p}$ для всех простых p, и одному классу, если они сопряжены в $G_{\mathbb{Z}}$. Обозначим через $[a]_G$ род элемента $a \in G_{\mathbb{Z}}$, и пусть $f_G(a)$ — число классов, содержащихся в $[a]_G$. Число $f_G(a)$ всегда конечно (см. предложение 6). Проблема рода заключается в исследовании свойств функции $f_G(a)$ $(a \in G_{\mathbb{Z}})$ и оказывается тесно связанной с задачей о финитной аппроксимируемости конечно порожденных линейных групп относительно сопряженности, с оценками чисел классов максимальных торов редуктивных групп и другими арифметическими и теоретико-групповыми вопросами.

Для коммутативных групп проблема рода является бессодержательной, поэтому наибольший интерес представляет исследование $f_G(a)$ для полупростой группы G. Оказывается, что в этой ситуации функция f_G является неограниченной на любой арифметической подгруппе $H \subset G_{\mathbb{Z}}$ при том естественном условии, что группа $G_{\mathbb{Z}}$ бесконечна, или, что эквивалентно (см. § 4.6), группа вещественных точек $G_{\mathbb{R}}$ некомпактна.

Теорема 15. *Пусть G — полупростая $\mathbb{Q}$-определенная алгебраическая группа такая, что группа вещественных точек $G_{\mathbb{R}}$ некомпактна. Тогда $\sup\limits_{a \in H} f_G(a) = \infty$ для любой арифметической подгруппы $H \subset G_{\mathbb{Z}}$*

Для $\mathbb{Q}$-изотропных групп теорема 15 была получена В. П. Платоновым [8]. Там же им была высказана гипотеза о справедливости теоремы 15 в общей ситуации. Для ортогональных групп над $\mathbb{Q}$ эта гипотеза была подтверждена

Г. В. Матвеевым [1]. В окончательной форме теорема 15 была установлена А. С. Рапинчуком [1].

Вначале проведем редукцию доказательства теоремы 15 к случаю односвязных $\mathbb{Q}$-простых групп.

Предложение 22. *Пусть* $\pi\colon \tilde{G} \to G$ — *$\mathbb{Q}$-определенная изогения $\mathbb{Q}$-групп. Тогда если для любой арифметической подгруппы* $\tilde{H} \subset \tilde{G}_{\mathbb{Z}}$ *имеем* $\sup\limits_{a \in \tilde{H}} f_{\tilde{G}}(a) = \infty$, *то и для любой арифметической подгруппы* $H \subset G_{\mathbb{Z}}$ *также* $\sup\limits_{a \in H} f_G(a) = \infty$.

Доказательство. Из непрерывности морфизма $\pi_A\colon \tilde{G}_A \to G_A$ и конечности группы $F = \operatorname{Ker}\pi$ вытекает существование такого открытого нормального делителя $U \subset \tilde{G}_{A(\infty)}$, содержащего G_∞, что $\pi_A(U) \subset G_{A(\infty)}$ и $U \cap F_{\mathbb{Q}} = \{1\}$. Индекс $[G_{A(\infty)} : U]$, очевидно, конечен; обозначим его через l. Далее, группа $\Gamma = \tilde{G}_{\mathbb{Q}} \cap U$ имеет конечный индекс в $\tilde{G}_{\mathbb{Z}} = \tilde{G}_{\mathbb{Q}} \cap \tilde{G}_{A(\infty)}$, поэтому из теоремы 4.1 получаем конечность индекса $[G_{\mathbb{Z}} : \pi(\Gamma)]$, который мы обозначим через m (отметим, что $\pi(\Gamma) \subset G_{\mathbb{Q}} \cap \pi_A(U) \subset G_{\mathbb{Q}} \cap G_{A(\infty)} = G_{\mathbb{Z}}$). Из теоремы 4.1 также вытекает, что прообраз $\pi^{-1}(H)$ любой арифметической подгруппы $H \subset G_{\mathbb{Z}}$ является арифметической подгруппой в $\tilde{G}$, поэтому группа $\tilde{H} = \pi^{-1}(H) \cap \Gamma \subset \tilde{G}_{\mathbb{Z}}$ арифметическая. Для доказательства предложения мы покажем, что если $a \in \tilde{H}$, то найдется $b \in [a]_{\tilde{G}}$ такой, что $f_G(\pi(b)) \geqslant \dfrac{f_{\tilde{G}}(a)}{ml}$.

Положим $t = f_{\tilde{G}}(a)$, и пусть $a_1 = a, a_2, \ldots, a_t$ — представители различных классов, содержащихся в $[a]_{\tilde{G}}$. Из определения рода вытекает, что для каждого $i = 1, \ldots, t$ найдется $g_i \in \tilde{G}_{A(\infty)}$ со свойством $a_i = g_i^{-1} a g_i$. Рассмотрим разбиение $\{1, \ldots, t\} = \bigcup\limits_{j=1}^{l} I_j$, считая, что индексы i_1, i_2 попадают в один и тот же класс I_j, если $g_{i_1} U = g_{i_2} U$. Тогда, очевидно, найдется такое j_0, что множество $I = I_{j_0}$ содержит не менее t/l элементов. Положим $b = a_i$, где $i \in I$, и покажем, что элемент b искомый. Для этого, во-первых, отметим, что поскольку $a \in \tilde{H} \subset U$, то для любого $i = 1, \ldots, t$ имеем $a_i = g_i^{-1} a g_i \in U \cap \tilde{G}_{\mathbb{Q}} = \Gamma$, ибо U — нормальный делитель в $\tilde{G}_{A(\infty)}$, так что $c_i = \pi(a_i) \in G_{\mathbb{Z}}$. Далее, по построению элементы a_i для $i \in I$ являются сопряженными в группе U, поэтому соответствующие c_i сопряжены в $\pi(U)$, и тем более — в группе $G_{A(\infty)}$. Кроме того, элементы a_i сопряжены в $\tilde{G}_{\mathbb{Q}}$, поэтому c_i сопряжены в $G_{\mathbb{Q}}$. Это рассуждение показывает, что элементы c_i для $i \in I$ лежат в одном роде,

т. е. $c_i \in [\pi(b)]_G$. Для доказательства неравенства $f_G(\pi(b)) \geqslant [I]/m \geqslant t/ml$ теперь достаточно найти среди элементов c_i, $i \in I$, не менее $[I]/m$ элементов, которые не сопряжены в $G_{\mathbb{Z}}$. С этой целью мы опять рассмотрим разбиение $I = \bigcup_{k=1}^{s} J_k$, относя индексы i_1, $i_2 \in I$ в один класс, если элементы c_{i_1}, c_{i_2} сопряжены в $G_{\mathbb{Z}}$. Покажем, что для любого k имеем $[J_k] \leqslant m$. Тогда $s \geqslant [I]/m$, и с другой стороны, $f_G(\pi(b)) \geqslant s$, что и даст требуемое. Предположим, что $[J_k] > m$. Зафиксируем некоторый индекс $i_0 \in J_k$ и для каждого $i \in J_k$ найдем элемент $z_i \in G_{\mathbb{Z}}$ со свойством $c_i = z_i^{-1} c_{i_0} z_i$. Поскольку индекс $[G_{\mathbb{Z}} : \pi(\Gamma)]$ равен m, для двух различных i_1, $i_2 \in J_k$ имеем $z_{i_1} = z_{i_2}\pi(g)$ для подходящего $g \in \Gamma$. Тогда $c_{i_1} = z_{i_1}^{-1} c_{i_0} z_{i_1} = \pi(g)^{-1} z_{i_2}^{-1} c_{i_0} z_{i_2} \pi(g) = \pi(g)^{-1} \times c_{i_2}\pi(g)$. Вспоминая, что $c_i = \pi(a_i)$, получим $\pi(a_{i_1}) = \pi(g^{-1} a_{i_2} g)$, т. е. $x = a_{i_1}^{-1} g^{-1} a_{i_2} g \in F_{\mathbb{Q}}$. С другой стороны, из наших построений и того факта, что U является нормальным делителем в $\tilde{G}_{A(\infty)}$, вытекает включение $x \in U$. Поэтому $x \in U \cap F_{\mathbb{Q}} = \{1\}$, и, следовательно, $a_{i_1} = g^{-1} a_{i_2} g$, — противоречие, ибо элементы a_i не являются сопряженными в $G_{\mathbb{Z}}$ и тем более в Γ. Предложение 22 доказано.

Пусть теперь G — произвольная полупростая $\mathbb{Q}$-определенная группа с некомпактной группой $\mathbb{R}$-точек. Обозначим через π: $\tilde{G} \to G$ универсальное $\mathbb{Q}$-определенное накрытие. Тогда из предложения 22 вытекает, что достаточно доказать теорему 15 для группы $\tilde{G}$. Но $\tilde{G}$ является прямым произведением своих $\mathbb{Q}$-простых компонент G^i, причем для некоторого i_0 группа $G^{i_0}_{\mathbb{R}}$ некомпактна. Утверждается, что если теорема 15 справедлива для G^{i_0}, то она справедлива и для $\tilde{G}$. В самом деле, из предложения 22 вытекает, что справедливость теоремы 15 для группы $\tilde{G}$ не зависит от ее реализации, поэтому мы можем зафиксировать реализацию $\tilde{G}$, которая является прямым произведением реализаций компонент. Тогда $\tilde{G}_{\mathbb{Z}} = \prod_i G^i_{\mathbb{Z}}$, $\tilde{G}_{\mathbb{Z}_p} = \prod_i G^i_{\mathbb{Z}_p}$ для любого p, откуда следует, что для любого $a \in \tilde{G}_{\mathbb{Z}}$ справедливо неравенство $f_{\tilde{G}}(a) \geqslant f_{G^{i_0}}(\mathrm{pr}_{i_0}(a))$, где pr_{i_0}: $\tilde{G} \to G^{i_0}$ — соответствующая проекция. Так как для произвольной арифметической подгруппы $H \subset \tilde{G}_{\mathbb{Z}}$ группа $H' = \mathrm{pr}_{i_0}(H) \subset G^{i_0}_{\mathbb{Z}}$ является арифметической (теорема 4.1), то доказав, что $\sup_{a \in H'} f_{G^{i_0}}(a) = \infty$, мы докажем также, что $\sup_{a \in H} f_{\tilde{G}}(a) = \infty$.

Таким образом, достаточно доказать теорему 15 для $\mathbb{Q}$-простых односвязных групп. Покажем, что в этом случае справедливо более точное утверждение:

Предложение 23. *Пусть G — почти $\mathbb{Q}$-простая односвязная алгебраическая группа с некомпактной группой $\mathbb{R}$-точек. Тогда для любой арифметической подгруппы $H \subset G_{\mathbb{Z}}$ и любого натурального r найдется такой элемент $a \in H$, что $f_G(a)$ делится на r.*

Доказательство опирается на следующие два факта:

Предложение 24. *Пусть T — нецентральный K-определенный тор связной K-группы G. Тогда для любого натурального r существует такой элемент $g \in G_K$, что число классов $\mathrm{cl}(g^{-1}Tg)$ делится на r.*

Лемма 18. *В условиях предложения 23 существует такой полупростой элемент $\varepsilon \in G_{\mathbb{Z}}$, что элемент ε^m регулярен для любого натурального m.*

Доказательство. Пусть G является линейной группой степени n, т. е. $G \subset \boldsymbol{GL}_n$. Хорошо известно, что функция Эйлера обладает свойством $\varphi(r) \xrightarrow[r\to\infty]{} \infty$, поэтому существует такое $t \in \mathbb{N}$, что $\varphi(r) > n!$ при $r > t$. Положим $d = t!$ и рассмотрим отображение τ_d: $G \to G$, определяемое формулой $\tau_d(x) = x^d$. Если теперь обозначить через G_s множество всех полупростых элементов группы G, через U — открытое плотное по Зарисскому подмножество в G, состоящее из регулярных полупростых элементов (см. § 2.1, п. 11), то, очевидно, $\tau_d(G_s) = G_s \supset U$, в частности, $\tau_d(G)$ плотно в G. Но $G_{\mathbb{Z}}$ также плотно в G (теорема 4.10), поэтому, окончательно, $\tau_d(G_{\mathbb{Z}})$ является плотным подмножеством в G. В силу открытости U пересечение $U \cap \tau_d(G_{\mathbb{Z}})$ содержит хотя бы один элемент θ. Покажем, что если $\theta = \tau_d(\varepsilon)$, где $\varepsilon \in G_{\mathbb{Z}}$, то элемент ε искомый.

Пусть T — максимальный тор группы G, содержащий ε. Согласно критерию регулярности (см. § 2.1, п. 11), элемент $x \in T$ регулярен в том и только том случае, если $\alpha(x) \neq 1$ для любого корня $\alpha \in R(T, G)$, поэтому нам надо показать, что $\rho = \alpha(\varepsilon)$ не является корнем из единицы. Установим вначале, что ρ принадлежит расширению $F = \mathbb{Q}(\varepsilon_1, \ldots, \varepsilon_n)$ поля $\mathbb{Q}$, порожденному собственными значениями $\varepsilon_1, \ldots, \varepsilon_n$ элемента ε. Действительно, по определению, в алгебре $\mathfrak{g} = L(G)$ найдется такой ненулевой элемент X, что $\varepsilon^{-1}X\varepsilon = \alpha(\varepsilon)X$. Приведем ε к диагональному виду, т. е. найдем такую матрицу $z \in \boldsymbol{GL}_n$, что $\xi = z^{-1}\varepsilon z$ является диагональной матрицей $\mathrm{diag}(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$. Тогда для элемента $Y = z^{-1}Xz$ должно выполняться соотношение $\xi^{-1}Y\xi = \alpha(\varepsilon)Y$. Поэтому если $Y = (y_{ij})$ и $y_{i_0j_0} \neq 0$, то $\alpha(\varepsilon) = \varepsilon_{i_0}^{-1}\varepsilon_{j_0} \in F$. Поле F является полем разложения многочлена степени n с рациональными коэффициентами (характеристического многочлена ε), поэтому $[F : \mathbb{Q}] \leqslant n!$. С другой стороны, если $\rho^r = 1$, причем r — минимальное число с таким свойством, то $[\mathbb{Q}(\rho) : \mathbb{Q}] = \varphi(r)$, откуда $\varphi(r) \leqslant n!$. По построению отсюда по-

лучаем, что $r \leqslant t$, и, следовательно, r является делителем $d = t!$. Поэтому $\alpha(\theta) = \alpha(\varepsilon^d) = \rho^d = 1$, что противоречит регулярности θ. Лемма 18 доказана.

Доказательство предложения 24 мы проведем позднее, а сейчас завершим доказательство предложения 23. Пусть ε — элемент, построенный в лемме 18. Тогда централизатор $T = Z_G(\varepsilon)$ является максимальным тором в G. Действительно, в силу регулярности ε связная компонента $Z_G(\varepsilon)^0$ является максимальным тором, но известно (см. Стейнберг [2]), что в односвязном случае централизаторы полупростых элементов связны. Заметим, что в силу регулярности ε^m для любого m централизатор $Z_G(\varepsilon^m)$ также равен T.

Зафиксируем теперь произвольное натуральное число r. Согласно предложению 24 найдется такой элемент $g \in G_{\mathbb{Q}}$, что число классов $\mathrm{cl}(g^{-1}Tg)$ делится на r. Из предложения 4.1 вытекает, что группа $D = g^{-1}G_{\mathbb{Z}}g$ является арифметической в G, откуда следует, что индекс $[D : D \cap H]$ конечен. Выберем нормальный делитель $N \subset D$ конечного индекса, содержащийся в $D \cap H$, и обозначим через l экспоненту группы D/N. Тогда $\zeta = g^{-1}\varepsilon^l g \in H$ и число $f_G(\zeta)$ классов в роде делится на r. Действительно, в условиях предложения 23 для группы G имеет место свойство сильной аппроксимации, поэтому $\mathrm{cl}(G) = 1$, и, следовательно, $f_G(\zeta) = \mathrm{cl}(Z_G(\zeta))$ (предложение 6). Но $Z_G(\zeta) = g^{-1}Z_G(\varepsilon^l)g = g^{-1}Tg$, и число классов $\mathrm{cl}(g^{-1}Tg)$ делится на r. Таким образом, предложение 23, а вместе с тем и теорема 15 доказаны.

Доказательство предложения 24. Пусть реализация $G \subset \boldsymbol{GL}_n$ задается решеткой $L \subset K^n$, и P — поле разложения тора T. Поскольку тор T нецентрален в G, его присоединенное действие на соответствующей алгебре Ли $\mathfrak{g} = L(G)$ нетривиально. Следовательно, найдутся такой неединичный характер $\alpha \in \mathbf{X}(T)$ и такой ненулевой элемент $X \in \mathfrak{g}$, что $\mathrm{Ad}(t)(X) = \alpha(t)X$ для всех $t \in T$. При этом, поскольку характер α определен над P, элемент X можно выбрать из $\mathfrak{g}_P$. Пусть l — такое натуральное число, что пересечение $\mathbf{X}(T) \cap \mathbb{Q}\alpha$ порождается характером $\beta = \frac{1}{l}\alpha$. Так как $\alpha \neq 1$, то элемент X нильпотентен ($X^n = 0$), и можно рассмотреть «усеченное» экспоненциальное отображение

$$\varphi(a) = \sum_{m=0}^{n-1} \frac{a^m X^m}{m!}, \tag{1}$$

которое задает P-определенный морфизм алгебраических групп $\varphi\colon \boldsymbol{G}_a \to \boldsymbol{GL}_n$ (см. § 2.1, п. 8). Пусть $W = \varphi(\boldsymbol{G}_a)$ — соответствующая одномерная унипотентная подгруппа. Тогда алгебра Ли $L(W)$ порождается X, и, следовательно, $L(W) \subset \mathfrak{g}$, $W \subset G$. Ясно также, что обратный к φ морфизм $\psi\colon W \to \boldsymbol{G}_a$ задается

«усеченным» логарифмическим отображением:

$$\psi(u) = \sum_{m=1}^{n-1} (-1)^{m+1} \frac{(u-1)^m}{m}. \tag{2}$$

При этом для любых $a \in G_a$, $t \in T$, имеем

$$t^{-1}\varphi(a)\,t = \varphi(\alpha(t)\,a). \tag{3}$$

Пусть $e_1, \ldots, e_n$ — базис пространства P^n, в котором элементы тора T записываются диагональными матрицами; обозначим через M порожденную этим базисом $\mathcal{O}_P$-решетку. Пусть S состоит из всех таких $v \in V_f^K$, что для некоторого продолжения $w|v$ нарушается хотя бы одно из условий:

(i) $\{a \in P_w \mid aX \in M_n(\mathcal{O}_{P_w})\} = \mathcal{O}_{P_w}$,

(ii) $M_w = \mathcal{O}_{P_w} L$,

(iii) $w((n-1)!\,l) = 0$.

Легко видеть, что множество S конечно, поэтому из теоремы плотности Чеботарева вытекает бесконечность множества

$$V_0 = \{v \in V_f^K \setminus S \mid P \subset K_v\}.$$

Лемма 19. 1) *Для любого $v \notin S$ и любого $g \in G_{K_v}$ справедливо включение $g(g^{-1}Tg)_{\mathcal{O}_v} g^{-1} \subset T_{\mathcal{O}_v}$.*

2) *Если $v \in V_0$, то $\alpha(T_{\mathcal{O}_v}) = U_v^1$, где U_v — группа v-адических единиц.*

3) *Для $v \in V_0$ положим $g = \varphi(\pi_v^{-1})$. Тогда $\alpha\left(g(g^{-1}Tg)_{\mathcal{O}_v} g^{-1}\right) \subset U_v^{(1)}$ (здесь π_v — униформизующий элемент, $U_v^{(1)} = \{a \in U_v \mid a \equiv 1 \pmod{\mathfrak{p}_v}\}$).*

Доказательство. 1) Рассмотрим произвольный P-определенный изоморфизм $T \xrightarrow{\sim} D_r$ с группой диагональных матриц. При доказательстве следствия 2 в § 8.4 мы видели, что если привести T к диагональному виду, то этот изоморфизм становится определенным над $\mathcal{O}_P$. Следовательно, для любого $w \in V^P$ имеем $T_{\mathcal{O}_{P_w}}^{M_w} \xrightarrow{\sim} (D_r)_{\mathcal{O}_{P_w}}$. Но $(D_r)_{\mathcal{O}_{P_w}}$, очевидно, является единственной максимальной компактной подгруппой в $(D_r)_{P_w}$ (т. е. содержит любую компактную подгруппу), поэтому $T_{\mathcal{O}_{P_w}}^{M_w}$ обладает аналогичным свойством в T_{P_w}. Таким образом,

$$g(g^{-1}Tg)_{\mathcal{O}_v} g^{-1} \subset T_{\mathcal{O}_{P_w}}^{M_w} \cap T_{K_v} = T_{\mathcal{O}_v},$$

ибо $M_w = \mathcal{O}_{P_w} L_v$ в силу условия $v \notin S$.

2) Из наших построений вытекает существование такого базиса $\chi_1, \ldots, \chi_r$ группы $\boldsymbol{X}(T)$, что $\chi_1 = \beta$. Тогда в силу теоремы 2.1 найдется такой P-определенный изоморфизм $T \xrightarrow{\sim} D_r$, при котором характеру χ_1 отвечает базисный характер $\zeta_1 \in \mathbf{X}(D_r)$, определенный формулой $\zeta_1(\operatorname{diag}(x_1, \ldots, x_r)) = x_1$. Так как $v \in V_0$, т. е. $v \notin S$ и $P_w = K_v$, то из доказательства п. 1) вытекает, что изоморфизм $T \xrightarrow{\sim} D_r$ индуцирует изоморфизм $T_{\mathcal{O}_v} \xrightarrow{\sim} (D_r)_{\mathcal{O}_v}$, откуда $\beta(T_{\mathcal{O}_v}) = U_v$ и $\alpha(T_{\mathcal{O}_v}) = U_v^t$.

3) Если $t \in g(g^{-1}Tg)_{\mathcal{O}_v} g^{-1}$, то $g^{-1}tg \in G_{\mathcal{O}_v}$, причем согласно п. 1) одновременно $t \in G_{\mathcal{O}_v}$. Используя (3), тогда получим, что

$$t^{-1}g^{-1}tg = \varphi(1 - \alpha(t)\pi_v^{-1}) \in G_{\mathcal{O}_v}.$$

В силу условия (iii) знаменатели всех членов разложения (2) являются v-целыми, поэтому

$$\psi(t^{-1}g^{-1}tg)X = (1 - \alpha(t))\pi_v^{-1}X \in M_n(\mathcal{O}_v).$$

Но тогда из условия (i) вытекает, что $(1 - \alpha(t))\pi_v^{-1} \in \mathcal{O}_v$, т. е. $\alpha(t) \equiv 1 \pmod{\mathfrak{p}_v}$. Лемма 19 доказана.

Искомые элементы $g \in G_K$ в предложении 26 мы построим, аппроксимируя подходящим образом элементы $\varphi(\pi_v^{-1})$. Более точно, для каждого $v_0 \in V$ найдем элемент $g(v_0) \in G_K$ со свойствами $g(v_0) \in \varphi(\pi_{v_0}^{-1}) G_{\mathcal{O}_{v_0}}$ и $g(v_0) \in G_{\mathcal{O}_v}$ для $v \in S$. Такой элемент всегда существует, даже если G не обладает свойством слабой аппроксимации. Действительно, пусть $G = HR_u(G)$ — разложение Леви группы G, $B = [H, H]$ — полупростая часть H и θ: $\tilde{B} \to B$ — универсальное K-определенное накрытие. Используя θ, определим действие $\tilde{B}$ на $R_u(G)$ и рассмотрим изогению τ: $\tilde{D} = \tilde{B}R_u(G) \to BR_u(G) = D$ соответствующих полупрямых произведений. Поскольку фактор $G/D = H/B$ является тором, то унипотентный элемент $x_{v_0} = \varphi(\pi_{v_0}^{-1})$ лежит в D. Далее, рассуждая как и в § 7.2, легко показать, что на самом деле $x_{v_0} \in \tau(\tilde{D}_{K_{v_0}})$. Пусть $x_{v_0} = \tau(y_{v_0})$, $y_{v_0} \in \tilde{D}_{K_{v_0}}$. Выберем открытые подгруппы $E_v \subset \tilde{D}_{K_v}$ для $v \in \{v_0\} \cup S$ таким образом, чтобы $\tau(E_v) \subset G_{\mathcal{O}_v}$. Из предложения 7.9 вытекает, что группа $\tilde{D}$ всегда обладает свойством слабой аппроксимации, и, значит, можно найти элемент $h \in \tilde{D}_K$ со следующими свойствами: $h \in y_{v_0}E_{v_0}$ и $h \in E_v$ для $v \in S$. Тогда элемент $g(v_0) = \tau(h)$ будет искомым. Покажем, что для подходящего $v_0 \in V_0$ число классов $\operatorname{cl}(g(v_0)^{-1}Tg(v_0))$ делится на любое наперед заданное натуральное число r.

Лемма 20. *Число* $c(v_0) = \mathrm{cl}\,(g(v_0)^{-1}Tg(v_0))$ *делится на индекс* $[U^l_{v_0} : \Gamma U^{(1)}_{v_0}]$, *где* $\Gamma = \alpha(T_0)$.

Доказательство. Положим $C_v = g(v_0)\,(g(v_0)^{-1}Tg(v_0))_{\mathcal{O}_v}\,g(v_0)^{-1}$ для $v \in V_f^K$. Тогда $c(v_0)$, очевидно, совпадает с индексом $[T_A : CT_K]$, где $C = T_\infty \times \prod_{v \in V_f^K} C_v$. Из утверждения 1) леммы 19 вытекает, что для $v \notin S$ имеет место включение $C_v \subset T_{\mathcal{O}_v}$. Однако по построению $g(v_0) \in G_{\mathcal{O}_v}$ для $v \in S$, и поэтому последнее включение сохраняется и для $v \in S$. Тем самым $C \subset T_{A(\infty)}$, и можно проделать следующие преобразования:

$$c(v_0) = [T_A : CT_K] = [T_A : T_{A(\infty)}T_K]\,[T_{A(\infty)}T_K : CT_K] =$$
$$= \mathrm{cl}\,(T)\,[T_{A(\infty)} : T_{A(\infty)} \cap (CT_K)] = \mathrm{cl}\,(T)\,[T_{A(\infty)} : CT_{\mathcal{O}}].$$

Проектируя на v_0-компоненту, получим, что $[T_{A(\infty)} : CT_{\mathcal{O}}]$ делится на $[T_{\mathcal{O}_{v_0}} : C_{v_0}T_{\mathcal{O}}]$. Наконец, применяя α и используя утверждения 2), 3) предыдущей леммы, получаем требуемое утверждение (отметим, что $U^{(1)}_{v_0} \subset U^l_{v_0}$ в силу условия $v(l) = 0$). Лемма 20 доказана.

Теперь уже легко завершить доказательство предложения 24. По теореме 4.20 группа $T_{\mathcal{O}}$ является конечно порожденной. Пусть $a_1, \ldots, a_s$ — конечная система образующих группы $\Gamma = \alpha(T_{\mathcal{O}})$. Положим $d = lr$ и, пользуясь теоремой плотности Чеботарева, найдем $v_0 \in V_f^K \setminus S$, взаимно простое с r и такое, что $P\left(\rho_d, \sqrt[d]{a_1}, \ldots, \sqrt[d]{a_s}\right) \subset K_{v_0}$, где ρ_d — примитивный корень степени d из единицы. Тогда, очевидно, $v_0 \in V_0$. Покажем, что индекс $[U^l_{v_0} : \Gamma U^{(1)}_{v_0}]$ делится на r. Факторгруппа $U_{v_0}/U^{(1)}_{v_0}$ изоморфна мультипликативной группе $k^*_{v_0}$ соответствующего поля вычетов и поэтому является циклической. Обозначим через Σ циклическую подгруппу порядка d в K_{v_0}, порожденную ρ_d. Так как $U^{(1)}_{v_0}$ является про-p-группой относительно простого p, отвечающего v_0, и $v_0(d) = 0$, то $\Sigma \cap U^{(1)}_{v_0} = (1)$, откуда вытекает, что факторгруппа $U_{v_0}/U^{(1)}_{v_0}$ содержит изоморфный образ Σ и, следовательно, имеет порядок, делящийся на d. Но тогда порядок факторгруппы $U^l_{v_0}/U^d_{v_0}$ равен r. С другой стороны, по построению $\Gamma U^{(1)}_{v_0} \subset U^d_{v_0}$, так что индекс $[U^l_{v_0} : \Gamma U^{(1)}_{v_0}]$ делится на r. Предложение 24 доказано.

Из предложения 24, в частности, непосредственно вытекает характеризация чисел классов алгебраических торов.

Предложение 25. *Пусть* $T \subset \boldsymbol{GL}_n$ — *алгебраический тор положительной размерности. Тогда*

(i) *если T совпадает с тором S, состоящим из скалярных матриц, то для любой решетки $L \subset K^n$ число классов* $\mathrm{cl}(T^L)$ *равно числу классов идеалов h_K поля K;*

(ii) *если $T \neq S$, то для любого натурального r существует такая решетка $L(r) \subset K^n$, что число классов* $\mathrm{cl}(T^{L(r)})$ *делится на r.*

Теперь мы в состоянии дать ответ на основной вопрос настоящей главы: какие значения может принимать число классов $\mathrm{cl}(\varphi(G))$ алгебраической группы G для всевозможных реализаций φ.

Теорема 16. *Пусть G — редуктивная алгебраическая K-группа степени n. Тогда*

(i) *если G является полупростой группой некомпактного типа, то число классов* $\mathrm{cl}(\varphi(G))$ *для любой реализации φ имеет вид $p_1^{\alpha_1}, \ldots, p_r^{\alpha_r}$, где $p_1, \ldots, p_r$ — различные простые делители порядка фундаментальной группы G, причем все числа такого вида действительно реализуются для подходящих φ;*

(ii) *в противном случае для любого натурального r найдется решетка $L(r) \subset K^{2n}$ такая, что число классов* $\mathrm{cl}(G^{L(r)})$ *делится на r.*

Доказательство. Числа классов полупростых групп некомпактного типа были определены нами в теореме 5. Утверждение пункта (ii) для полупростых групп смешанного типа доказано в теореме 7. Случай, когда G — алгебраический тор, рассмотрен в предложении 25. Разобрать оставшийся случай почти прямого произведения тора на полупростую группу мы предоставляем читателю в качестве итогового упражнения к настоящей главе. Следует еще раз обратить внимание читателя на то обстоятельство, что при изучении чисел классов мы вынуждены были «раздувать» исходную реализацию. Поэтому в качестве ближайшей задачи здесь следует сформулировать задачу вычисления $\mathrm{cl}(\varphi(G))$ для того случая, когда степень φ и степень линейной группы G совпадают.

Теорема 15 имеет одно интересное применение к абстрактной теории групп (см. Платонов, Матвеев [1]). Напомним, что абстрактная группа Γ называется *финитно аппроксимируемой относительно сопряженности*, если любые ее два элемента сопряжены в Γ в том и только том случае, если сопряжены их образы во всех конечных факторгруппах Γ (другими словами, если классы сопряженности в Γ являются замкнутыми относительно проконечной топологии Γ). Это понятие оказывается полезным при исследовании алгоритмических проблем, в частности, известно, что в любой конечно определенной финитно аппроксимируемой относительно сопряженности группе положительно решается проблема сопряженности. Указанное свойство имеет место для свободных групп, для полициклических групп

и групп некоторых других классов (см. Ремесленников [1]). В то же время теорема 15 позволяет строить большие серии примеров арифметических групп, которые не являются финитно аппроксимируемыми относительно сопряженности.

Пусть G — односвязная $\mathbb{Q}$-простая алгебраическая группа с некомпактной группой $\mathbb{R}$-точек. Чтобы сформулировать условия, при которых группа $\Gamma = G_{\mathbb{Z}}$ не является финитно аппроксимируемой относительно сопряженности, нам понадобятся некоторые элементарные сведения по так называемой конгруэнц-проблеме, обзор которой мы дадим в § 9.5. Ниже через τ_a и τ_c мы будем обозначать соответственно арифметическую и конгруэнц-топологии и через $C = C(\Gamma)$ — соответствующее конгруэнц-ядро (отметим, что $C = C^{VK}_{\infty}(G)$ в обозначениях § 9.5).

Предложение 26. *Если в описанной выше ситуации конгруэнц-ядро $C(\Gamma)$ центрально, то группа $\Gamma = G_{\mathbb{Z}}$ не является финитно аппроксимируемой относительно сопряженности.*

Доказательство. Известно (см. § 9.5), что из центральности конгруэнц-ядра $C(\Gamma)$ вытекает его конечность. Поэтому если обозначить через $\hat{\Gamma}$ пополнение Γ относительно τ_a, то найдется открытый нормальный делитель $N \subset \Gamma$ такой, что $N \cap C(\Gamma) = \{1\}$; положим $d = [\hat{\Gamma} : N]$. Мы покажем, что если $a \in \Gamma$ и $a_1, \ldots, a_r$ принадлежат роду $[a]_G$, то найдется такое подмножество $I \subset \{1, \ldots, r\}$ мощности $[I] \geqslant r/d^2$, что для $i, j \in I$ элементы a_i, a_j сопряжены в $\hat{\Gamma}$. Прежде всего заметим, что из сильной аппроксимационной теоремы вытекает, что пополнение $\bar{\Gamma}$ группы Γ относительно τ_c совпадает с $\prod_p G_{\mathbb{Z}_p}$, так что принадлежность a_i одному роду влечет их сопряженность в $\bar{\Gamma}$. Отсюда следует, что для любого $i = 1, \ldots, r$ найдутся $z_i \in \hat{\Gamma}$, $c_i \in C(\Gamma)$ со свойством $z_i^{-1} a_i z_i = c_i a_i$. Введем разбиение $\{1, \ldots, r\} = \bigcup_{k=1}^{t} I_k$, относя индексы i, j к одному классу, если $a_i \in a_j N$, $z_i \in z_j N$. Очевидно, что число t таких классов не превосходит d^2 и поэтому среди I_k найдется множество I мощности $[I] \geqslant r/d^2$. Покажем, что множество I — искомое.

Действительно, для $i, j \in I$ из наших определений получаем, что $c_i = z_i^{-1} a_i z_i a_i^{-1} \in (z_j^{-1} a_i z_j a_j^{-1}) N = c_j N$, откуда $c_j^{-1} c_i \in N \cap C(\Gamma) = \{1\}$, т. е. $c_j = c_i$. Тогда для элемента $s = z_i^{-1} z_j$ с учетом центральности $C(\Gamma)$ имеем $s^{-1} a_i s = c_i^{-1} s^{-1} (c_i a_i) s = c_i^{-1} z_j^{-1} z_i z_i^{-1} a_i z_i z_i^{-1} z_j = c_i^{-1} z_j^{-1} a_i z_j = c_i^{-1} c_j a_j = a_j$, что и требовалось.

По теореме 15 найдется $a \in G_{\mathbb{Z}}$ с числом классов в роде $r = f_G(a) > d^2$. Пусть $a_1, \ldots, a_r$ — представители непересекаю-

щихся классов рода $[a]_G$ и $I \subset \{1, \ldots, r\}$ — построенное выше подмножество мощности $|I| \geqslant r/d^2 > 1$. Тогда для $i, j \in I$, $i \neq j$, элементы a_i и a_j сопряжены в $\tilde{\Gamma}$, т. е. их образы сопряжены во всех конечных факторгруппах группы Г. С другой стороны, по построению a_i, a_j лежат в разных классах и, следовательно, не сопряжены в Г. Предложение 26 доказано.

Из предложения 26 и известных результатов по конгруэнц-проблеме (см. § 9.5) вытекает, что если, например, $G = \mathbf{R}_{K/Q}(\boldsymbol{SL}_n)$, где $n \geqslant 3$, K — любое поле алгебраических чисел, то группа $\Gamma = G_{\mathbf{Z}}$ не является финитно аппроксимируемой относительно сопряженности, ибо здесь $C(\Gamma)$ либо тривиально, либо является центральной циклической подгруппой. При этом следует отметить, что поскольку, вообще говоря, $C(\Gamma) \neq 1$, то для доказательства предложения 26 недостаточно построения элементов $a \in G_{\mathbf{Z}}$ с $f_G(a) > 1$, т. е. элементов, для которых нарушается локально-глобальный принцип относительно сопряженности, а требуется утверждение теоремы 15 о существовании $a \in G_{\mathbf{Z}}$ с произвольно большим $f_G(a)$.

Замечание. Как мы увидим в § 9.5, конгруэнц-проблему естественно исследовать в более общем контексте S-арифметических подгрупп, ибо тогда условие центральности соответствующего конгруэнц-ядра гипотетически можно выразить в единообразном виде $\operatorname{rang}_S G = \sum_{v \in S} \operatorname{rang}_{K_v} G \geqslant 2$ и $\operatorname{rang}_{K_v} G \geqslant 1$ для $v \in S \setminus V_\infty^K$. В связи с этим укажем, что все результаты настоящего параграфа без всяких изменений распространяются на эту ситуацию. При этом вместо обычных двойных классов $G_{A(\infty)} \backslash G_A / G_K$ приходится работать с двойными классами $G_{A(S)} \backslash G_A / G_K$. Методика подсчета этих классов практически не отличается от развитых в § 8.2—8.4 методов вычисления обычных чисел классов, и поэтому все результаты главы, включая обобщающую теорему 16, имеют свои S-арифметические аналоги.

Кроме проблемы рода в арифметических группах мы рассмотрим *проблему рода для целочисленных представлений* конечных групп (соответствующие определения см. в § 8.1). Хотя последовательное изложение теории целочисленных представлений не входит в наши цели (см., например, Кэртис, Райнер [1]), мы остановимся на этой теме по двум причинам. Во-первых, она доставляет пример эффективного использования групп аделей и чисел классов алгебраических групп в этой, казалось бы, далекой от арифметики алгебраических групп области. Во-вторых, ответ на проблему рода здесь диаметрально противоположен теореме 15, а именно, основной результат утверждает равномерную ограниченность чисел классов в роде всех целочисленных представлений данной конечной группы Г (среди которых, вообще говоря, имеется бесконечное число неэквивалентных,

см. Кэртис, Райнер [1], § 8.1 А). Излишне говорить, что ввиду краткости нашего экскурса в теорию целочисленных представлений изложение здесь приобретает эскизный характер.

Теорема 17. *Пусть* Γ — *конечная группа. Тогда существует эффективно определяемая константа* t *такая, что число классов в роде любого целочисленного представления* Γ *не превосходит* t.

Доказательство (Платонов [1]). Пусть $\rho\colon \Gamma \to GL_n(\mathbb{Z})$ — произвольное целочисленное представление, $G = Z_{GL_n}(\rho(\Gamma))$ — его централизатор. Мы уже знаем (см. предложение 5), что число классов в роде представления ρ совпадает с числом классов $\mathrm{cl}(G^L)$, где $L = \mathbb{Z}^n$, поэтому наша цель — получить оценку для $\mathrm{cl}(G^L)$, которая бы не зависела от ρ, а определялась только свойствами Γ. Даже поверхностное знакомство с теорией представлений конечных групп подсказывает, что ответ должен быть связан со свойствами соответствующей групповой алгебры $D = \mathbb{Q}[\Gamma]$. По теореме Машке алгебра D полупроста, т. е. имеет вид $D = \bigoplus_{i=1}^{d} M_{n_i}(T_i)$, где T_i — некоторые алгебры с делением над $\mathbb{Q}$. В действительности алгебры T_i взаимно однозначно соответствуют классам эквивалентности R_i неприводимых над $\mathbb{Q}$ представлений группы Γ, а именно, если $\rho_i \in R_i$ и $\rho_i\colon \Gamma \to GL_{l_i}(\mathbb{Q})$, то T_i — централизатор $\rho_i(\Gamma)$ в $M_{l_i}(\mathbb{Q})$. (Эти и некоторые другие факты из теории представлений, которые понадобятся нам в доказательстве, читатель может найти у Кэртиса и Райнера [1].) Если рассмотреть ρ как представление над полем $\mathbb{Q}$, то имеет место разложение в прямую сумму

$$\rho = \bigoplus_{i=1}^{d}\left(\bigoplus_{j=1}^{m_i} \rho_j\right), \quad m_i \geqslant 0.$$

Тогда группа G является алгебраической $\mathbb{Q}$-группой следующего вида: $G = \prod_{i=1}^{d} \mathbf{R}_{K_i/\mathbb{Q}}(\boldsymbol{GL}_{m_i}(T_i))$, где K_i — центр T_i и группа $\boldsymbol{GL}_0$ над любым телом считается тривиальной. Мы стремимся получить оценку для $\mathrm{cl}(G^L)$, которая была бы независима от m_i. Для этого в каждой группе $G_i = \mathbf{R}_{K_i/\mathbb{Q}}(\boldsymbol{GL}_{m_i}(T_i))$ рассмотрим подгруппу

$$H_i = \begin{pmatrix} \mathbf{R}_{K_i/\mathbb{Q}}(\boldsymbol{GL}_1(T_i)) & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$$

и положим $H = \prod_{i=1}^{d} H_i$.

Лемма 21. *Для любой решетки $M \subset \mathbb{Q}^n$ справедливо неравенство* $\mathrm{cl}(G^M) \leqslant \mathrm{cl}(H^M)$.

Доказательство. Для каждого $i = 1, \ldots, d$ обозначим через F_i подгруппу $\mathbf{R}_{K_i/\mathbb{Q}}(\boldsymbol{SL}_{m_i}(T_i)) \subset G_i$, если $m_i > 1$, и положим $F_i = (1)$ в противном случае. Очевидно, $F = \prod_{i=1}^{d} F_i$ является нормальным делителем в G. Покажем, что $G_A = F_A H_A$. Достаточно установить, что $G_{i_A} = F_{i_A} H_{i_A}$ для любого i. Если $m_i \leqslant 1$, то $G_i = H_i$, и доказывать нечего, поэтому можно предполагать, что $m_i > 1$. Обозначив через D_i алгебру $M_{m_i}(T_i)$, центр которой есть K_i, очевидно, будем иметь $\mathrm{Nrd}_{D_i/K_i}(GL_{m_i}(T_i)) = \mathrm{Nrd}_{D_i/K_i}(GL_1(T_i))$, где $GL_1(T_i)$ естественным образом вложено в $GL_{m_i}(T_i)$, Nrd_{D_i/K_i} — гомоморфизм приведенной нормы. Аналогичное равенство сохраняет силу и при замене основного поля на произвольное расширение $P/\mathbb{Q}$, откуда $G_{i_P} = F_{i_P} H_{i_P}$. В частности, для любого простого p имеет место разложение $G_{i_{\mathbb{Q}_p}} = F_{i_{\mathbb{Q}_p}} H_{i_{\mathbb{Q}_p}}$. Кроме того, для почти всех p группу $G_{i_{\mathbb{Q}_p}}$ можно отождествить с группой $GL_s(K_i \otimes \mathbb{Q}_p)$, где $s = m_i b$, b — индекс тела T_i, $H_{i_{\mathbb{Q}_p}}$ — с подгруппой

$$\begin{pmatrix} GL_b(K_i \otimes \mathbb{Q}_p) & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix},$$

откуда следует, что $G_{i_{\mathbb{Z}_p}} = F_{i_{\mathbb{Z}_p}} H_{i_{\mathbb{Z}_p}}$. Поэтому $G_{i_A} = F_{i_A} H_{i_A}$, что и требовалось. Из наших построений вытекает, что группа F_i обладает свойством абсолютной сильной аппроксимации, поэтому, применяя к разложению $G_A = F_A H_A$ рассуждение из доказательства предложения 5.4, мы и получим требуемое неравенство. Лемма 21 доказана.

Дальнейшие рассуждения связаны с использованием результатов о порядках в полупростых алгебрах (см. § 1.5, п. 3). Целочисленное групповое кольцо $\Delta = \mathbb{Z}[\Gamma]$ является порядком в алгебре $D = \mathbb{Q}[\Gamma]$ и поэтому содержится в некотором максимальном порядке $\tilde{\Delta}$. Положим $f = [\tilde{\Delta} : \Delta]$; тогда $f\tilde{\Delta} \subset \Delta$. Продолжим ρ до представления алгебры D. Так как ρ является целочисленным представлением Γ, то $\rho(\Delta) L = L$, и поэтому

$$M = \rho(\tilde{\Delta}) L \subset \frac{1}{f} \rho(\Delta) L = \frac{1}{f} L. \tag{4}$$

В частности, M является решеткой, причем, очевидно, $\rho(\tilde{\Delta}) \subset \mathrm{End}(M)$. Обозначим через C централизатор $\rho(D)$ в $M_n(\mathbb{Q})$.

Тогда алгебра C имеет следующую структуру: $C=\bigoplus_{i=1}^{d} M_{m_i}(T_i)$; ясно также, что для любого расширения $P/\mathbb{Q}$ группа G_P совпадает с группой обратимых элементов алгебры $C\otimes_{\mathbb{Q}} P$. Пусть Θ — централизатор $\rho(\tilde{\Delta})$ в $\mathrm{End}(M)$; можно показать, что Θ является максимальным порядком в C. Чтобы получить оценку числа классов группы G, нам потребуется совершить переход от порядка Θ к порядку $\Phi\subset C$, который имеет вид $\bigoplus_{i=1}^{d} M_{m_i}(\mathcal{O}_i)$, где $\mathcal{O}_i$ — некоторый максимальный порядок в T_i. Порядок Φ является максимальным в C, так что для любого p порядки $\Theta_p=\Theta\otimes_{\mathbb{Z}}\mathbb{Z}_p$, $\Phi_p=\Phi\otimes_{\mathbb{Z}}\mathbb{Z}_p$ являются максимальными порядками в $C_p=C\otimes_{\mathbb{Q}}\mathbb{Q}_p$. Следовательно, по теореме о сопряженности максимальных порядков в полупростых алгебрах над локальным полем найдется такой $g_p\in C_p^*=G_{\mathbb{Q}_p}$, что $g_p\Theta_p g_p^{-1}=\Phi_p$. При этом для почти всех p имеем $\Theta_p=\Phi_p$, и можно положить $g_p=1$.

Обозначим через g элемент из G_A, p-компонента которого совпадает с g_p, а вещественная компонента равна единице. Положим $L_1=g(L)$, $M_1=g(M)$ в смысле определенного в § 8.1 действия группы $GL_n(A)$ на решетках в пространстве $\mathbb{Q}^n$. Тогда, используя лемму 21, получим

$$\mathrm{cl}\,(G^L)=\mathrm{cl}\,(G^{L_1})\leqslant \mathrm{cl}\,(H^{L_1}). \tag{5}$$

Утверждается, что $H_{\mathbb{Z}_p}^{L_{1p}}\subset H_{\mathbb{Z}_p}^{M_{1p}}$ для всех p, и, следовательно, $H_{A(\infty)}^{L_1}\subset H_{A(\infty)}^{M_1}$. В самом деле, достаточно показать, что $G_{\mathbb{Z}_p}^{L_{1p}}\subset G_{\mathbb{Z}_p}^{M_{1p}}$. Имеем $G_{\mathbb{Z}_p}^{L_{1p}}=g_pG_{\mathbb{Z}_p}^{L_p}g_p^{-1}$, $G_{\mathbb{Z}_p}^{M_{1p}}=g_pG_{\mathbb{Z}_p}^{M_p}g_p^{-1}$, поэтому все сводится к доказательству включения $G_{\mathbb{Z}_p}^{L_p}\subset G_{\mathbb{Z}_p}^{M_p}$. Но любой элемент из $G_{\mathbb{Z}_p}^{L_p}$ перестановочен с $\rho(\tilde{\Delta})$ и поэтому оставляет на месте также решетку $M_p=\rho(\tilde{\Delta})L_p$, что и требовалось. Таким образом, используя (5), получаем

$$\mathrm{cl}\,(G^L)\leqslant \mathrm{cl}\,(H^{L_1})\leqslant \mathrm{cl}\,(H^{M_1})\left[H_{A(\infty)}^{M_1}:H_{A(\infty)}^{L_1}\right]. \tag{6}$$

Рассмотрим, далее, отдельно каждый сомножитель. По построению, для любого p группа $G_{\mathbb{Z}_p}^{M_p}$ совпадает с Θ_p^*, поэтому группа $G_{\mathbb{Z}_p}^{M_{1p}}=g_pG_{\mathbb{Z}_p}^{M_p}g_p^{-1}$ совпадает с Φ_p^*. Отсюда следует, что $H_{\mathbb{Z}_p}^{M_{1p}}$ естественно изоморфно $\prod_{i,\ m_i\neq 0}\mathcal{O}_{ip}^*$. Таким образом, число $\mathrm{cl}\,(H^{M_1})$ оценивается сверху произведением $h=\prod_{i=1}^{d}h_i$, где h_i есть число двойных смежных классов $(\mathcal{O}_i\otimes_{\mathbb{Z}}A(\infty))^*\backslash(T_i\otimes_{\mathbb{Q}}A)^*/T_i^*$.

Некоммутативный аналог предложения 1 показывает, что h_i совпадает с так называемым числом классов идеалов тела T_i, которое не зависит от выбора максимального порядка $\mathcal{O}_i$ (подробности см. в книге Дойринга [1]).

Чтобы оценить второй сомножитель в (6), заметим, что из (4) вытекают включения $fM_1 \subset L_1 \subset M_1$. Отсюда следует, что для любого p группа $H_{\mathbf{Z}_p}^{L_{1p}}$ содержит конгруэнц-подгруппу $H_{\mathbf{Z}_p}^{M_{1p}}(f) = H_{\mathbf{Z}_p}^{M_{1p}} \cap (E_n + f\,\mathrm{End}\,(M_{1p}))$. Действительно, для любого $g \in H_{\mathbf{Z}_p}^{M_{1p}}(f)$ и любого $l \in L_{1p}$ имеем

$$g(l) = (g - E_n)(l) + l \in fM_{1p} + l \subset L_{1p},$$

что и требовалось. Поэтому, отождествляя, как и выше, $H_{\mathbf{Z}_p}^{M_{1p}}$ с $\prod_{i,\, m_i \neq 0} \mathcal{O}_{ip}^*$, мы видим, что индекс $\left[H_{A(\infty)}^{M_1} : H_{A(\infty)}^{L_1}\right]$ оценивается произведением $k = \prod_{i=1}^{d} k_i$, где $k_i = \prod_p [\mathcal{O}_{ip}^* : \mathcal{O}_{ip}^* \cap \cap (1 + f\mathcal{O}_{ip})]$ (отметим, что число k_i также не зависит от выбора максимального порядка $\mathcal{O}_i \subset T_i$). Таким образом, окончательно получаем, что в качестве константы t в теореме 17 можно взять $t = hk$. Доказательство завершено.

Отметим, что приведенное доказательство теоремы 17 сохраняет силу и для целочисленных представлений произвольного полупростого $\mathbf{Z}$-кольца Δ, ибо тот факт, что $\Delta = \mathbf{Z}[\Gamma]$, фактически не использовался.

Библиографические замечания. Проблема изучения числа классов в роде квадратичных форм и чисел классов идеалов числовых полей рассматривалась еще Гауссом [1]. Число появившихся с тех пор работ, посвященных этим вопросам, огромно. В них рассматриваются самые разные аспекты проблемы — от определения числа классов в конкретных ситуациях до получения асимптотических оценок чисел классов определенных совокупностей форм, полей и т. д. Настоящая глава посвящена изложению результатов, связанных с обобщением понятия числа классов на призвольные алгебраические группы. Тот факт, что числа классов в роде объектов арифметического типа связаны с числами классов соответствующих алгебраических групп (теорема 2), хорошо известен, однако в такой общности, по-видимому, нигде не отмечался. Эта связь была эффективно использована Кнезером [1] для полного описания чисел классов в роде неопределенных квадратичных форм (теорема 6). Дальнейшие результаты по описанию чисел и групп классов полупростых групп некомпактного типа были получены в цикле работ Платонова, Бондаренко, Рапинчука [1—3]. Кроме полного доказательства теоремы о реализации, эти работы содержат теорему о неограниченности в совокупности чисел классов групп без

свойства абсолютной сильной аппроксимации, оценки чисел классов максимальных торов, а также ряд примеров и приложений полученных результатов к решению классических арифметических задач (в частности, к подсчету числа классов в роде решеток на полной матричной алгебре относительно сопряженности). В работе [3] было также начато исследование чисел классов в роде полупростых групп смешанного типа на решетках удвоенной размерности. В исходной размерности для групп компактного типа такое исследование было выполнено Рапинчуком [2], что позволило, в частности, получить характеризацию чисел классов в роде положительно определенных квадратичных форм. Заключительный параграф главы содержит решение проблемы рода в арифметических группах, полученное Рапинчуком [1], и эффективную оценку числа классов в роде целочисленных представлений данной конечной группы, принадлежащую Платонову [2].

ГЛАВА IX

НОРМАЛЬНОЕ СТРОЕНИЕ ГРУПП РАЦИОНАЛЬНЫХ ТОЧЕК АЛГЕБРАИЧЕСКИХ ГРУПП

Основные результаты этой главы концентрируются вокруг следующей проблемы: пусть G — простая односвязная алгебраическая группа, определенная над полем алгебраических чисел K; что можно сказать о строении группы K-рациональных точек G_K? Из большого круга возникающих здесь вопросов выделяют проблему изучения нормального строения группы G_K. В этом видится как дань алгебраической традиции, восходящей к работам Артина и Дьедонне по изучению нормального строения группы $SL_n(D)$ и других классических групп, так и выполнение «заказа» смежных дисциплин, в частности, теории автоморфных функций, теории представлений групп и др. Как мы указывали в гл. VII, следует различать случаи, когда G является соответственно K-изотропной и K-анизотропной. Если в первом случае основные усилия были направлены на доказательство для G гипотезы Кнезера — Титса (см. теорему 1), то для K-анизотропных групп ситуация долгое время оставалась неясной даже с принципиальной точки зрения. Так, до 1979 г. единственным результатом по этой проблеме была работа М. Кнезера [2] 1956 г., посвященная изучению спинорных групп квадратичных форм. В последнее десятилетие работа в этом направлении заметно активизировалась, в чем немалую роль сыграла гипотеза, содержащая критерий проективной простоты группы G_K, которую первый автор выдвинул на Международном математическом конгрессе в Ванкувере (1974 г.). Мы начинаем изложение с обсуждения этой гипотезы и ее обобщений, а затем переходим к имеющимся в настоящее время результатам (§ 9.1). Дальнейшие § 9.2—9.4 посвящены доказательству сформулированных в § 9.1 теорем. Следует отметить, что речь здесь идет о результатах, которые были получены в самое последнее время (вплоть до 1989 г. включительно) и по своему характеру являются весьма сложными. Поэтому изложение в этих параграфах приближается к стилю журнальной статьи и становится более насыщенным. Кроме того, чтобы не отходить от основной линии рассуждений, мы ряд вспомогательных утверждений оставляем читателю в качестве упражнений. Одним словом, требования к читателю здесь несколько выше, чем в остальной части книги. С другой стороны, внимательный читатель получит на наш взгляд необходимую подготовку для самостоятельной работы в этой области. Наконец, в § 9.5 мы даем обзор последних результатов по так называемой конгруэнц-проблеме.

§ 9.1. Основные гипотезы и результаты

В этой главе через G, как правило, будет обозначаться простая односвязная алгебраическая группа, определенная над полем алгебраических чисел K. Основной интересующий нас вопрос заключается в следующем: когда группа K-рациональных точек G_K не имеет нецентральных нормальных подгрупп? Более общая проблема связана с описанием всевозможных нормальных подгрупп в G_K. Аналогичные проблемы можно ставить и над произвольным полем K, однако в такой общности они представляются малореальными. (Отметим также, что вряд ли разумно обсуждать их для более широкого класса групп, чем мы условились выше, ибо при наличии у G разрешимого радикала задача становится малосодержательной, в то время как случай полупростых групп фактически сводится к простым). Ситуация в случае числового поля представляется более обнадеживающей, ибо здесь гипотетически возможен переход от локального изучения нормального строения к глобальному. Соответствующая гипотеза была сформулирована В. П. Платоновым [11].

Гипотеза 1. *Группа G_K проективно проста (т. е. проста ее факторгруппа $G_K/Z(G_K)$ по центру*)) в том и только том случае, когда для всех $v \in V^K$ проективно просты локальные группы G_{K_v}.*

В такой форме эта гипотеза представляет качественно новый вариант локально-глобального принципа, пронизывающего всю арифметическую теорию алгебраических групп. Его предшествовавшие формы были связаны с локально-глобальными изоморфизмами объектов и поэтому, как правило, сводились к доказательству инъективности некоторых отображений для когомологий (см. гл. VI). Здесь же гипотетически утверждается возможность локально-глобального перехода относительно абстрактной простоты группы — свойства, никак априори не выразимого через когомологические инварианты.

Можно дать эквивалентную формулировку гипотезы 1: если G — абсолютно простая односвязная K-группа, то группа G_K проективно проста в том и только том случае, когда для всех $v \in V_f^K$ группа G является K_v-изотропной. Действительно, для $v \in V_\infty^K$ группа G_{K_v} всегда является проективно простой (предложение 7.6), поэтому остается показать, что для $v \in V_f^K$ проективная простота группы G_{K_v} равносильна K_v-изотропности G. В одну сторону это следует из доказательства гипотезы Кнезера — Титса над неархимедовыми локальными полями (теоре-

*) Отметим, что фактически в приводимых ниже теоремах мы рассматриваем проективную простоту в более сильном смысле, а именно, как отсутствие собственных нецентральных нормальных подгрупп, однако данная формулировка представляется нам более изящной.

ма 7.6). Обратная импликация вытекает из того факта, что для K_v-анизотропной группы G группа G_{K_v} является компактной (теорема 3.1) и, следовательно, проконечной (см. § 3.3). Поэтому G_{K_v} обладает базой окрестностей единицы, состоящей из нормальных подгрупп, и о простоте G_{K_v} не может быть и речи. Кроме того, если $N \subset G_{K_v}$ — открытая нормальная подгруппа (а таковой является произвольная нецентральная нормальная подгруппа в G_{K_v}, см. теорему 3.3), то пересечение $N_1 = N \cap G_K$ является нормальной подгруппой в G_K. При этом из свойства слабой аппроксимации для G (предложение 7.9) вытекает, что $G_{K_v} = NG_K$, откуда $G_{K_v}/N \simeq G_K/N_1$. Таким образом, любая собственная нецентральная нормальная подгруппа группы G_{K_v} высекает собственную нормальную подгруппу группы G_K (отметим, что в силу предложения 3.17 N имеет конечный индекс в G_{K_v}, и поэтому N_1 всегда бесконечна); тем самым установлена необходимость условий гипотезы I для проективной простоты G_K. Более того, если условия гипотезы 1 нарушаются, то из предыдущего вытекает, что группа G_K вместе с группой G_{K_v} обладает такой системой нормальных подгрупп $\mathfrak{N} = \{N\}$ конечного индекса, что $\bigcap\limits_{N \in \mathfrak{N}} N = (1)$, т. е. G_K является финитно аппроксимируемой.

Рассуждения предыдущего абзаца допускают следующее уточнение. Если для $v \in V_f^K$ группа G является K_v-анизотропной, то $G \simeq \boldsymbol{SL}_1(D)$ над K_v, где D — конечномерная центральная алгебра с делением над K_v (теорема 6.5). Но тогда в силу результатов п. 4 § 1.4 группа $G_{K_v} \simeq SL_1(D)$ является проразрешимой. Поэтому в случае нарушения условий гипотезы 1 группа G_K аппроксимируется нормальными подгруппами конечного индекса с разрешимой факторгруппой и, в частности, $G_K \neq [G_K, G_K]$.

Итак, если группа G является K_v-изотропной для всех $v \in V_f^K$ (а это всегда так, если тип группы G отличен от A_n), то гипотетически группа G_K проективно проста. В общем случае следует рассмотреть множество $T = \{v \in V_f^K \mid G - K_v\text{-анизотропна}\}$; из теоремы 6.7 вытекает, что множество T всегда конечно. Если $T \neq \varnothing$, то, как мы отмечали выше, для любого $v \in T$ группа G_{K_v} обладает базой окрестностей единицы, состоящей из нормальных подгрупп, каждая из которых «высекает» нетривиальную нормальную подгруппу группы G_K. Легко видеть, что аналогичное утверждение имеет место и в том случае, если вместо индивидуальной группы G_{K_v} рассмотреть произведение $G_T = \prod\limits_{v \in T} G_{K_v}$, а именно, G_T обладает базой окрест-

ностей единицы, состоящей из нормальных подгрупп, и каждая собственная открытая нормальная подгруппа $H \subset G_T$ определяет собственную нормальную подгруппу $N = G_K \cap H$. Так как для $v \in T$ группа G_{K_v} изоморфна группе типа $SL_1(D)$, то результаты п. 4 § 1.4 (в частности, теорема 1.10) дают описание нормальных подгрупп в локальной ситуации. Поэтому нормальное строение группы G_K можно считать изученным, если известно, что все нецентральные нормальные подгруппы G_K получаются указанным выше способом.

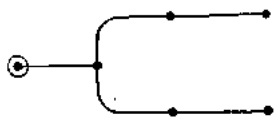
Гипотеза 2 (Маргулис [3]). *Для любой нецентральной нормальной подгруппы N группы G_K найдется такая открытая нормальная подгруппа $H \subset G_T$, что $N = G_K \cap \delta^{-1}(H)$, где δ: $G_K \to G_T$ — диагональное вложение.*

Гипотеза 2 имеет характер конгруэнц-проблемы для групп рациональных точек, обсуждение которой для S-арифметических групп мы дадим в § 9.5. Отметим также, что в случае $T = \varnothing$ (в частности, если тип G отличен от A_n) гипотезы 1 и 2 фактически эквивалентны.

Цель настоящей главы — изложить имеющиеся в настоящее время результаты по этим гипотезам. Прежде всего необходимо различать два случая, когда G является соответственно K-изотропной и K-анизотропной. В первом случае изучение нормального строения группы G_K сводится к вопросу о справедливости для G гипотезы Кнезера — Титса (см. § 7.2), и для числовых полей имеем следующий результат, близкий к окончательному.

Теорема 1. *Пусть G — простая односвязная алгебраическая группа, определенная и изотропная над полем алгебраических чисел K. Предположим, что тип G отличен от ${}^2E_6$. Тогда $G_K = G_K^+$, и, следовательно, группа G_K не имеет собственных нецентральных подгрупп.*

Основные моменты доказательства этой теоремы для групп классических типов мы изложили в § 7.2. Для групп исключительных типов рассуждения носят переборный характер, причем в силу теоремы 7.4 достаточно ограничиться рассмотрением групп K-ранга 1. К сожалению, полное изложение этой части доказательства до сих пор не опубликовано (хотя и обещано Прасадом и Рагунатаном в статье [3]), но его можно восстановить, используя доклад Титса [4] на семинаре Бурбаки. Случай K-формы типа ${}^2E_6$ K-ранга 1 с диаграммой Титса



пока не рассмотрен.

Пусть теперь G — простая односвязная K-анизотропная группа. Труднее всего поддаются исследованию группы типа A_n, причем для большинства внешних форм типа A_n какие-либо результаты в настоящее время (1989 г.) вообще отсутствуют. Поэтому предположим, что G — внутренняя форма типа A_n. Тогда $G = \boldsymbol{SL}_1(D)$, где D — конечномерная центральная алгебра с делением над K. В этой ситуации введенное перед формулировкой гипотезы 2 множество T совпадает с множеством таких $v \in V_f^K$, что алгебра $D_v = D \otimes_K K_v$ остается алгеброй с делением. Полный ответ на гипотезу 2 получен лишь для тела кватернионов.

Теорема 2. *Пусть D — тело кватернионов над K, $G = \boldsymbol{SL}_1(D)$. Тогда для G_K выполняется гипотеза 2. В частности, если $T = \varnothing$, то группа G_K не имеет собственных нецентральных нормальных подгрупп.*

(Отметим, что предположение о проективной простоте группы $SL_1(D)$, где D — тело кватернионов, для которого $T = \varnothing$, высказанное М. Кнезером в работе [2], оставалось недоказанным почти 25 лет! Обратим также внимание читателя на тот факт, что рассмотренными в теореме 2 группами исчерпываются все анизотропные группы типа A_1.)

Для тел произвольного индекса имеется пока лишь следующий частичный результат:

Теорема 3. *Пусть N — нормальная подгруппа группы G_K, для которой выполняется утверждение гипотезы 2. Тогда для коммутанта $[N, N]$ также выполняется утверждение гипотезы 2.*

Для удобства ссылок сформулируем отдельно теорему 3 для $N = G_K$.

Теорема 4. *В описанной ситуации*

$$[G_K, G_K] = G_K \cap \prod_{v \in T} [G_{K_v}, G_{K_v}].$$

В частности, если $T = \varnothing$, то $G_K = [G_K, G_K]$.

Исторически доказательство этих теорем было получено в несколько этапов. Вначале Платонов, Рапинчук [1] получили доказательство теоремы 4 для случая D — тело кватернионов, $T = \varnothing$. При этом была развита мультипликативная арифметика тел кватернионов, используя которую, Маргулис [4] доказал теорему 2. В дальнейшем нам удалось обобщить методы и результаты работы [1] на тела произвольного индекса. А именно, была развита мультипликативная арифметика тел произвольного индекса, которая была применена для доказательства теоремы 4 при одном небольшом ограничении: предполагалось, что $v((n, 2)) = 0$ для $v \in T$, где n — индекс тела D. Наконец, Рагунатан [7] показал, что это условие является излишним, и вывел из теоремы 4 более общую теорему 3.

Доказательству теорем 2—4 посвящен § 9.2. Вначале доказывается наиболее сложная в техническом плане теорема 4. Здесь рассуждения следуют общей схеме из работы Платонова, Рапинчука [4] с некоторыми модификациями, при помощи которых, во-первых, снимается налагавшееся ранее условие на тело D, а во-вторых, сводится к минимуму использование теории полей классов. В частности, в приводимом варианте доказательства не используется теорема Грюнвальда — Ванга, играющая в несколько обобщенной форме ключевую роль в доказательстве Рагунатана [7]. Затем из теоремы 4 мы выводим теорему 3. Приводимое нами рассуждение является более прямым по сравнению с оригинальным рассуждением Рагунатана [7] и основано на установлении связи с так называемой метаплектической проблемой, рассматриваемой в § 9.5. В заключение, следуя Маргулису [4], мы доказываем теорему 2.

Изучению нормального строения групп рациональных точек алгебраических групп, относящихся к другим классическим типам, посвящен § 9.3. Основной результат здесь может быть сформулирован следующим образом.

Теорема 5. *Пусть G — простая односвязная алгебраическая K-группа одного из следующих типов: B_l $(l \geqslant 2)$, C_l $(l \geqslant 2)$, D_l $(l \geqslant 4$, кроме ${}^3D_4$ и ${}^6D_4)$, либо специальная унитарная группа $\boldsymbol{SU}_m(L, f)$ невырожденной m-мерной эрмитовой формы f над квадратичным расширением L/K, относящаяся к типу ${}^2A_{m-1}$ $(m \geqslant 3)$. Тогда группа G_K не имеет собственных нецентральных нормальных подгрупп, в частности, справедлива гипотеза* 1.

В таком завершенном виде эта теорема, по-видимому, публикуется впервые. Путь к ее доказательству занял более чем тридцатилетний исторический промежуток от работы Кнезера [2], относящейся к 1956 г., до нынешнего времени. Ключевую роль в рассуждениях играет наличие у рассматриваемых групп удобной геометрической реализации как группы автоморфизмов некоторых векторных пространств над телом, снабженных эрмитовой либо косоэрмитовой формой. Этот подход был реализован Кнезером [2] для доказательства проективной простоты групп рациональных точек спинорных групп $G = \boldsymbol{Spin}(f)$ невырожденных квадратичных форм от $n \geqslant 5$ переменных, которые относятся к типу $B_{\frac{n-1}{2}}$ при нечетном n и к типу $D_{\frac{n}{2}}$ при четном n. Случай групп типа C_l и специальных унитарных групп $\boldsymbol{SU}_m(L, f)$ типа ${}^2A_{m-1}$, связанных с квадратичным расширением L/K и невырожденной эрмитовой формой f, был рассмотрен М. В. Боровым [1]. Затем В. И. Черноусовым [4] была получена редукция доказательства теоремы 5 для групп типа D_l $(l \geqslant 4)$ к группам типа $D_3 = A_3$. Окончательный результат для групп типа D_l был независимо получен Томановым [2] и Боро-

вым [3]. При этом рассуждения Томанова являются прямыми аналогами рассуждений Кнезера [2], в то время как Боровой [3] развивает метод своей более ранней работы [1]. Ключевое наблюдение состоит в том, что в действительности можно редуцировать доказательство теоремы 5 для групп типа D_l не просто к группам типа $D_3 = A_3$, а к группам этого типа, изоморфным $\boldsymbol{SU}_4(L, f)$, которые были разобраны ранее. (Отметим, что используя это замечание, можно довести до конца и рассуждение Черноусова [4].)

Мы даем новое доказательство теоремы 5, которое хотя и использует некоторые моменты упомянутых выше работ (в большей степени это относится к работам Борового [1], [3]), но отличается от них прежде всего своим универсальным характером, исключающим необходимость специального изучения каждого типа. В целом рассуждение носит индуктивный характер, причем роль базы индукции играет теорема 2 (напомним, что $B_1 = C_1 = A_1$, $D_2 = A_1 + A_1$), а индуктивный шаг обосновывает теорема 13.

Метод доказательства теоремы 5 применим не только к группам классических типов. Так, применяя его к 7-мерному представлению группы типа G_2, мы получаем следующий результат:

Теорема 6. *Пусть G — простая K-определенная группа типа G_2. Тогда группа G_K проективно проста.*

Таким образом, остаются не рассмотренными группы типов E_6, E_7, E_8, F_4. Изучение этих типов осложняется тем обстоятельством, что удобные геометрические реализации для групп серии E отсутствуют. Доказательство проективной простоты групп K-рациональных точек простых групп трех последних типов, полученное Черноусовым [3], [5], явилось довольно неожиданным. А именно, используя некоторые методы, развитые им ранее в [2] для исследования рациональности многообразий вещественных алгебраических групп, Черноусов доказал следующую теорему:

Теорема 7. *Пусть G — простая односвязная алгебраическая группа ранга $l \geqslant 2$, определенная и анизотропная над полем K, но разложимая над некоторым квадратичным расширением L/K. Тогда группа G_K не имеет собственных нецентральных нормальных подгрупп, и, в частности, проективно проста.*

K-формы, к которым применима теорема 7, существуют у групп всех типов, отличных от A_1. С другой стороны, любая K-группа, относящаяся к одному из типов B_l, C_l, E_7, E_8, F_4, G_2, всегда разложима над некоторым квадратичным расширением поля K (предложение 6.17). Так как для K-изотропных групп этих типов отсутствие нецентральных нормальных подгрупп G_K уже доказано (теорема 1), то из теоремы 7 получаем

Следствие. *Группы K-рациональных точек простых односвязных групп типов B_l $(l \geqslant 2)$, C_l $(l \geqslant 2)$, E_7, E_8, F_4, G_2 не имеют собственных нецентральных нормальных подгрупп.*

Тем самым для групп G типов B_l, C_l $(l \geqslant 2)$ мы получаем еще одно доказательство проективной простоты G_K. В § 9.4 мы приводим модифицированное доказательство теоремы 7. Как и первоначальное доказательство Черноусова (см. [3], [5]), оно имеет индуктивный характер, причем индукция ведется по рангу l рассматриваемой группы начиная с $l=2$. Так как имеется всего лишь три типа простых групп ранга 2 (A_2, $B_2=C_2$, G_2), причем K-анизотропная группа типа A_2, разложимая над квадратичным расширением L/K, — это в точности группа $\boldsymbol{SU}_3(L, f)$, то базу индукции дают теоремы 5, 6.

Подводя итоги, мы видим, что если оставить в стороне случай групп типа A_l $(l \geqslant 2)$, то к настоящему времени гипотезы 1, 2 доказаны для всех групп, за исключением некоторых форм типов ${}^3D_4$, ${}^6D_4$ и E_6. Поэтому, оценивая перспективы, следует подчеркнуть, что основной задачей в данном направлении является завершение исследования групп типа A_l, относящихся как к внутренним формам, для которых известные результаты собраны в теоремах 2—4, так и к внешним формам этого типа, для которых аналогичные результаты пока не получены.

Несмотря на различие методов, применяемых в каждом из § 9.2—9.4, доказательства всех результатов используют аппроксимационные соображения. По этой причине мы выносим следующие два результата, которые будут многократно использоваться в дальнейшем, в настоящий вводный параграф.

Пусть G — простая односвязная алгебраическая K-группа, $T=\{v \in V_f^K \mid G_{K_v} - K_v\text{-анизотропна}\}$. Для любой нецентральной нормальной подгруппы $N \subset G_K$ и любого конечного подмножества $S \subset V^K$ обозначим через N_S замыкание N в группе $G_S = \prod_{v \in S} G_{K_v}$.

Лемма 1. 1) *N_S является открытой нормальной подгруппой в G_S.*

2) *$N_S = N_{T \cap S} \times G_{S \setminus (T \cap S)}$; в частности, если $T \cap S = \varnothing$, то $N_S = G_S$.*

Доказательство. В силу предложения 7.9, G_K плотно в G_S, поэтому N_S является нормальной подгруппой в группе G_S. Для $v \in S$ группа G_{K_v} естественным образом вкладывается в G_S, и можно рассмотреть взаимный коммутант $W_v = [N_S, G_{K_v}]$. Ясно тогда, что W_v является нормальным делителем в G_{K_v}, причем $W_v \not\subset Z(G_{K_v})$. Действительно, пусть $x \in N$ — нецентральный элемент и φ: $G \to G$ — отображение, определяемое формулой $\varphi(g) = [x, g]$. Поскольку $x \notin Z(G)$ и группа G связна,

то замыкание образа φ имеет положительную размерность. Но G_{K_v} плотно в G в топологии Зарисского (теорема 2.2), поэтому $\varphi(G_{K_v}) \subset W_v$ бесконечно; в частности, $W_v \not\subset Z(G_{K_v})$. Из теоремы 3.3 теперь вытекает открытость $W_v \subset G_{K_v}$. С другой стороны, в силу нормальности подгруппы N_S имеем $W_v \subset N_S$ для любого $v \in S$, так что $\prod_{v \in S} W_v \subset N_S$, и подгруппа N_S открыта. Если же $v \in S \setminus (T \cap S)$, то группа G_{K_v} не имеет нецентральных нормальных подгрупп, откуда $W_v = G_{K_v} \subset N_S$, и, значит, $G_{S \setminus (T \cap S)} \subset N_S$. Рассмотрим теперь проекцию N_S на $G_{S \cap T}$. Ее образ является открытой подгруппой в $G_{S \cap T}$ и одновременно содержит N в качестве плотной подгруппы, т. е. совпадает с $N_{T \cap S}$, что и доказывает лемму.

Лемма 2. *В вышеприведенных обозначениях следующие условия эквивалентны:*

(i) *N удовлетворяет конгруэнц-утверждению гипотезы 2;*

(ii) *N открыта в G_K в T-адической топологии;*

(iii) *N замкнута в G_K в T-адической топологии.*

Доказательство. Импликации (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) очевидны, поэтому докажем импликацию (iii) $\Rightarrow$ (i). Как и выше, обозначим через N_T замыкание N в группе G_T. Из леммы 1 вытекает, что N_T является открытой нормальной подгруппой в G_T, и поэтому N плотно в $G_K \cap N_T$ в T-адической топологии группы G_K. Тогда в силу (iii) имеем $N = G_K \cap N_T$, что означает справедливость для N конгруэнц-утверждения гипотезы 2 (а именно, ее утверждение выполняется для $H = N_T$). Лемма 2 доказана.

В заключение рассмотрим один качественный аспект проблемы изучения нормального строения групп рациональных точек. Из теоремы 3.1 вытекает, что для $v \in T$ группа G_{K_v} компактна, поэтому вся группа G_T также компактна. Предположим теперь, что для нормальной подгруппы $N \subset G_K$ выполняется конгруэнц-утверждение гипотезы 2, т. е. $N = G_K \cap H$ для некоторой открытой нормальной подгруппы $H \subset G_T$. Тогда из компактности G_T немедленно вытекает конечность индекса $[G_T : H]$, а следовательно, и конечность индекса $[G_K : N]$. Поскольку гипотеза 2 еще не доказана, естественно задаться вопросом, может ли группа G_K априори обладать нецентральными нормальными подгруппами бесконечного индекса? Ответ на этот вопрос дает следующая

Теорема 8 (Прасад [1], Маргулис [3]). *Пусть G — простая односвязная алгебраическая K-группа. Тогда любая нецентральная нормальная подгруппа группы G имеет в ней конечный индекс.*

Доказательство легко получается с помощью сильной аппроксимационной теоремы из следующего общего результата.

Теорема 9 (Маргулис [3]). *Пусть Γ — S-арифметическая подгруппа простой алгебраической K-группы G, где $S \subset V^K$ — некоторое конечное подмножество, содержащее V^K_∞. Если $\operatorname{rang}_S G = \sum_{v \in S} \operatorname{rang}_{K_v} G \geqslant 2$, то любая нормальная подгруппа группы Γ либо имеет в ней конечный индекс, либо содержится в центре группы G.*

Некоторые частные случаи теоремы 9 были известны до работы Маргулиса [3] и доказывались чисто алгебраическими методами. Так, при условии $\operatorname{rang}_K G \geqslant 2$ теорема 9 была получена Рагунатаном [4]. По-видимому, модификация рассуждений Рагунатана может привести к доказательству теоремы 9 для произвольной S-арифметической подгруппы в K-изотропной группе G при условии $\operatorname{rang}_S G \geqslant 2$. Однако эти методы оказываются неприменимыми в K-анизотропном случае. Рассуждения Маргулиса [3] имеют принципиально другую природу. Они основываются на том факте, что Γ является решеткой в группе G_S (теорема 5.7), и используют глубокие результаты теории меры и теории бесконечномерных представлений. Поскольку эти методы в данной книге не рассматриваются, мы, к сожалению, не сможем изложить здесь доказательство теоремы 9, отсылая читателя к оригинальной работе Маргулиса [3].

Приведем, однако, вывод теоремы 8 из теоремы 9. Введем такое конечное подмножество $S \subset V^K$, содержащее T и V^K_∞, что выполняются следующие условия:

(i) $\operatorname{rang}_S G \geqslant 2$;

(ii) пересечение $N \cap G_{\mathcal{O}(S)}$ не содержится в центре $Z(G)$ группы G.

Такое множество S легко построить, исходя из двух фактов: 1) для почти всех $v \in V^K_f$ группа G является K_v-изотропной, т. е. $\operatorname{rang}_{K_v}(G) \geqslant 1$; 2) если $x \in N \setminus Z(G)$, то $x \in G_{\mathcal{O}(S)}$ для достаточно большого S. Рассмотрим, далее, диагональное вложение группы G_K в группу S-аделей G_{A_S} и обозначим через $\overline{N}$ замыкание N в G_{A_S}. Тогда $\overline{N} = G_{A_S}$. Действительно, в силу сильной аппроксимационной теоремы G_K плотно в G_{A_S}, следовательно, $\overline{N}$ является нормальным делителем в G_{A_S}. Для любого $v \notin S$ группа G_{K_v} естественным образом вкладывается в G_{A_S}, причем взаимный коммутант $[G_{K_v}, \overline{N}]$ содержится в $\overline{N}$ и является нецентральной нормальной подгруппой в G_{K_v}. Но по построению $v \notin T$, так что группа G_{K_v} не имеет собственных нецентральных нормальных подгрупп (теорема 7.6), и, следовательно, $G_{K_v} \subset \overline{N}$. Из определения адельной топологии вытекает, что подгруппа в G_{A_S}, порожден-

ная всеми группами G_{K_v} ($v \notin S$), является плотной, поэтому окончательно $\bar{N} = G_{A_S}$. В частности,

$$G_{A_S} = N G_{A_S(S)}, \tag{1}$$

где $G_{A_S(S)}$ — группа S-целых аделей в G_{A_S}. Из (1) получаем, что $G_K = N G_{\mathcal{O}(S)}$, откуда $G_K/N \simeq G_{\mathcal{O}(S)}/N \cap G_{\mathcal{O}(S)}$. Остается заметить, что по построению $N \cap G_{\mathcal{O}(S)} \not\subset Z(G)$, так что в силу (i) и теоремы 9 последняя факторгруппа конечна. Поэтому факторгруппа G_K/N также конечна, и теорема 8 доказана.

Отметим, что теорема 8 играет существенную роль при доказательстве сформулированных выше теорем, в частности, теорем 2 и 5.

§ 9.2. Группы типа A_n

Всюду в этом параграфе через G будет обозначаться простая односвязная K-анизотропная группа, являющаяся внутренней формой типа A_{n-1}. Таким образом, $G = \boldsymbol{SL}_1(D)$, где D — конечномерная центральная алгебра с делением над K индекса n. Положим $T = \{v \in V_f^K \mid D_v = D \otimes_K K_v \text{ — тело}\}$. Как мы уже отмечали в § 9.1, имеющаяся к настоящему времени информация о нормальных подгруппах группы G_K заключена в теоремах 2—4, доказательству которых и посвящен настоящий параграф. Наши рассуждения базируются на использовании аппроксимационных теорем для группы G и некоторых норменных свойств максимальных подполей тела D, с которых мы и начинаем изложение.

Наиболее технически сложная часть доказательства теорем 2—4 заключена в следующем утверждении, для формулировки которого условимся в некоторых обозначениях. Зафиксируем произвольный нецентральный нормальный делитель $N \subset G_K = SL_1(D)$ и для $x \in D^*$ обозначим через $\Omega(x)$ подгруппу в D^*, порожденную мультипликативными группами всех максимальных подполей в D^* вида $K(xz)$, $z \in N$. Далее, пусть N_T — замыкание N в G_T и $\Omega_T(x)$ — подгруппа в $D_T^* = \prod_{v \in T} D_v^*$, порожденная произведениями $\prod_{v \in T} K_v[xz_v]^*$ такими, что $\bar{z} = (z_v) \in N_T$ и $K_v[xz_v]$ — максимальная полупростая коммутативная подалгебра в D_v для всех $v \in T$.

Теорема 10. $\mathrm{Nrd}_{D/K}(\Omega(x)) = \mathrm{Nrd}_{D/K}(D^*) \cap \mathrm{Nrd}_{D_T/K_T}(\Omega_T(x))$. (*Здесь через* Nrd_{D_T/K_T} *обозначено произведение отображений* Nrd_{D_v/K_v} *для* $v \in T$).

Покажем вначале, как теорема 10 выводится из следующего утверждения:

Предложение 1. *Положим* $T_0 = \{v \in V_f^K \mid D_v \not\simeq M_n(K_v)\}$. *Тогда для любого* $x \in D^*$

$$\mathrm{Nrd}_{D/K}(D^*) \cap \prod_{v \in T_0} K_v^{*\,m} \subset \mathrm{Nrd}_{D/K}(\Omega(x)), \qquad \text{где } m = n!.$$

Нам понадобятся две леммы.

Лемма 3. *Пусть* $v \in V^K$, $x \in D_v^*$ *и* $H \subset D_v$ — *максимальная полупростая коммутативная подалгебра. Тогда если* $\mathrm{Nrd}_{D_v/K_v}(x) \in \mathrm{Nrd}_{D_v/K_v}(H^*)$, *то* $H = K_v[xz]$ *для подходящего* $z \in G_{K_v}$. *В частности:*

1) *если* $D_v \simeq M_n(K_v)$, *то существует такой* $z \in G_{K_v}$, *что* $K_v[xz] \simeq K_v^n$;

2) *если* $v \in V_f^K \setminus T$, *то существует такой* $z \in G_{K_v}$, *что* $\mathrm{Nrd}_{D_v/K_v}(K_v[xz]^*) = K_v^*$.

Доказательство использует следующий факт: если $y \in H^*$, то для любой открытой подгруппы $R \subset G_{K_v}$ найдется $z \in R \cap H$ со свойством $H = K[yz]$. Для доказательства обозначим через B отвечающий H максимальный K_v-определенный тор группы $\boldsymbol{GL}_1(D)$, и пусть W — множество регулярных элементов в B; тогда W открыто в B в топологии Зарисского (см. § 2.1, п. 11). Поскольку $B = B_1 B_2$, где $B_1 = \boldsymbol{G}_m$, $B_2 = B \cap G$, то для любого $y \in B$ множество $W(y) = \{b \in B_2 \mid yb \in W\}$ непусто и открыто в B_2. С другой стороны, пересечение $B_2 \cap R$ является открытой в v-адической топологии подгруппой в B_{2K_v}, и, следовательно, плотно в B_2 в топологии Зарисского (лемма 3.2). Поэтому можно выбрать элемент $z \in W(y) \cap R$, который и будет искомым.

Из доказанного непосредственно вытекает справедливость первого утверждения леммы и п. 1), причем для доказательства п. 2) нам остается построить максимальную полупростую коммутативную подалгебру $H \subset D_v$ со свойством $\mathrm{Nrd}_{D_v/K_v}(H^*) = K_v^*$. Для этого представим алгебру D_v в виде $D_v = M_l(\Delta)$, где Δ — алгебра с делением над K_v. Так как $v \in V_f^K \setminus T$, то $l > 1$, и можно рассмотреть алгебру $H = E \oplus P^{l-1}$, где E (соответственно P) — максимальное неразветвленное (соответственно вполне разветвленное) подполе в Δ. Тогда $\mathrm{Nrd}_{D_v/K_v}(H^*)$ содержит группы $\mathrm{Nrd}_{\Delta/K_v}(E^*)$ и $\mathrm{Nrd}_{\Delta/K_v}(P^*)$. Но первая из них содержит группу v-адических единиц U_v, а вторая — униформизующий элемент поля K_v, так что в итоге $\mathrm{Nrd}_{D_v/K_v}(H^*) = K_v^*$. Лемма доказана.

Лемма 4. *Пусть* $x \in D^*$, $S \subset V^K$ — *конечное подмножество и для каждого* $v \in S$ *задана максимальная полупростая коммутативная* K_v-*подалгебра* $H_v \subset D_v$. *Предположим, что существует* $\bar{z} = (z_v) \in N_S$ *со свойством* $K_v[xz_v] \simeq H_v$ *для любого* $v \in S$. *Тогда найдется такой* $z \in N$, *что* $K_v[xz] \simeq H_v$ *для всех* $v \in S$.

Доказательство. Без ограничения общности можно считать, что $H_v = K_v[xz_v]$. Из доказательства предложения 6.13 вытекает, что множество Y_v таких $y \in D_v^*$, что алгебра $K_v[y]$ сопряжена в D_v алгебре H_v, открыто в D_v^*. Множество $Y = N_S \cap \left(\prod_{v \in S} x^{-1}Y_v\right)$ содержит $\bar{z}$ и поэтому является непустым открытым подмножеством в N_S. Следовательно, пересечение $Y \cap N$ непусто, и любой элемент $z \in Y \cap N$ будет искомым. Лемма доказана.

Пусть теперь $a \in \mathrm{Nrd}_{D/K}(D^*) \cap \mathrm{Nrd}_{D_T/K_T}(\Omega_T(x))$. Это значит, что существуют такие $\bar{z}_1, \ldots, \bar{z}_r \in N_T$, $\bar{z}_i = (z_{iv})$, что $a \in \mathrm{Nrd}_{D_T/K_T}(\bar{x}_1 \ldots \bar{x}_r)$, где $\bar{x}_i \in \prod_{v \in T} K_v[xz_{iv}]^*$, причем $K_v[xz_{iv}]$ — максимальная полупростая коммутативная подалгебра в D_v для всех $v \in T$, $i = 1, \ldots, r$. Используя лемму 4, найдем такие элементы $z_1, \ldots, z_r \in N$, что $K_v[xz_i] \simeq K_v[xz_{iv}]$ для всех $v \in T$ и всех $i = 1, \ldots, r$. Тогда $\mathrm{Nrd}_{D_T/K_T}(\bar{x}_i) = \mathrm{Nrd}_{D_T/K_T}(x_i)$ для подходящих $x_i \in \prod_{v \in T} K_v[xz_i]^*$. Далее, выберем такой элемент $z_{r+1} \in N$, что $\mathrm{Nrd}_{D_v/K_v}(K_v[xz_{r+1}]^*) = K_v^*$ для всех $v \in T_0 \setminus T$ (возможность такого выбора вытекает из лемм 1, 3 и 4). Из наших построений вытекает существование таких $t_i \in Z_i = \prod_{v \in T_0} K_v[xz_i]^*$ $(i = 1, \ldots, r+1)$, что $a = \mathrm{Nrd}_{D_{T_0}/K_{T_0}}(t_1 \ldots t_{r+1})$. Применяя слабую аппроксимационную теорему к полям $K(xz_i)$, найдем элементы $s_i \in K(xz_i)^* \cap t_i Z_i^m$. Имеем

$$a\,\mathrm{Nrd}_{D/K}(s_1 \ldots s_{r+1})^{-1} \in \mathrm{Nrd}_{D/K}(D^*) \cap \prod_{v \in T_0} K_v^{*m},$$

и, значит, согласно предложению 1, $a\,\mathrm{Nrd}_{D/K}(s_1 \ldots s_{r+1})^{-1} \in \mathrm{Nrd}_{D/K}(\Omega(x))$. Но тогда и $a \in \mathrm{Nrd}_{D/K}(\Omega(x))$, что и требовалось.

Опишем теперь общую схему доказательства предложения 1. Пусть $a \in \mathrm{Nrd}_{D/K}(D^*) \cap \prod_{v \in T_0} K_v^{*m}$. Достаточно найти такие $z_1, z_2 \in N$, что $M_i = K(xz_i)$ — максимальные поля в D и $a \in N_{M_1/K}(M_1^*)\,N_{M_2/K}(M_2^*)$. Доказательство последнего включения будет получено нами с помощью мультинорменного принципа (см. § 6.3), примененного к нормальным замыканиям P_i полей M_i в фиксированном алгебраическом замыкании (тогда $L_i = P_i$ в обозначениях предложения 6.11). Чтобы построить поля $M_i = K(xz_i)$ таким образом, чтобы для P_i выполнялись условия предложения 6.11, уже недостаточно леммы 4, а нужен следующий ее усиленный вариант.

Предложение 2. *Пусть заданы элемент $x \in D^*$, конечное расширение F поля K, конечное подмножество $S \subset V^K$ и такой*

элемент $\bar{z}=(z_v)\in N_S$, *что* $K_v[xz_v]$ — *максимальная полупростая коммутативная подалгебра в* D_v *для всех* $v\in S$. *Тогда существует такой элемент* $z\in N$, *что для поля* $M=K(xz)$ *и его нормального замыкания* P (*в фиксированном алгебраическом замыкании*) *выполняются следующие утверждения*: 1) $M\otimes_K K_v\simeq K[xz_v]$ *для всех* $v\in S$; 2) $P\cap F=K$; 3) P/K *удовлетворяет норменному принципу Хассе.*

Доказательство получается редукцией к лемме 4. А именно, мы установим существование такого конечного подмножества $S_1\subset V_f^K\setminus((V_f^K\cap S)\cup T_0)$ и для каждого $v\in S_1$ такой максимальной полупростой коммутативной подалгебры $H_v\subset D_v$, что $H_v=K_v[xz_v]$ для подходящего $z_v\in G_{K_v}$, и если $M\otimes_K K_v\simeq H_v$ для $v\in S_1$, то выполняются условия 2), 3). (Неформально говоря, мы покажем, что можно обеспечить выполнение условий 2), 3), задав конечное число локальных условий, которые «независимы» от условий, указанных в 1).) Тогда существование элемента $z\in N$ с требуемыми свойствами непосредственно вытекает из леммы 4, для применения которой следует заметить, что элемент $\bar{z}=(z_v)_{v\in S\cup S_1}$ лежит в $N_{S\cup S_1}$ в силу леммы 1.

Наиболее просто разобраться с условием 2).

Лемма 5. *Для любого конечного подмножества* $S_0\subset V^K$ *и любого конечного расширения* F/K *существует такое конечное подмножество* $S(F)\subset V_f^K\setminus(V_f^K\cap S_0)$, *что если* $P\supset K$ *и* $P_w=K_v$ *для всех* $v\in S(F)$ *и всех* $w|v$, *то* $P\cap F=K$.

Действительно, можно без ограничения общности предполагать, что F/K — расширение Галуа. Рассмотрим некоторую систему образующих $\sigma_1,\ldots,\sigma_r$ группы Галуа $\mathrm{Gal}(F/K)$. По теореме плотности Чеботарева для каждого $i=1,2,\ldots,r$ найдется такое нормирование $v_i\in V_f^K\setminus(V_f^K\cap S_0)$ и его продолжение $\bar{v}_i$ на F, что автоморфизм Фробениуса $\mathrm{Fr}(F_{\bar{v}_i}/K_{v_i})$ равен σ_i. Положим $S(F)=\{v_1,\ldots,v_r\}$. Если теперь $P\supset K$ и $E=P\cap F\neq K$, то найдется автоморфизм σ_i, нетривиально действующий на E. Обозначим через w нормирование поля P, продолжающее ограничение $\bar{v}_i$ на E. Тогда $w|v_i$ и $P_w\neq K_v$, ибо автоморфизм $\sigma_i\in\mathrm{Gal}(F_{\bar{v}_i}/K_{v_i})$ не является тождественным на подполе $E_{\bar{v}_i}$, и, следовательно, $E_{\bar{v}_i}\neq K_{v_i}$. Полученное противоречие и доказывает лемму.

Выберем конструируемое в лемме 5 подмножество $S(F)$ вне множества $S_0=T_0\cup S$. Тогда, с одной стороны, для любого $v\in S(F)$ существует $z_v\in G_{K_v}$ со свойством $K_v[xz_v]\simeq K_v^n$ (утверждение 1) леммы 3), с другой — если $M\otimes_K K_v\simeq K_v^n$ для всех $v\in S(F)$, то для нормального замыкания P поля M имеем $P_w=K_v$ при $v\in S(F)$ и $w|v$, следовательно, $P\cap F=K$, т. е. выполняется условие 2).

Осталось разобраться с условием 3). В силу теоремы 6.11 справедливость принципа Хассе для расширения Галуа P/K с группой Галуа $\mathcal{G}$ равносильна инъективности канонического отображения

$$H^3(\mathcal{G}, Z) \to \prod_v H^3(\mathcal{G}_v, Z),$$

где $\mathcal{G}_v$ — группа разложения некоторого продолжения нормирования v. Так как в нашей ситуации P является нормальным замыканием расширения степени n, то группа $\mathcal{G}$ изоморфна подгруппе симметрической группы S_n, и, следовательно, из леммы 1.2 вытекает, что P/K при $n \leqslant 3$ всегда удовлетворяет принципу Хассе. Поэтому ниже будем предполагать, что $n \geqslant 4$.

Выберем произвольные два нормирования $v_1, v_2 \in V_f^K \setminus (S \cup T_0 \cup S(F))$ и введем в рассмотрение максимальные полупростые коммутативные подалгебры $H_{v_i} \subset D_{v_i} \simeq M_n(K_{v_i})$ следующего вида:

$$\begin{aligned} H_{v_1} &= E \oplus K_{v_1}, \\ H_{v_2} &= R_1 \oplus R_2 \oplus K_{v_2}^{(n-4)}, \end{aligned} \tag{1}$$

где E — неразветвленное расширение поля K_{v_1} степени $n-1$, R_1, R_2 — соответственно неразветвленное и вполне разветвленное квадратичные расширения поля K_{v_2}. Очевидно, для $i = 1, 2$ имеем $\mathrm{Nrd}_{D_{v_i}/K_{v_i}}(H_{v_i}^*) = K_{vi}^*$, поэтому из леммы 3 вытекает существование таких $z_i \in G_{K_{vi}}$, что $H_{v_i} = K_{v_i}[xz_i]$. Покажем, что если M — расширение K степени n и $M \otimes_K K_{v_i} \simeq H_{v_i}$ для $i = 1, 2$, то для P/K выполняется принцип Хассе. Вычислим вначале группу Галуа $\mathcal{G} = \mathrm{Gal}(P/K)$. Пусть f — неприводимый полином степени n, задающий расширение M/K. Действие $\mathcal{G}$ на корнях f задает инъективный гомоморфизм θ: $\mathcal{G} \to S_n$ в симметрическую группу, причем ввиду неприводимости f образ $\theta(\mathcal{G})$ является транзитивной подгруппой. Из (1) вытекает, что для $w_1 | v_1$ имеем $P_{w_1} = E$, так что группа разложения $\mathcal{G}(w_1)$ является циклической группой порядка $n-1$, причем любая ее образующая переходит при θ в цикл длины $n-1$. Аналогично, для $w_2 | v_2$ имеем $P_{w_2} = R_1 R_2$, следовательно, $\mathcal{G}(w_2)$ является прямым произведением двух циклических групп второго порядка, образующие которых переходят при θ в две коммутирующие транспозиции.

Таким образом, $\theta(\mathcal{G})$ является транзитивной подгруппой S_n, содержащей цикл длины $n-1$ и транспозицию, так что $\theta(\mathcal{G}) = S_n$ (см. Ван дер Варден [1], с. 238). Тогда из леммы 1.2 и описания группы $\mathcal{G}(w_2)$ вытекает инъективность отображения $H^3(\mathcal{G}, Z) \to H^3(\mathcal{G}(w_2), Z)$ и, следовательно, справедливость принципа Хассе для расширения P/K. Предложение 2 полностью доказано.

Завершим доказательство предложения 1. Пусть $a \in \mathrm{Nrd}_{D/K}(D^*) \cap \prod_{v \in T_0} K_v^{*m}$; покажем, что тогда $a \in \mathrm{Nrd}_{D/K}(K(xz_1)^* \times K(xz_2)^*)$ для подходящих $z_i \in N$ таких, что $M_i = K(xz_i)$ — максимальные подполя в D. Выберем элемент $z_1 \in N$ таким образом, чтобы выполнялись следующие условия:

$1)_1$ $K_v[xz_1] \simeq K_v^n$ для $v \in V(a) \setminus (V(a) \cap T_0)$ (напомним, что $V(a) = \{v \in V_f^K \mid v(a) \neq 0\}$;

$2)_1$ для нормального замыкания P_1 поля $M_1 = K(xz_1)$ выполняется принцип Хассе;

$3)_1$ $a \in N_{P_{1w}/K_v}(P_{1w}^*)$ для $w \mid v \in V_\infty^K$.

Существование такого z_1 вытекает из лемм 1, 3 и предложения 2. Более подробно, из лемм 1 и 3 вытекает существование такого $z = (z_v) \in N_S$, где $S = (V(a) \setminus (V(a) \cap T_0)) \cup (V_\infty^K \setminus T_\infty)$, $T_\infty = \{v \in V_\infty^K \mid D_v \not\simeq M_n(K_v)\}$, что $K_v[xz_v] \simeq K_v^n$ для всех $v \in S$. Применяя тогда предложение 2, мы найдем такой элемент $z_1 \in N$, что выполняются условия 1), 2) и, сверх того, $K_v[xz_1] \simeq K_v^n$ для $v \in V_\infty^K \setminus T_\infty$. Используя последнее обстоятельство, проверим выполнимость условия 3). Для $v \in V_{00}^K \setminus T_{00}$ имеем $P_{1w} = K_v$, и 3), очевидно, выполняется. Если же $v \in T_{00}$, то поскольку $a \in \mathrm{Nrd}_{D_v/K_v}(D_v^*)$, имеем $a > 0$ в K_v, и опять $a \in N_{P_{1w}/K_v}(P_{1w}^*)$, ибо здесь $K_v = \mathbb{R}$, $P_{1w} = \mathbb{C}$.

Далее, выбор $z_2 \in N$ осуществим, исходя из условий:

$1)_2$ $K_v[xz_2] \simeq K_v^n$ для всех $v \in V_f^K \setminus T_0$ таких, что расширение P_{1w}/K_v разветвлено;

$2)_2$ для нормального замыкания P_2 поля $M_2 = K(xz_2)$ имеем $P_1 \cap P_2 = K$.

Возможность такого выбора элемента z_2 обосновывается аналогично. Покажем, что $a \in N_{M_1/K}(M_1^*) N_{M_2/K}(M_2^*)$. На самом деле в нашей ситуации выполняется более сильное утверждение: $a \in N_{P_1/K}(P_1^*) N_{P_2/K}(P_2^*)$, которое мы и будем доказывать. В силу предложения 6.11 и выполнимости условий $2)_1$ и $2)_2$ достаточно показать, что $a \in N_{P_1/K}(J_{P_1}) N_{P_2/K}(J_{P_2})$. (Отметим, что у нас $L_i = P_i$ в обозначениях предложения 6.11.) Если $v \in V_f^K \setminus V(a)$ и расширение P_{1w}/K_v неразветвлено, то a является нормой w-адической единицы из P_{1w}. Поэтому с учетом $3)_1$ остается проверить условие

$$a \in N_{P_{1w}/K_v}(P_{1w}) N_{P_{2w}/K_v}(P_{2w}) \tag{2}$$

для таких $w \mid v \in V_f^K$, что либо $v \in V(a)$, либо расширение P_{1w}/K_v разветвлено. Если при этом $v \in T_0$, то по условию $a \in K_v^{*m}$ и (2), очевидно, выполняется, ибо степень $[P_{1w} : K_v]$

делит $m=n!$. Если же $v \notin T_0$, то по построению соответственно либо $P_{1w}=K_v$, либо $P_{2w}=K_v$, и (2) опять выполняется. Доказательство предложения 1 завершено.

Сделаем теперь одно замечание общего характера. Если $N \subset G_K$ — нецентральная нормальная подгруппа, то в силу теоремы 8 индекс $d=[G_K:N]$ конечен. В этом случае подгруппа $N_0 \subset G_K$, порожденная множеством $\{x^d \mid x \in G_K\}$, содержится в N и является нормальной подгруппой в D^*. При этом, как следует, например, из леммы 2 справедливость гипотезы 2 для N_0 влечет ее справедливость для N. Поэтому в дальнейшем мы будем рассматривать лишь те нормальные подгруппы группы G_K, которые являются нормальными подгруппами в D^*.

Итак, пусть $N \subset G_K$ — нецентральная нормальная подгруппа в D^*. Для $x \in D^*$ положим $Z(x)=\{u \in D^* \mid uxu^{-1}x^{-1} \in N\}$.

Лемма 6. $\Omega(x) \subset Z(x)$. *Следовательно, для любых* $x, y \in D^*$ *и любых* $a \in \Omega(x)$, $b \in \Omega(y)$ *имеем*

$$[x, y] \equiv [x, ya] \equiv [xb, y],$$

где $[x, y]=xyx^{-1}y^{-1}$, *а знак* $\equiv$ *означает сравнимость по модулю* N.

Действительно, достаточно показать, что $K(xz)^* \subset Z(x)$ для любого $z \in N$. Пусть $u \in K(xz)^*$. Тогда поскольку N является нормальной подгруппой в D^*, имеем $[u, x] \equiv [u, xz]=1$, что и требовалось. Далее, так как $Z(x)=Z(x^{-1})$, то

$$[x, ya]=xyax^{-1}a^{-1}y^{-1} \equiv xyx^{-1}y^{-1}=[x, y].$$

Аналогично, $[xb, y]=xbyb^{-1}x^{-1}y^{-1} \equiv [x, y]$, и лемма 6 доказана.

Введем теперь некоторые дополнительные обозначения. Положим $\widetilde{N}_T=N_T \prod_{v \in T} K_v^*$. Если применить к морфизму-произведению ψ: $\boldsymbol{G}_m \times G \to \boldsymbol{GL}_1(D)$ следствие 1 из предложения 3.3, то мы получим, что отображение $K_v^* \times G_{K_v} \to D_v^*$ является открытым для любого $v \in V^K$. Поэтому, учитывая открытость $N_T \subset G_T$ (см. доказательство леммы 1), мы видим, что $\widetilde{N}_T$ является открытой нормальной подгруппой в $D_T^*=\prod_{v \in T} D_v^*$. Отсюда следует, что подгруппы $\widetilde{N}=D^* \cap \widetilde{N}_T$ и $\overline{N}=G_K \cap N_T$ являются открытыми в T-адической топологии подгруппами групп D^* и G_K соответственно и нормализуются группой D^*.

Предложение 3. *Пусть* $N \subset G_K$ — *нецентральный нормальный делитель в* D^*, $x \in \widetilde{N}$. *Тогда* $Z(x)\overline{N}=D^*$.

Доказательство. Покажем вначале, что $G_K \subset Z(x)\overline{N}$. Пусть $P \subset D$ — произвольное максимальное подполе такое, что все расширения P_v/K_v для $v \in T$ неразветвлены, и $S=\mathbf{R}_{P/K}(\boldsymbol{G}_m)$ — соответствующий максимальный тор группы $H=\boldsymbol{GL}_1(D)$. Обозначим через W множество регулярных элементов в S. Тогда

с помощью предложения 3.3 легко проверяется, что для любого $v \in V^K$ отображение $\varphi_v\colon D_v^* \times W_{K_v} \to D_v^*$, $\varphi_v(g, x) = gxg^{-1}$, является открытым, так что отображение $\varphi_T = \prod \varphi_v\colon D_T^* \times W_T \to D_T^*$ также открыто. Поэтому если мы рассмотрим убывающую последовательность $U_1 \supset U_2 \supset \ldots$ открытых подгрупп группы D_T^*, сходящуюся к единице, то для любого $r \geqslant 1$ множество $B_r = \varphi_T(U_r, W_T)$ открыто в D_T^*. Так как множество NK^*, очевидно, плотно в $\tilde{N}_T$, то для любого $r \geqslant 1$ множество $x^{-1}B_r$ пересекается с NK^*. Отсюда следует существование таких элементов $y_r \in N$, $u_r \in U_r$, что $u_r(S_r)_T u_r^{-1} = S_T$, где $S_r = Z_H(xy_r)$ — централизатор регулярного элемента xy_r. Ясно, что S_r имеет вид $\mathbf{R}_{P_r/K}(\boldsymbol{G}_m)$, где $P_r = K(xy_r)$, причем все расширения P_{rv}/K_v для $v \in T$ являются неразветвленными. Поэтому из предложения 7.8 вытекает, что для соответствующих норменных торов $S_r^{(1)} = S_r \cap G$ имеет место слабая аппроксимация относительно множества T. В частности, для произвольного элемента $z \in S_K^{(1)}$ можно найти элементы $z_r \in (u_r^{-1} z u_r) N_T \cap (S_r^{(1)})_K$. Для достаточно больших r имеем $z^{-1} z_r \in G_K \cap ((z^{-1} u_r^{-1} z u_r) N_T) = G_K \cap N_T = \bar{N}$, ибо $u_r \to 1$, а подгруппа N_T открыта в G_T. С другой стороны, $z_r \in \Omega(x) \subset Z(x)$, откуда $z \in Z(x)\bar{N}$, и, значит, $S_K^{(1)} \subset Z(x)\bar{N}$. Отметим, что в качестве P может быть взято произвольное максимальное подполе в D такое, что все расширения P_v/K_v $(v \in T)$ являются неразветвленными, поэтому остается показать, что соответствующие группы $S_K^{(1)}$ в совокупности порождают G_K. Положим для краткости $P^{(1)} = S_K^{(1)}$ и обозначим через B подгруппу в G_K, порожденную группами $P^{(1)}$ для всех $P \subset D$ с описанными свойствами. Далее, для $v \in T$ обозначим через Δ_v совокупность таких $z \in G_{K_v}$, что $K_v[z]$ — максимальное неразветвленное подполе в D_v. Тогда Δ_v открыто в G_{K_v}, и из теоремы 1.8 легко выводится, что Δ_v порождает G_{K_v}. Отсюда следует, что $\Delta = \prod_{v \in T} \Delta_v$ открыто в G_T и порождает G_T.

Лемма 7. *Пусть Γ — плотная подгруппа топологической группы Φ и $U \subset \Phi$ — открытое подмножество. Тогда подгруппа, порожденная $\Gamma \cap U$, совпадает с пересечением $\Gamma \cap W$, где W — подгруппа, (алгебраически) порожденная U.*

Доказательство — простое упражнение для читателя.

Поскольку G_K плотно в G_T, то из леммы 7 получаем, что подгруппа в G_K, порожденная $G_K \cap \Delta$, совпадает с G_K. С другой стороны, по построению для любого $z \in G_K \cap \Delta$ алгебра $K_v[z]$ является неразветвленным расширением поля K_v степени n для всех $v \in T$, т. е. расширение $P = K[z]$ удовлетворяет описан-

ным свойствам, и, следовательно, $P^{(1)} \subset B$. Тем самым $G_K \cap \Delta \subset \subset B$ и $G_K = B \subset Z(x)\bar{N}$.

Для завершения доказательства предложения 3 остается показать, что $\mathrm{Nrd}_{D/K}(Z(x)) = \mathrm{Nrd}_{D/K}(D^*)$. С учетом включения $\Omega(x) \subset Z(x)$ в силу теоремы 10 достаточно установить, что $\Omega_T(x) = D_T^*$ для $x \in \tilde{N}$. Но из определения $\tilde{N}$ вытекает, что в рассматриваемой ситуации для любого набора максимальных полупростых коммутативных подалгебр $H_v \subset D_v$, $v \in T$, найдется такой элемент $\bar{z} = (z_v) \in N_T$, что $K[xz_v] \simeq H_v$, откуда и следует требуемое. Доказательство предложения 3 завершено.

Следствие. *Если факторгруппа $\tilde{N}/N$ абелева, то факторгруппа $\tilde{N}/N$ лежит в центре факторгруппы D^*/N.*

Действительно, пусть $x \in D^*$, $y \in \tilde{N}$. Так как согласно предложению 3 $D^* = \bar{N}Z(y)$, то $[x, y] \equiv [s, y]$ для некоторого $s \in \bar{N}$. Симметричным образом, используя разложение $D^* = = \bar{N}Z(s)$ $(s \in \bar{N}!)$, получим, что $[x, y] \equiv [s, t]$ для подходящих $s, t \in \bar{N}$. Но поскольку группа $\tilde{N}/N$ абелева, то $[s, t] \equiv 1$, и, значит, $[x, y] \equiv 1$, т. е. x централизует y.

После проделанной подготовительной работы переходим непосредственно к доказательству теорем 2—4.

Доказательство теоремы 4. Ключевую роль здесь играет следующая

Теорема 11 (конгруэнц-теорема). *Пусть $x \in U = \{x \in \in D^* | \mathrm{Nrd}_{D/K}(x) \in U_v \forall v \in T\}$, $y \in D^*$. Предположим, что $x \in \in U_v(1 + \mathfrak{P}_v)$ для всех $v \in T \cap V(\mathrm{Nrd}_{D/K}(y))$, где $\mathfrak{P}_v$ — идеал нормирования в D_v (см. § 1.4). Тогда коммутатор $[x, y] = = xyx^{-1}y^{-1} \in [G_K, G_K]$. В частности, $[U, U] = [G_K, G_K]$.*

Мы вначале проведем доказательство теоремы 4, считая теорему 11 известной. Оно основывается на следующей естественной идее: так как $G_K = [D^*, D^*]$ (теорема 2.14), то, используя представление элемента $z \in G_K \cap \prod_{v \in T} [G_{K_v}, G_{K_v}]$ в виде произведения коммутаторов, можно попытаться заменить z на такой элемент из zN, где $N = [G_K, G_K]$, который бы выражался через коммутаторы описанного в теореме 11 вида; тогда $z \in [G_K, G_K]$. На протяжении всего доказательства теоремы 4 буква N будет обозначать коммутант $[G_K, G_K]$, а запись $z_1 \equiv z_2$ — тот факт, что $z_1^{-1}z_2 \in [G_K, G_K]$. Отметим также, что здесь для любого конечного подмножества $S \subset V^K$ имеем $N_S = \prod_{v \in S} N_v$, где $N_v = = [G_{K_v}, G_{K_v}]$, причем $N_v = G_{K_v}$ для $v \notin T$.

Лемма 8. *Любой элемент из G_K является произведением коммутаторов вида $[x, y]$, где $x \in U$, $y \in D^*$.*

Доказательство. Поскольку $G_K = [D^*, D^*]$, то достаточно показать, что произвольный коммутатор $[x, y]$ $(x, y \in D^*)$ представляется в виде произведения коммутаторов указанного вида.

Пусть F — такое максимальное подполе в D, что для любого $v \in T$ расширение F_v/K_v является вполне разветвленным. Тогда $v\left(\mathrm{Nrd}_{D_v/K_v}(F_v^*)\right) = \mathbb{Z}$, и поэтому, используя слабую аппроксимационную теорему для поля F, можно найти такие элементы $s, t \in F$, что

$$\begin{aligned} v(\mathrm{Nrd}_{D/K}(s)) &= v(\mathrm{Nrd}_{D/K}(x)), \\ v(\mathrm{Nrd}_{D/K}(t)) &= v(\mathrm{Nrd}_{D/K}(y)) \end{aligned} \tag{3}$$

для всех $v \in T$. В силу (3) $x_0 = xs^{-1}$, $y_0 = yt^{-1} \in U$. Но тогда из соотношения

$$[x, y] = [x_0, t]\,[tx_0t^{-1}, sy_0s^{-1}]\,[y_0^{-1}, y_0sy_0^{-1}]$$

непосредственно получается доказательство леммы.

Будем по-прежнему обозначать через F такое максимальное подполе в D, что расширение F_v/K_v вполне разветвлено для всех $v \in T$. Выберем, далее, элемент $t \in F^*$ со свойством $v(\mathrm{Nrd}_{D/K}(t)) = 1$ для всех $v \in T$. Тогда для любого $v \in T$ элемент t является униформизующим элементом тела D_v.

Предложение 4. *Для любого $z \in G_K$ найдется такой элемент $x \in U$, что $z \equiv [x, t]$.*

Доказательство. Для $x, y \in U$ и любого $s \in D^*$ имеем

$$[xy, s] = xysy^{-1}x^{-1}s^{-1} = x[y, s](sx^{-1}s^{-1}) \equiv [x, s][y, s], \tag{4}$$

ибо элементы $[y, s]$, $sx^{-1}s^{-1}$ лежат в U и, следовательно, перестановочны по модулю N в силу конгруэнц-теоремы. Поэтому, учитывая лемму 8, достаточно показать, что любой коммутатор $[a, b]$, где $a \in U$, $b \in D^*$, эквивалентен коммутатору $[x, t]$ для подходящего $x \in U$.

Пусть $T = \{v_1, \ldots, v_d\}$. Из слабой аппроксимационной теоремы для поля $K(a)$ вытекает существование таких элементов $a_1, \ldots, a_d \in U$, что $a = a_1 \ldots a_d$ и

$$\begin{aligned} a_i &\equiv a \left(\mathrm{mod}\ \mathfrak{P}_{v_i}\right), \\ a_i &\equiv 1 \left(\mathrm{mod}\ \mathfrak{P}_{v_j}\right), \quad j \neq i, \end{aligned}$$

для всех $i = 1, \ldots, d$. Тогда в силу (4)

$$[a, b] \equiv [a_1, b] \ldots [a_d, b]. \tag{5}$$

Далее, положив $\alpha_i = v_i(\mathrm{Nrd}_{D/K}(b))$, будем иметь

$$[a_i, b] = a_i t^{\alpha_i}\left(t^{-\alpha_i}b\right)a_i^{-1}b^{-1} \equiv [a_i, t^{\alpha_i}], \tag{6}$$

ибо по построению $T \cap V\left(\mathrm{Nrd}_{D/K}\left(t^{-\alpha_i}b\right)\right) \subset T \setminus \{v_i\}$, так что $a_i \equiv 1 \ (\mathrm{mod}\ \mathfrak{P}_v)$ для $v \in T \cap V\left(\mathrm{Nrd}_{D/K}\left(t^{-\alpha_i}b\right)\right)$, и согласно конгруэнц-теореме a_i и $t^{-\alpha_i}b$ перестановочны по модулю N. Из (5)

и (6) вытекает, что для завершения рассуждений остается показать, что любой коммутатор $[a, t^\alpha]$, где $a \in U$, $\alpha \in \mathbb{Z}$, эквивалентен коммутатору вида $[d, t]$ для подходящего $d \in U$.

При $\alpha > 0$ положим $d = \prod_{i=0}^{\alpha-1} (t^i a t^{-i}) = a(ta)^{\alpha-1} t^{-(\alpha-1)} \in U$. Тогда, используя (4), будем иметь

$$[d, t] \equiv \prod_{i=0}^{\alpha-1} [t^i a t^{-i}, t] = \prod_{i=0}^{\alpha-1} (t^i a t a^{-1} t^{-(i+1)}) = [a, t^\alpha].$$

Аналогично, при $\alpha < 0$, полагая $d = \prod_{i=\alpha}^{-1} (t^i a^{-1} t^{-i}) = t^\alpha (a^{-1} t)^{-\alpha} \in U$, получим

$$[d, t] = \prod_{i=\alpha}^{-1} [t^i a^{-1} t^{-i}, t] = \prod_{i=\alpha}^{-1} (t^i a^{-1} t a t^{-(i+1)}) = t^\alpha a^{-1} t^{-\alpha} a \equiv [a, t^\alpha],$$

поскольку элементы a, $t^\alpha a^{-1} t^{-\alpha}$ лежат в U и значит, перестановочны по модулю N. Предложение 5 доказано.

Завершим доказательство теоремы 4. Пусть $z \in G_K \cap \cap \prod_{v \in T} [G_{K_v}, G_{K_v}]$. Используя предложение 4, выберем такой $x \in U$, что $z \equiv [x, t]$. Так как для $v \in T$ имеем $[G_{K_v}, G_{K_v}] = G_{K_v} \cap (1 + \mathfrak{P}_v)$ (теорема 1.9) то из включения $z = [x, t] \in [G_{K_v}, G_{K_v}]$ для любого $v \in T$ получаем сравнение

$$t x t^{-1} \equiv x \pmod{\mathfrak{P}_v}. \tag{7}$$

Но мы знаем (см. § 1.4, п. 1), что в нашей ситуации тело вычетов $d_v = \mathcal{O}_{D_v}/\mathfrak{P}_v$ коммутативно, является расширением Галуа поля вычетов k_v, причем автоморфизм, индуцируемый $\operatorname{Int} t$, порождает всю группу Галуа $\operatorname{Gal}(d_v/k_v)$. Поэтому из (7) вытекает, что вычет $\bar{x}$ элемента x попадает в k_v, т. е. $x \in U_v(1 + \mathfrak{P}_v)$. Так как последнее включение справедливо для всех $v \in T$, то в силу конгруэнц-теоремы $[x, t] \in N$, а тогда и $z \in N$. Теорема 4 доказана.

Доказательство конгруэнц-теоремы начнем со второго утверждения, а именно, покажем, что $[U, U] = [G_K, G_K]$. Учитывая, что $[x, y] \equiv [x, ya] \equiv [xb, y]$ для $a \in \Omega(x)$, $b \in \Omega(y)$ (лемма 6), легко видеть, что этот факт вытекает из следующего утверждения:

Лемма 9. *Если $x \in U$, то* $\operatorname{Nrd}_{D/K}(\Omega(x)) \supset \operatorname{Nrd}_{D/K}(U)$.

Доказательство. В силу теоремы 10 достаточно показать, что $\prod_{v \in T} U_v \subset \operatorname{Nrd}_{D_T/K_T}(\Omega_T(x))$. Поскольку $N_T = \prod_{v \in T} N_v$, то, очевидно, $\Omega_T(x) = \prod_{v \in T} \Omega_v(x)$, где $\Omega_v(x)$ — подгруппа в D_v^*, порожденная мультипликативными группами максимальных подполей вида

$K_v(xz)$, $z \in N_v$. Достаточно установить, что среди этих подполей содержится максимальное неразветвленное подполе $L \subset D_v$, ибо в силу предложения 1.2 $U_v \subset N_{L/K_v}(L^*) = \mathrm{Nrd}_{D_v/K_v}(L^*)$. Так как по условию $\mathrm{Nrd}_{D/K}(x) \in U_v$, то $x \in L^* G_{K_v}$. Далее, из теоремы 1.8 вытекает, что $G_{K_v} = L^{(1)} N_v$, где $L^{(1)} = \{x \in L^* \mid N_{L/K_v}(x) = 1\}$, поэтому $x \in L^* N_v$. Но тогда $L = K[xz]$ для подходящего $z \in N_v$ (см. доказательство леммы 3). Лемма 9 доказана.

Чтобы разобраться с первым утверждением конгруэнц-теоремы, покажем, что при выполнении указанных условий $b = \mathrm{Nrd}_{D/K}(y) \in \mathrm{Nrd}_{D/K}(\Omega(x))$. В силу теоремы 10 достаточно убедиться, что $b \in \mathrm{Nrd}_{D_T/K_T}(\Omega_T(x))$, где в обозначениях леммы 9 $\Omega_T(x) = \prod_{v \in T} \Omega_v(x)$. Мы уже показали, что $b \in \Omega_v(x)$, если $v(b) = 0$. В противном случае по условию $x = st$, где $s \in U_v$, $t \in 1 + \mathfrak{P}_v$, так что $a = \mathrm{Nrd}_{D/K}(x) = s^n r$, где $r = \mathrm{Nrd}_{D_v/K_v}(t) \in 1 + \mathfrak{p}_v$. Покажем, что тогда $b \in \mathrm{Nrd}_{D_v/K_v}(K_v[xz]^*)$ для подходящего $z \in N_v$. Для этого вначале построим расширение L поля K_v степени n со свойством: a, $b \in N_{L/K_v}(L^*)$. Пусть p_v — отвечающее v простое число и $n = p_v^a m$, где m — взаимно просто с p_v.

Лемма 10. *Пусть $b \in K_v^*$, m — произвольное целое $\geqslant 1$. Тогда существует такое расширение F/K_v степени m, что $b \in N_{F/K_v}(F^*)$.*

Доказательство — упражнение для читателя. (Указание. Редуцировать задачу к случаю простого m. Далее разобрать отдельно случай $m = 2$ и случай нечетного m, причем в последнем уместно воспользоваться тем фактом, что если $b \notin K_v^{*m}$, то многочлен $X^m - b$ неприводим над K_v, см. Ленг [3].)

Пусть F — такое расширение поля K_v степени m, что $b = N_{F/K_v}(c)$, $c \in F^*$. Поскольку $a = s^n \cdot r$, где $r \in 1 + \mathfrak{p}_v$, то из взаимной простоты m и p_v вытекает, что $a = d^m$, где $d \in K_v^*$. Тогда, очевидно, в качестве L можно взять расширение поля F степени $l = p_v^a$ со свойством: c, $d \in N_{L/F}(L^*)$, в существовании которого мы сейчас убедимся. Известно (см. § 1.1, п. 2), что $F^* \simeq \mathbb{Z} \times E \times \mathbb{Z}_{p_v}^{\delta}$, где E — группа корней из единицы в F, $\delta = [F : \mathbb{Q}_{p_v}]$. Отсюда следует, что $F^*/F^{*l} \simeq (\mathbb{Z}/l\mathbb{Z})^{\delta+1} \times E/E^l$. Если $\delta > 1$, то подгруппа, порожденная образами c, d в F^*/F^{*l}, имеет индекс, делящийся на l, так что существует открытая подгруппа $W \subset F^*$ индекса l, содержащая c и d, и в качестве L можно взять абелево расширение поля F степени l с нормменной подгруппой W, конструируемое в локальной теории полей классов. Если $\delta = 1$ (т. е. $F = \mathbb{Q}_{p_v}$) и $p_v \neq 2$, то можно положить

$L = F(\sqrt[l]{p_v})$. Действительно, как показывает нижеследующее упражнение, L не содержит абелевых расширений поля F, и поэтому согласно локальной теории полей классов $N_{L/F}(L^*) = F^*$.

Упражнение. Если $p \neq 2$, то $\mathbb{Q}_p(\sqrt[l]{p})$ $(l = p^\alpha)$ не содержит абелевых (и даже нормальных) расширений поля $\mathbb{Q}_p$. (Указание. Провести индукцию по α. Случай $\alpha = 0$ очевиден. Пусть $\alpha \geqslant 1$ и $L \subset \mathbb{Q}_p(\sqrt[l]{p})$ — расширение Галуа поля $\mathbb{Q}_p$. Тогда $L \subset \mathbb{Q}_p(\sqrt[l]{p}) \cap \mathbb{Q}_p(\xi\sqrt[l]{p}) = \mathbb{Q}_p(\sqrt[p^{\alpha-1}]{p})$, где ξ — примитивный корень степени p из единицы, и можно воспользоваться предположением индукции.)

Нам осталось рассмотреть случай $p_v = 2$, т. е. $F = \mathbb{Q}_2$. Здесь $F^*/F^{*2} \simeq (\mathbb{Z}/2\mathbb{Z})^3$, поэтому, рассуждая как и выше, найдем квадратичное расширение P/F такое, что $c = N_{P/F}(c')$, $d = N_{P/F}(d')$ для некоторых $c', d' \in P$. Но согласно уже доказанному существует расширение M/P степени $p_v^{\alpha-1}$, для которого $c', d' \in N_{M/P}(M^*)$, и можно положить $L = M$. Итак, существование расширения L/K_v степени n со свойством $a, b \in N_{L/K_v}(L^*)$ доказано. Поле L вкладывается в D_v в качестве максимального подполя, и достаточно найти такой элемент $z \in N_v$, что $L = K_v(xz)$. Для этого вернемся к представлению $x = st$, где $s \in U_v$, $t \in 1 + \mathfrak{P}_v$. Поскольку $a = \mathrm{Nrd}_{D/K}(x) \in N_{L/K_v}(L^*)$, то $\mathrm{Nrd}_{D_v/K_v}(t) = s^{-n}a \in N_{L/K_v}(L^*) \cap (1 + \mathfrak{p}_v)$. Поэтому согласно предложению 1.3 $\mathrm{Nrd}_{D_v/K_v}(t) = N_{L/K_v}(g)$ для некоторого $g \in 1 + \mathfrak{P}_L$, где $\mathfrak{P}_L$ — идеал нормирования в поле L. Тогда $z = t^{-1}g \in G_{K_v} \cap (1 + \mathfrak{P}_v) = N_v$ и $xz = sg \in L$. Остается «подправить» элемент xz на элемент из $L^* \cap N_v$ таким образом, чтобы он порождал все поле L (см. доказательство леммы 3). Доказательство конгруэнц-теоремы, а вместе с тем и теоремы 4 завершено.

Замечание. Если $T = \varnothing$, то в силу теоремы 4 группа G_K совпадает со своим коммутантом, и можно ставить вопрос о вычислении коммутаторной длины G_K, т. е. нахождении такого минимального числа $l = l(G_K)$, что любой элемент из G_K является произведением не более l коммутаторов. При доказательстве теоремы 4 для случая D — тело кватернионов, $T = \varnothing$ (см. Платонов, Рапинчук [1]) было показано, что здесь $l(G_K) \leqslant 3$. Никаких других оценок для коммутаторной длины группы G_K (и даже доказательства ее конечности в общей ситуации) пока нет.

Переходим к доказательству теоремы 3. В силу леммы 2 достаточно показать следующее: если нормальный делитель $F \subset G_K$ открыт в T-адической топологии, то его коммутант $[F, F]$ также открыт. Рассмотрим вначале случай, когда D является телом кватернионов. Обозначим через τ каноническую

инволюцию (сопряжение) в D. Ограничение τ на любое максимальное подполе в D индуцирует нетривиальный автоморфизм, поэтому по теореме Сколема — Нётер для любого $x \in D^*$ найдется такой $y \in D^*$, что $\tau(x) = yxy^{-1}$. С другой стороны, имеем $\mathrm{Nrd}_{D/K}(x) = x\tau(x)$; в частности, элементы из $G_K = SL_1(D)$ характеризуются условием $\tau(x) = x^{-1}$. Таким образом, для любого $x \in G_K$ найдется $y \in D^*$ со свойством $x^{-1} = yxy^{-1}$.

Пусть теперь $F \subset G_K$ — произвольная подгруппа, открытая в T-адической топологии. Тогда для подходящих целых $\alpha_v > 0$ $(v \in T)$ имеем $F_0 = G_K \cap \prod_{v \in T} \left(1 + \mathfrak{P}_v^{\alpha_v}\right) \subset F$, где $\mathfrak{P}_v$ — идеал нормирования в D_v. Ясно, что F_0 является нормальной подгруппой в D^*, и из открытости коммутанта $[F_0, F_0]$, очевидно, вытекает открытость $[F, F]$. Поэтому в дальнейшем можно считать подгруппу F нормальной в D^*.

Положим $N = [F, F]$ и сохраним обозначения $\bar{N}$ и $\tilde{N}$, введенные выше (см. с. 567). Так как $\bar{N} \subset F$, то факторгруппа $\bar{N}/N$ абелева, поэтому в силу следствия из предложения 3 факторгруппа $\bar{N}/N$ лежит в центре D^*/N. Обозначим через Z множество элементов вида $x\tau(x)^{-1}$, $x \in \tilde{N}$, и пусть $z \in Z$. Мы отмечали, что $\tau(x) = yxy^{-1}$ для подходящего $y \in D^*$, так что из центральности $\tilde{N}/N$ в D/N вытекает включение $Z \subset N$. Покажем, что, с другой стороны, $\bar{N} \subset ZN$. Для этого достаточно установить открытость Z в G_K в T-адической топологии, что мы сейчас и сделаем. По построению группа $\tilde{N}$ является открытой в D^* в T-адической топологии, так что $D^* \cap \prod_{v \in T} \left(1 + \mathfrak{P}_v^{\beta_v}\right) \subset \tilde{N}$ для подходящих целых $\beta_v > 0$, $v \in T$. Тогда из тождества $x = \left(\frac{1+x}{2}\right)\tau\left(\frac{1+x}{2}\right)^{-1}$, справедливого для любого элемента $x \in G_K$, непосредственно вытекает включение $G_K \cap \prod_{v \in T}\left(1 + 2\mathfrak{P}_v^{\beta_v}\right) \subset Z$, что и требовалось.

Анализ приведенного рассуждения показывает, что оно дословно переносится в общую ситуацию, если известно, что для любой нормальной подгруппы $U \subset D^*$, открытой в T-адической топологии, взаимный коммутант $[U, D^*]$ также открыт (действительно, тогда $\bar{N} \subset [\bar{N}, D^*]N = N$). Получить информацию о $[U, D^*]$ можно из начального отрезка

$$H^1(D^*/U) \to H^1(D^*) \to H^1(U)^{D^*} \to H^2(D^*/U) \to H^2(D^*) \qquad (8)$$

спектральной последовательности Хохшильда — Серра, соответствующей расширению $1 \to U \to D^* \to D^*/U \to 1$, где $H^i(*)$ обозначает группу i-х когомологий с коэффициентами в тривиальном модуле $J = \mathbb{Q}/\mathbb{Z}$, а именно

$$H^1(U)^{D^*} = \mathrm{Hom}\,(U/[U, D^*], J). \qquad (9)$$

Но по условию $U = D^* \cap W$, где W — открытая нормальная подгруппа D_T^* (совпадающая с замыканием U), и можно рассмотреть последовательность Хохшильда — Серра непрерывных когомологий с коэффициентами в тривиальном дискретном модуле J:

$$H^1(D_T^*/W) \to H^1(D_T^*) \to H^1(W)^{D_T^*} \to H^2(D_T^*/W) \xrightarrow{\psi} H^2(D_T^*), \quad (10)$$

отвечающую топологическому расширению $1 \to W \to D_T^* \to \to D_T^*/W \to 1$. Считая когомологии в (8) непрерывными когомологиями дискретных групп, соединим последовательности (8), (10) в коммутативную диаграмму

$$\begin{array}{ccccccccc} H^1(D^*/U) & \to & H^1(D^*) & \xrightarrow{\varphi} & H^1(U)^{D^*} & \longrightarrow & H^2(D^*/U) & \longrightarrow & H^2(D^*) \\ \uparrow\alpha & & \uparrow & & \uparrow\beta & & \uparrow\gamma & & \uparrow\delta \\ H^1(D_T^*/W) & \to & H^1(D_T^*) & \to & H^1(W)^{D_T^*} & \to & H^2(D_T^*/W) & \xrightarrow{\psi} & H^2(D_T^*), \end{array} \quad (11)$$

в которой вертикальные стрелки являются отображениями ограничения. Из слабой аппроксимационной теоремы для D^* вытекает, что $D^*/U \simeq D_T^*/W$, т. е. α и γ являются изоморфизмами. Если известно, что отображение δ (или даже его ограничение на $\operatorname{Im}\psi$) инъективно, то из диаграммы (11) легко получается, что

$$H^1(U)^{D^*} = \operatorname{Im}\beta + \operatorname{Im}\varphi. \quad (12)$$

В смысле отождествления (9) любой элемент из $\operatorname{Im}\beta + \operatorname{Im}\varphi$ на пересечении $[D^*, D^*] \cap [W, D_T^*] = G_K \cap [W, D_T^*]$ индуцирует тривиальный гомоморфизм, поэтому из (12) вытекает равенство $[U, D^*] = G_K \cap [W, D_T^*]$; в частности, подгруппа $[U, D^*]$ открыта.

Таким образом, если бы нам была известна инъективность отображения δ: $H^2(D_T^*) \to H^2(D^*)$ (или даже инъективность ограничения δ на образ в $H^2(D_T^*)$ прямого предела $\varinjlim H^2(D_T^*/W)$ по всем открытым нормальным подгруппам $W \subset D_T^*$), то мы получили бы доказательство теоремы 3, не использующее теоремы 4, и, в частности, другое доказательство самой теоремы 4. Тем самым обнаружена связь теоремы 3 с проблемой вычисления $\operatorname{Ker}\delta$, которую естественно называть *слабой метаплектической проблемой* (терминология связана с соответствующими понятиями, используемыми при исследовании конгруэнц-проблемы, см. § 9.5). На эту связь впервые указал Рапинчук [6] при исследовании (сильной) метаплектической проблемы. К сожалению, непосредственного вычисления $\operatorname{Ker}\delta$, или даже $\operatorname{Ker}\delta|_{\varinjlim H^2(D_T^*/W)}$ пока не получено, однако Рапинчуком [6] была доказана

тривиальность ядра соответствующего отображения для группы G, а именно отображения θ: $H^2(G_T) \to H^2(G_K)$, где, как и выше, рассматриваются непрерывные когомологии с коэффициентами в тривиальном дискретном модуле J, а группа G_K считается наделенной дискретной топологией. В указанной работе тривиальность $\operatorname{Ker}\theta$ выводилась из теоремы 3, доказательство которой было получено Рагунатаном [7] другим способом. Здесь мы будем рассуждать в обратном направлении, а именно, покажем, что теорема 3 может быть получена из утверждения о тривиальности $\operatorname{Ker}\theta$, а затем воспользуемся следующим результатом:

Теорема 12 (слабая метаплектическая гипотеза). *Предположим, что $n > 2$. Тогда отображение θ: $H^2(G_T) \to H^2(G_K)$ инъективно.*

Доказательство теоремы 12, которое мы проведем в § 9.5 в связи с обсуждением конгруэнц-проблемы, использует результаты работы Прасада, Рагунатана [5]. Отметим, что утверждение теоремы 12 остается справедливым при $n = 2$, однако здесь тривиальность $\operatorname{Ker}\theta$, как и в работе Рапинчука [6], нужно выводить из теоремы 3, которая для тела кватернионов уже доказана.

Вывод теоремы 3 для $n > 2$ из теоремы 12 проводится по описанной выше схеме. А именно, пусть $U \subset G_K$ — нормальная подгруппа, открытая в T-адической топологии, W — ее замыкание в группе G_T; тогда $U = G_K \cap W$. Рассмотрим аналогичную (10) коммутативную диаграмму

$$\begin{array}{ccccccccc} H^1(G_K/U) & \to & H^1(G_K) & \to & H^1(U)^{G_K} & \to & H^2(G_K/U) & \to & H^2(G_K) \\ \uparrow\alpha & & \uparrow\beta & & \uparrow\gamma & & \uparrow\delta & & \uparrow\theta \\ H^1(G_T/W) & \to & H^1(G_T) & \to & H^1(W)^{G_T} & \to & H^2(G_T/W) & \to & H^2(G_T), \end{array} \tag{13}$$

вертикальные стрелки в которой являются отображениями ограничения, а строчки — начальными отрезками спектральных последовательностей Хохшильда — Серра, отвечающими расширениям $1 \to U \to G_K \to G_K/U \to 1$ и $1 \to W \to G_T \to G_T/W \to 1$. Слабая аппроксимационная теорема для группы G показывает, что $G_K/U \simeq G_T/W$, так что α и δ являются изоморфизмами. Далее, теорема 4 позволяет утверждать, что естественное отображение $G_K/[G_K, G_K] \to G_T/[G_T, G_T]$ является изоморфизмом, и тогда β — также изоморфизм. Используя эти факты и инъективность θ (теорема 12), из диаграммы (13) легко получить, что γ является изоморфизмом. Но $H^1(U)^{G_K} = \operatorname{Hom}(U/[U, G_K], J)$, $H^1(W)^{G_T} = \operatorname{Hom}(W/[W, G_T], J)$, поэтому доказанное означает, что вложение $U \subset W$ индуцирует изоморфизм $U/[U, G_K] \simeq W/[W, G_T]$, в частности, $[U, G_K] = U \cap [W, G_T]$ открыто в T-адической топологии.

Таким образом, мы показали, что если нормальная подгруппа $U \subset G_K$ открыта в T-адической топологии, то взаимный коммутант $[U, G_K]$ также открыт. Пусть теперь $F \subset G_K$ — произвольная T-адически открытая подгруппа; покажем, что коммутант $[F, F]$ также открыт. Без ограничения общности можно считать подгруппу F нормальной в D^*. Обозначим через U замыкание $[F, F]$ в T-адической топологии группы G_K. Тогда из доказанного выше утверждения вытекает открытость взаимного коммутанта $[U, G_K]$, так что

$$U = [U, G_K][F, F]. \tag{14}$$

С другой стороны, факторгруппа $U/[F, F]$ абелева, ибо $U \subset F$ в силу открытости F, и, значит, лежит в центре группы $D^*/[F, F]$ (следствие из предложения 3). В частности, $[U, G_K] \subset [F, F]$, так что из (14) получаем равенство $U = [F, F]$, что и требовалось.

Завершает настоящий параграф доказательство теоремы 2. Нам понадобится следующее усиление предложения 1:

Предложение 5. *Пусть D — тело кватернионов, $x \in D^*$, Ψ — конечный набор максимальных подполей в D. Тогда для любого конечного подмножества $B \subset \mathrm{Nrd}_{D/K}(D^*) \cap \prod_{v \in T} K_v^{*2}$ и любой нецентральной нормальной подгруппы $N \subset G_K$ найдется такой элемент $n \in N$, что $B \subset \mathrm{Nrd}_{D/K}(L^*K(xn)^*)$ для любого $L \in \Psi$.*

Доказательство. Положим $V_0 = \{v \in V^K \mid B \subset \mathrm{Nrd}_{D_v/K_v}(L_v^*)$ для любого $L \in \Psi\}$. Поскольку для почти всех $v \in V_f^K$ расширения $L_v/K_v (L \in \Psi)$ являются неразветвленными, а элементы из B — v-адическими единицами, то $S = V^K \setminus V_0$ — конечное множество. Кроме того, из условия $B \subset \mathrm{Nrd}_{D/K}(D^*) \cap \prod_{v \in T} K_v^{*2}$, очевидно, вытекает, что S не пересекается с множеством $T \cup T_\infty$. Поскольку в данном случае $T = T_0$, то из лемм 3 и 4 вытекает существование такого $n \in N$, что $K(xn)_v \simeq K_v \oplus K_v$ для всех $v \in S$. Тогда

$$B \subset \mathrm{Nrd}_{D_v/K_v}((L \otimes_K K_v)^* K_v [xn]^*) \quad \text{для всех} \quad v \in V^K.$$

Перейти от локальных норм к глобальным можно либо с помощью предложения 6.11, либо воспользовавшись следующим соображением, приспособленным непосредственно к нашему случаю. Пусть $\alpha \in B$, $L \in \Psi$. Тогда выражение $N_{L/K}(a) - \alpha N_{K(xn)/K}(b)$ является 4-мерной квадратичной формой относительно координат элементов $a \in L$, $b \in K(xn)$, и условие $\alpha \in \mathrm{Nrd}_{D/K}(L^*K(xn)^*)$ эквивалентно тому, что эта форма представляет нуль в K. По теореме Минковского — Хассе достаточно проверить представимость нуля над всеми пополнениями

K_v, где она является следствием условия $\alpha \in \mathrm{Nrd}_{D_v/K_v}((L \otimes_K \otimes_K K_v)^* K_v[xn]^*)$. Предложение доказано.

Как обычно, будем в дальнейшем предполагать, что $N \subset G_K$ является нормальным делителем в D^*. Для $v \in T$ обозначим через Φ_v открытую подгруппу в K_v^* конечного индекса, не содержащую -1, и положим $H = \left(N_T \prod_{v \in T} \Phi_v\right) \cap D^*$. Легко видеть, что H является T-адической открытой подгруппой в D^* конечного индекса, причем $H \cap G_K = N_T \cap G_K = \bar{N}$ в силу условия $-1 \notin \Phi_v$. Рассмотрим естественное действие группы H на факторгруппе $\bar{N}/N$ посредством внутренних автоморфизмов и обозначим через F ядро этого действия.

Лемма 11. *Для любого $x \in D^*$ найдется $n \in N$ со свойством $H = (K(xn)^* \cap H)\bar{N}F$.*

Доказательство. В силу теоремы 8 факторгруппа $\bar{N}/N$ конечна, и поэтому из конечности индекса $[D^* : H]$ вытекает конечность индекса $[D^* : F]$. В частности, конечна факторгруппа $\mathrm{Nrd}_{D/K}(D^*)/\mathrm{Nrd}_{D/K}(F)$; обозначим через q число ее подгрупп. Далее, выберем конечное подмножество B представителей смежных классов $\mathrm{Nrd}_{D/K}(H)/\mathrm{Nrd}_{D/K}(F)$ и заметим, что в силу наших построений $B \subset \mathrm{Nrd}_{D/K}(D^*) \cap \prod_{v \in T} K_v^{*2}$. Поэтому из предложения 5 при помощи индукции выводится существование таких $n_1 = 1, n_2, \ldots, n_{q+1} \in N$, что $B \subset \mathrm{Nrd}_{D/K}(K(xn_i)^* K(xn_j)^*)$ при $1 \leqslant i < j \leqslant q+1$. Из определения числа q вытекает, что для некоторых $i \neq j$ образы $\mathrm{Nrd}_{D/K}(K(xn_i)^*)$ и $\mathrm{Nrd}_{D/K}(K(xn_j)^*)$ в $\mathrm{Nrd}_{D/K}(D^*)/\mathrm{Nrd}_{D/K}(F)$ совпадают, и тогда для $n = n_i$ имеем

$$\mathrm{Nrd}_{D/K}(H) = B\,\mathrm{Nrd}_{D/K}(F) \subset \mathrm{Nrd}_{D/K}(K(xn)^*)\,\mathrm{Nrd}_{D/K}(F). \quad (15)$$

Покажем, что $\mathrm{Nrd}_{D/K}(H) \cap \mathrm{Nrd}_{D/K}(K(xn)^*) = \mathrm{Nrd}_{D/K}(H \cap K(xn)^*)$. Это вытекает из следующего утверждения:

Лемма 12. *Пусть L/K — квадратичное расширение, $T \subset V^K$ — конечное подмножество и $W \subset L_T = \prod_{v \in T} (L \otimes_K K_v)^*$ — произвольная открытая подгруппа. Тогда*

$$N_{L/K}(L^*) \cap N_{L_T/K_T}(W) = N_{L/K}(L^* \cap W).$$

Действительно, если для $a \in L^*$, $b \in W$ имеем $N_{L/K}(a) = N_{L_T/K_T}(b)$, то $ab^{-1} \in S_T$, где $S = \mathbf{R}^{(1)}_{L/K}(\mathbf{G}_m)$ — соответствующий норменный тор. Из предложения 7.8 вытекает, что S обладает слабой аппроксимацией относительно любого конечного подмножества, поэтому пересечение $(ab^{-1}W) \cap S_K$ непусто, т. е. содержит, скажем, элемент c. Тогда $ac^{-1} \in L^* \cap W$ и $N_{L/K}(ac^{-1}) = N_{L/K}(a)$, что и требовалось.

Теперь (15) можно преобразовать к виду

$$\mathrm{Nrd}_{D/K}(H) = \mathrm{Nrd}_{D/K}(K(xn)^* \cap H)\,\mathrm{Nrd}_{D/K}(F),$$

откуда $H=(K(xn)^*\cap H)(G_K\cap H)F$, и остается воспользоваться тем фактом, что $G_K\cap H=\bar{N}$. Лемма доказана.

Предположим теперь, что факторгруппа $\Gamma=\bar{N}/N$ нетривиальна. Из теоремы 3 вытекает, что Γ совпадает со своим коммутантом и, следовательно, не может быть разрешимой. Поэтому заменяя N на прообраз при естественном гомоморфизме $\bar{N}\to\bar{N}/N$ максимальной разрешимой нормальной подгруппы группы Γ, мы сведем нашу задачу к случаю, когда Γ не содержит разрешимых нормальных делителей. Тогда, в частности, центр Γ тривиален, так что $F\cap\bar{N}=N$, и мы имеем вложение

$$\Gamma=\bar{N}/N\hookrightarrow H/F=\Delta.$$

Как мы видели при доказательстве теоремы 3 для тела кватернионов, из открытости H в T-адической топологии вытекает открытость множества $Z=\{z=x\tau(x)^{-1}\mid x\in H\}$, так что $\bar{N}\subset ZN$. С другой стороны, для любого $x\in H$ найдется $y\in D^*$ со свойством $\tau(x)=yxy^{-1}$, и, следовательно, $z=x\tau(x)^{-1}=[x,\ y]\in G_K\cap$ $\cap\left[N_T\prod_{v\in T}\Phi_v,y\right]\subset G_K\cap N_T=\bar{N}$. Поэтому $Z\subset\bar{N}$ и $\bar{N}=ZN$. Учитывая соотношение $x\tau(x)^{-1}=x^2\,\mathrm{Nrd}_{D/K}(x)^{-1}$ и включение $K^*\subset F$, получаем, что $\Gamma=\Delta^2$. Таким образом, из леммы 11 вытекает, что мы находимся в условиях применимости следующего утверждения из теории групп:

Лемма 13. *Пусть Γ — конечная группа. Предположим, что Γ вкладывается в такую конечную группу Δ, что выполняются следующие условия:*

1) $\Delta^2=\Gamma$;

2) *для любого $g\in\Delta$ найдется такая содержащая g абелева подгруппа $B(g)\subset\Delta$, что $\Delta=B(g)\Gamma$.*

Тогда множество $\Gamma_2=\{g\in\Gamma\mid g^2=e\}$ является нормальной подгруппой в Γ.

(Отметим, что применяя лемму 11 в нашей ситуации, мы для $g=xN$ берем в качестве $B(g)$ образ в Δ пересечения $K(xn)^*\cap H$ из леммы 11.)

Доказательство. Рассмотрим отображение $\psi\colon\Delta\to\Gamma$, $\psi(g)=$ $=g^2$. Тогда из условия 1) получаем, что

$$[\Delta]=\sum_{h\in\Gamma}\left[\psi^{-1}(h)\right]. \tag{16}$$

С другой стороны, если $h\in\Gamma$ и $h=g^2$, $g\in\Delta$, то $\psi^{-1}(h)\supset$ $\supset gB(g)_2$, и поэтому

$$\left[\psi^{-1}(h)\right]\geqslant[B(g)_2]\geqslant[(B(g)/(B(g)\cap\Gamma))_2]=[(\Delta/\Gamma)_2]=[\Delta/\Gamma]. \tag{17}$$

Здесь мы воспользовались тем фактом, что для любой конечной абелевой группы B и любой ее подгруппы C справедливо неравенство $[B_2]\geqslant[(B/C)_2]$. Сопоставляя (16) и (17), получаем, что $[\psi^{-1}(h)]=[\Delta/\Gamma]$ для любого $h\in\Gamma$, и если $h=g^2$, то

$\psi^{-1}(h) = gB(g)_2$. В частности, $\Delta_2 = \psi^{-1}(e) = B(e)_2$ является подгруппой в Δ. Поэтому $\Gamma_2 = \Gamma \cap \Delta_2$ является подгруппой, причем, очевидно, нормальной в Γ. Лемма доказана.

Поскольку мы считаем, что Γ не имеет разрешимых нормальных подгрупп, то из леммы 12 вытекает, что $\Gamma_2 = (e)$, т. е. порядок Γ нечетен. Но тогда по теореме Фейта — Томпсона разрешимой является сама группа Γ — противоречие. Можно рассуждать и не используя теорему Фейта — Томпсона. Действительно, как мы отмечали в начале доказательства теоремы 2, для любого $x \in G_K$ элементы x и $x^{-1} = \tau(x)$ сопряжены в D^*. Если к тому же $x \in \bar{N}$, то из предложения 3 получаем, что образы x и x^{-1} в Γ сопряжены (в Γ). Отсюда следует, что если $g \in \Gamma$ и $g^2 \neq e$, то множество $\{h \in \Gamma \mid hgh^{-1} \in \{g, g^{-1}\}\}$ состоит из двух смежных классов по централизатору элемента g. Тем самым если группа Γ нетривиальна, то она обязательно имеет четный порядок, и, следовательно, $\Gamma_2 \neq (e)$.

Таким образом, мы завершили доказательство теорем 2—4, которое потребовало развития специфического аппарата, названного нами в [4] *мультипликативным арифметическим методом*. Мы сознательно изложили основные результаты мультипликативной арифметики в несколько большей общности, чем это надо для доказательства сформулированных теорем. Естественно, что стремление к такой общности не является здесь самоцелью, а отражает нашу уверенность в том, что использование развитой техники позволит в будущем доказать гипотезу 2 для всех групп G, являющихся внутренними формами типа A_n. В то же время пока мы не имеем практически никаких результатов для алгебраических групп вида $G = \boldsymbol{SU}_1(D)$, где D — конечномерное тело с инволюцией τ второго рода, которые относятся к внешним формам типа A_n. Здесь, по-видимому, следует начать с получения аналогов теорем 3, 4. Отправным пунктом должно стать доказательство совпадения коммутанта унитарной группы $U_1(D) = \{x \in D^* \mid xx^\tau = 1\}$ с $SU_1(D) = U_1(D) \cap SL_1(D)$, что явилось бы аналогом неоднократно использованного нами равенства $SL_1(D) = [D^*, D^*]$. Один из возможных путей видится здесь в использовании тривиальности приведенной унитарной группы Уайтхеда $SUK_1(D) = \Sigma'_\tau/\Sigma_\tau$ (см. § 7.2), где Σ'_τ — подгруппа элементов в D^* с симметрической относительно τ приведенной нормой, Σ_τ порождена симметрическими элементами. А именно, пусть $a \in SU_1(D)$ — элемент, порождающий над центром L тела D максимальное подполе P. Тогда $\tau(P) = P$ и $N_{P/M}(a) = aa^\tau = 1$, где M — подполе симметрических элементов в P. Поэтому по теореме 90 Гильберта $a = b(b^\tau)^{-1}$ для некоторого $b \in P$. При этом

$$\mathrm{Nrd}_{D/K}(b)/\mathrm{Nrd}_{D/K}(b^\tau) = \mathrm{Nrd}_{D/K}\left(b\left(b^\tau\right)^{-1}\right) = \mathrm{Nrd}_{D/K}(a) = 1,$$

так что $b \in \Sigma_\tau'$. Из тривиальности $SUK_1(D)$ вытекает существование таких симметрических $t_1, \ldots, t_r \in D^*$, что $b = t_1, \ldots, t_r$, и тогда

$$a = t_1 \ldots t_r t_1^{-1} \ldots t_r^{-1}. \tag{18}$$

Можно ли преобразовать (18) таким образом, чтобы получить для a выражение в виде произведения коммутаторов из группы $U_1(D)$? Мы рекомендуем читателю поразмышлять над этим (нерешенным) вопросом.

§ 9.3. Группы классических типов

Цель настоящего параграфа — доказать теорему 5. Если рассуждения предыдущего параграфа основывались на использовании внутренней структуры исследуемой группы G, то здесь ключевую роль играет наличие у группы G, относящейся к одному из рассматриваемых типов, удобной геометрической реализации. Исходная идея основана на том факте, что все рассматриваемые классические серии «вырастают» из групп типа $A_1 (B_1 = C_1 = A_1,\ D_2 = A_1 + A_1)$, для которых описание нормальных делителей дает теорема 2, и задача сводится к обоснованию возможности индуктивного перехода от низшей размерности к высшей в вопросе описания нормальных делителей. Здесь удобно условиться о следующей терминологии. Будем говорить, что для односвязной полупростой K-группы G в группе G_K имеет место *стандартное описание нормальных делителей*, если существует такое конечное подмножество $S \subset V^K$, что любой плотный по Зарисскому нормальный делитель $N \subset G_K$ является открытым в G_K в S-адической топологии.

Лемма 14. 1) *Если нормальный делитель $N \subset G_K$ открыт в S-адической топологии, то он открыт и в S_f-адической топологии, где $S_f = S \cap V_f^K$.*

2) *Для простой односвязной K-группы G стандартное описание нормальных делителей в G_K имеет место в том и только том случае, если для нее справедлива гипотеза 2.*

3) *Если полупростая односвязная K-группа G имеет вид $G = \prod_{i=1}^{l} \mathbf{R}_{L_i/K}(G_i)$, где G_i — простые L_i-определенные группы, то стандартное описание нормальных делителей в G_K имеет место в том и только том случае, если оно имеет место во всех группах $(G_i)_{L_i}$. В частности, если все простые компоненты G имеют тип A_1, то для нее имеет место стандартное описание нормальных делителей.*

Доказательство. 1) Если $N = G_K \cap W$, где $W \subset G_S$ — открытое подмножество, то из свойства слабой аппроксимации для G (предложение 7.9) вытекает, что замыкание N_S группы N в G_S

содержит W и поэтому является открытой нормальной подгруппой. Так как для $v \in V_\infty^K$ группа G_{K_v} не имеет нецентральных нормальных подгрупп (предложение 7.6), то рассуждая как и при доказательстве леммы 3, получим, что $N_S = G_{S \cap V_\infty^K} \times N_{S_f}$, причем N_{S_f} — открытый нормальный делитель в G_{S_f}. Учитывая, что N является S-адически замкнутым в G_K, отсюда получаем $N = G_K \cap N_S = G_K \cap N_{S_f}$, т. е. N открыт в S_f-адической топологии.

2) Если для G_K выполняется гипотеза 2, то, очевидно, для нее имеет место стандартное описание нормальных делителей относительно множества $S = T$. Обратно, если в G_K имеет место стандартное описание нормальных делителей относительно множества S, то из формулы $N_S = N_{S \cap T} \times G_{S \setminus (S \cap T)}$ для замыкания N_S нормального делителя $N \subset G_K$ в S-адической топологии (см. лемму 1) вытекает, что любой нецентральный нормальный делитель замкнут в $(S \cap T)$-адической топологии и тем более — в T-адической топологии, что в силу леммы 2 равносильно справедливости гипотезы 2.

3) Имеем $G_K \simeq \prod_{i=1}^{l} (G_i)_{L_i}$, причем для любого конечного подмножества $S \subset V^K$ S-адическая топология на G_K совпадает с произведением $\bar{S}_i$-адических топологий на группах $(G_i)_{L_i}$, где $\bar{S}_i$ состоит из всех продолжений на L_i нормирований из S. Отсюда, в частности, следует, что если стандартное описание нормальных делителей имеет место в группе G_K относительно множества S, то оно имеет место в каждой из групп $(G_i)_{L_i}$ относительно $\bar{S}_i$. Обратно, из стандартного описания нормальных делителей в группах $(G_i)_{L_i}$ относительно подмножеств $S_i \subset V^{L_i}$ вытекает стандартное описание в группе G_K относительно подмножества $S = \bigcup_i V_i$, где V_i состоит из ограничений на K нормирований из S_i. Последнее утверждение п. 3) вытекает из теоремы 2. Лемма 14 полностью доказана.

Пусть теперь G — простая односвязная K-группа одного из типов, указанных в теореме 5. В силу результатов § 2.3 имеется естественное действие группы G на пространстве $\bar{W} = W \otimes_K \bar{K}$, где W — m-мерное пространство над некоторым телом D с инволюцией τ, причем это действие сохраняет эрмитову либо косоэрмитову форму f на W. Все возникающие при этом типы форм перечислены в списке, приведенном в конце п. 4 § 2.3, к которому мы будем постоянно обращаться. Отметим, что в ситуации п. 1) этого списка (группы типа ${}^2A_n$) по условию имеем $D = L$ — квадратичное расширение поля K. С другой стороны, в ситуации п. 3) группа G является K-разложимой, и проектив-

ная простота группы G_K здесь хорошо известна (см. § 7.2); тем самым мы имеем полное право исключить этот случай из дальнейшего рассмотрения. В остальных случаях в пространстве W существуют анизотропные относительно f векторы, и можно воспользоваться следующим утверждением, которое играет ключевую роль при доказательстве теоремы 5.

Теорема 13. *Пусть $m \geqslant m_0+1$, $x \in W$ — произвольный анизотропный вектор и $G(x)$ — его стабилизатор. Тогда если в группе $G(x)_K$ имеет место стандартное описание нормальных делителей, то оно имеет место и в группе G_K.*

(Число m_0 для каждого типа форм было указано в списке из п. 4 § 2.3. Отметим, что при $m \geqslant m_0+1$ группа $G(x)$ односвязна и полупроста (предложение 2.21), и поэтому можно говорить о стандартном описании нормальных делителей в $G(x)_K$.)

Доказательство. Пусть теперь $N \subset G_K$ — произвольный нецентральный (= плотный по Зарисскому) нормальный делитель. По условию существует такое конечное подмножество $S \subset V^K$, что любой плотный по Зарисскому нормальный делитель группы $G(x)_K$ является открытым в S-адической топологии. При этом в силу утверждения 1) леммы 14 можно без ограничения общности считать, что $S \subset V_f^K$. Поскольку N имеет конечный индекс в G_K (теорема 8), то пересечение $G(x)_K \cap N$ имеет конечный индекс в $G(x)_K$ и, в частности, плотно в $G(x)$ в топологии Зарисского. Так как $S \subset V_f^K$, то найдется такая открытая подгруппа $U \subset G_S$, что

$$G(x)_K \cap U \subset G(x)_K \cap N. \tag{1}$$

Положим $X = \{y \in \overline{W} \mid f(y) = f(x)\}$. Мы покажем, что

$$\textit{орбита } (U \cap N)x \textit{ открыта в } G_K x \textit{ в } S_0\textit{-адической топологии}, \tag{2}$$

$$\textit{где } S_0 = S \cup V_\infty^K.$$

Тогда из непрерывности действия G_{S_0} на X_{S_0} вытекает существование такого открытого подмножества $B \subset G_{S_0}$, содержащего единицу, что $(B \cap G_K)x \subset (U \cap N)x$. Пусть $\overline{N}$ — замыкание N в G_K в S_0-адической топологии. Тогда $U \cap N$ плотно в $U \cap \overline{N}$ относительно этой топологии, и, в частности, $U \cap \overline{N} \subset (U \cap N)(B \cap G_K)$. Отсюда следует, что

$$(U \cap \overline{N})x \subset (U \cap N)(B \cap G_K)x \subset (U \cap N)x,$$

и поэтому $U \cap \overline{N} \subset (U \cap N)(G(x)_K \cap U) \subset N$ в силу (1). Но $\overline{N} = (U \cap \overline{N})N$, так что $\overline{N} = N$, и теорема доказана.

Итак, осталось доказать (2). Для этого введем одно техническое понятие. Будем называть вектор $z \in \overline{W}$ *регулярным*, если $f(z) \in \overline{D}^*$. Более общо, $\overline{D}$-подмодуль $V \subset \overline{W}$ называется

регулярным, если он свободен и его дискриминант относительно некоторого (эквивалентно, произвольного) $\bar{D}$-базиса лежит в $\bar{K}^*$.

Лемма 15. 1) *Вектор $z \in W$ регулярен в том и только том случае, если он анизотропен, а для D-подпространства $V \subset W$ $\bar{D}$-подмодуль $V \otimes_K \bar{K}$ регулярен в том и только том случае, если V невырожденно.*

2) *Если $z \in \bar{W}$ — регулярный вектор, то $Z = \{z' \in \bar{W} \mid f(z') = f(z)\}$ является однородным пространством группы G.*

Доказательство. Утверждение 1) очевидно. Для доказательства 2) рассмотрим произвольный анизотропный вектор $x \in W$. Тогда существует такой элемент $d \in \bar{D}^*$, что $f(z) = f(xd)$. Так как согласно теореме Витта (теорема 2.11) многообразие $\{y \in \bar{W} \mid f(y) = f(x)\}$ является однородным пространством группы G, то это же справедливо и для Z. Лемма доказана.

Положим $Y = \{(y, z, g) \in X \times X \times G \mid gx = y,\ gz = z\}$ и обозначим через Y_0 подмножество в Y, состоящее из таких (y, z, g), что:

а) $(x - y)$ — регулярный вектор;

б) $\bar{D}$-подмодуль в $\bar{W}$, порожденный x и z, является $\bar{D}$-свободным и регулярным. (3)

Рассмотрим, далее, проекции

$$p\colon Y \to X \times X,\ p(y, z, g) = (y, z),$$
$$q\colon X \times X \to X,\ q(y, z) = y.$$

Очевидно, $p(Y) \subset F = \{(y, z) \in X \times X \mid f(z, x) = f(z, y)\}$. При этом $p(Y_0) \subset F_0$, где F_0 состоит из пар (y, z), удовлетворяющих (3).

Лемма 16. *Подмножества $Y_0 \subset Y$, $F_0 \subset F$ являются непустыми и открытыми в топологии Зарисского, а морфизмы $p\colon Y_0 \to F_0$ и $q\colon F_0 \to X$ — доминантными.*

Доказательство. Ясно, что $\bar{D}^*$ является открытым по Зарисскому подмножеством в $\bar{D}$, поэтому множество векторов $y \in \bar{W}$, удовлетворяющих условию а) в (3), являясь прообразом $\bar{D}^*$ при отображении $y \mapsto f(x - y)$, также открыто. Аналогично показывается, что множество векторов $z \in \bar{W}$, удовлетворяющих б), открыто. Отсюда следует открытость подмножеств $Y_0 \subset Y$, $F_0 \subset F$.

Обозначим через X_0 подмножество в X, состоящее из таких y, что выполняются следующие условия:

$$\left.\begin{array}{l} \text{(i) вектор } x - y \text{ регулярен;} \\ \text{(ii) } \bar{D}\text{-подмодуль, порожденный } x \text{ и } y\text{, является} \\ \qquad\qquad \bar{D}\text{-свободным и регулярным;} \\ \text{(iii) } f(x - y, x) \in \bar{D}^* \text{ и } f(x - y, x)^{-1} f(x - y, y) - 1 \in \bar{D}^*. \end{array}\right\} \quad (4)$$

Из предыдущего ясно, что X_0 является открытым по Зарисскому

подмножеством в X. Кроме того, если $y \in \overline{W}$ обладает свойствами: $y \perp x$ и $f(y) = f(x)$, то непосредственно проверяется, что $y \in X_0$, и тем самым $X_0 \neq \varnothing$. Поскольку из теоремы Витта вытекает неприводимость X, то X_0 является открытым плотным в X подмножеством. Покажем, что $X_0 \subset q(F_0)$, откуда будет следовать непустота F_0 и доминантность морфизма q: $F_0 \to X$. Итак, пусть $y \in X_0$; положим $\lambda = -f(x-y, x)^{-1} f(x-y, y)$, $t = x\lambda + y$. Непосредственная проверка показывает, что векторы t, $x - y$ образуют ортогональный $\bar{D}$-базис $\bar{D}$-подмодуля, порожденного x и y. Поэтому вектор t регулярен, и подбирая $d \in \bar{D}^*$ таким образом, чтобы $f(td) = f(x)$ для $z = td$, будем иметь $(y, z) \in F_0$, и все доказано. Для доказательства оставшихся утверждений леммы покажем, что $p(Y_0) = F_0$, т. е. если $(y, z) \in F_0$, то $y = g(x)$ для подходящего $g \in G$ со свойством $gz = z$. В силу теоремы 2.11 найдется $h \in G$ со свойством $hx = z$. Тогда, полагая $x_1 = h^{-1}x$, $y_1 = h^{-1}y$, легко видеть, что для построения g достаточно найти такой $s \in G(x)$, что $sx_1 = y_1$. Обозначим через W_0 ортогональное дополнение к x в W и положим $x_2 = x_1 - x f(x)^{-1} f(x_1, x)$, $y_2 = y_1 - x f(x)^{-1} f(y_1, x)$. Тогда $x_2, y_2 \in \overline{W}_0 = W_0 \otimes_K \bar{K}$, $f(x_2) = f(y_2)$ и векторы x_2, y_2 регулярны. Тогда, применяя к пространству $\overline{W}_0$ утверждение 2) леммы 15 и учитывая, что группа $G(x)$ совпадает с универсальной накрывающей специальной унитарной группы пространства W_0, мы и получаем требуемое. Лемма 16 доказана.

Переходим непосредственно к доказательству утверждения (2). При этом нам будет удобно считать, что открытая подгруппа $U \subset G_S$ в (1) имеет вид $U = \prod_{v \in S} U_v$, где $U_v \subset G_{K_v}$ — открытая подгруппа для каждого $v \in S$ (этого всегда можно достичь, уменьшая U). Положим $U_0 = U \times G_{S_0 \setminus S} = \prod_{v \in S_0} U_v$, где считаем $U_v = G_{K_v}$ для $v \in S_0 \setminus S = V_\infty^K$, $C = (Y_0)_{S_0} \cap (X_{S_0} \times U_0 x \times U_0)$.

Лемма 17. 1) *Многообразия Y и F_0 неприводимы.*

2) $C = \prod_{v \in S_0} C_v$, *где $C_v \subset Y_{0K_v}$ — непустое открытое в v-адической топологии подмножество, плотное в топологии Зарисского.*

Доказательство. Рассмотрим отображение φ: $P = G \times G(x) \to X \times X \times G$, $(g, h) \mapsto ((ghg^{-1})x, gx, ghg^{-1})$. Используя теорему Витта, легко показать, что $\varphi(P) = Y$. Отсюда вытекает неприводимость Y, а следовательно, и неприводимость F_0, ибо Y_0 открыто в Y, а морфизм p: $Y_0 \to F_0$ доминантен (лемма 16). Легко видеть, что $C = \prod_{v \in S_0} C_v$, где $C_v = (Y_0)_{K_v} \cap (X_{K_v} \times U_v x \times U_v)$, и поэтому из предложения 3.3 вытекает открытость $C_v \subset Y_{K_v}$. С другой стороны, $C_v \supset \varphi((U_v \times (G(x) \cap U_v)) \cap P_0)$, где $P_0 = \varphi^{-1}(Y_0)$. В силу гладкости и неприводимости P множество

$U_v \times (G(x) \cap U_v)$ является плотным (лемма 3.2), а множество P_0 — открытым по Зарисскому в P, откуда без труда следует плотность C_v. Лемма 17 доказана.

Для каждого $v \in S_0$ из плотности C_v в Y вытекает существование такой простой точки $c \in C_v$, что $b = p(c)$ — простая точка многообразия F_0 и дифференциал $d_c p$: $T_c(Y) \to T_b(F)$ сюръективен. Тогда в силу предложения 3.3 $p(C_v)$ содержит открытое в v-адической топологии подмножество $B_v \subset F_{0K_v}$, плотное в топологии Зарисского. Применяя это рассуждение еще раз, получим, что $q(B_v)$ содержит открытое в X_{K_v} подмножество E_v. Положим $B = \prod_{v \in S_0} B_v$, $E = \prod_{v \in S_0} E_v$. Тогда для доказательства (2) достаточно установить включение

$$E \cap X_K \subset (U \cap N)\, x. \tag{5}$$

Пусть $y \in E \cap X_K$. Тогда по построению найдется такая точка $\bar{z} \in X_{S_0}$, что $(y, \bar{z}) \in B$. Если $\bar{z} = (z_v)_{v \in S_0}$, то для любого $v \in S_0$ имеем

$$f(z_v, x) = f(z_v, y),$$
$$f(z_v) = f(x).$$

Таким образом, если обозначить через g ограничение формы f на ортогональное дополнение W_0 к вектору $(x - y)$, то для многообразия $Z = \{t \in W_0 \otimes_K \bar{K} \mid g(t) = f(x)\}$ имеем $Z_{K_v} \neq \varnothing$ для всех $v \in S_0$; в частности, $Z_{K_v} \neq \varnothing$ для $v \in V_\infty^K$. Так как $m \geqslant m_0 + 1$, то $\dim W_0 = m - 1 \geqslant m_0$. Поэтому сопоставляя значения числа m_0 с минимальными значениями размерности в утверждениях 1′, 2—3 из § 6.6, получаем, что $Z_K \neq \varnothing$. Далее, существует такая окрестность $J \subset Z_{S_0}$ точки $\bar{z}$, что $(y, J) \subset B$. Согласно следствию 2 из предложения 7.4 многообразие Z обладает слабой аппроксимацией, в силу чего найдется точка $z \in Z_K \cap J$. Тогда $(y, z) \in p(C)$, т. е. $z \in U_0 x$, и подпространство, натянутое на x, z, является невырожденным. Воспользуемся теперь следующим утверждением:

Лемма 18. *Пусть заданы K-определенное действие алгебраической K-группы H на алгебраическом K-многообразии M и конечное подмножество $S \subset V^K$, содержащее V_∞^K. Если $x \in M_K$ — такая точка, что стабилизатор $H(x)$ полупрост и односвязен, то для любой открытой подгруппы $U \subset H_S$ справедливо равенство $M_K \cap Ux = (H_K \cap U)\, x$.*

Доказательство вытекает из справедливости для $H(x)$ принципа Хассе (теорема 6.6) и свойства о слабой аппроксимации (предложение 7.9). Действительно, пусть $y \in M_K \cap Ux$ и $y = hx$, где $h \in H_{\bar{K}}$. Тогда для любого $\sigma \in \mathrm{Gal}(\bar{K}/K)$ элемент $\alpha_\sigma = h^{-1}\sigma(h)$ лежит в $H(x)$, причем семейство $\{\alpha_\sigma\}$ определяет

коцикл $\xi \in H^1(K, H(x))$. Так как по условию $y \in H_{K_v}x$ для $v \in S \supset V_\infty^K$, то ξ лежит в ядре отображения $H^1(K, H(x)) \to \to \prod_{v \in V_\infty^K} H^1(K_v, H(x))$. Поэтому из справедливости для $H(x)$ принципа Хассе получаем, что коцикл ξ тривиален, т. е. $a_\sigma = h^{-1}\sigma(h) = g^{-1}\sigma(g)$ для подходящего $g \in H(x)$ и для всех $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Тогда $h' = hg^{-1} \in H_K$ и $y = h'x \in H_K x$. Итак, $y = h_1 x = h_2 x$, где $h_1 \in H_K$, $h_2 \in U$. Тогда $r = h_1^{-1}h_2 \in H(x)_S$, и по свойству слабой аппроксимации существует элемент $t \in H(x)_K \cap (r(H(x)_S \cap U))$. Имеем $h_1 t \in H_K \cap U$ и $y = (h_1 t)x \in (H_K \cap U)x$. Лемма доказана.

Применяя лемму 18 к действию G на X, с учетом односвязности $G(x)$ (предложение 2.21) получим, что $X_K \cap U_0 x = (G_K \cap U_0)x$ и, в частности,

$$z = gx, \quad g \in G_K \cap U_0. \tag{6}$$

Далее, по построению $(y, z) \in p(C)$, т. е. $y \in (G(z)_{S_0} \cap U_0)x$. Поэтому, применяя лемму 5 к действию группы $G(z)$ на X, что возможно, ибо в силу предложения 2.21 группа $G(x, z)$ опять односвязна, получим, что

$$y = hx, \quad h \in G(z)_K \cap U_0. \tag{7}$$

Поскольку $G(z) = gG(x)g^{-1}$, то из (6), (7) вытекает, что $h \in G(z)_K \cap U_0 = g(G(x)_K \cap U_0)g^{-1} = g(G(x)_K \cap U)g^{-1} \subset N \cap U$ и $y = hx \in (N \cap U)x$. Доказательство теоремы 13 завершено.

Доказательство теоремы 4. В силу утверждения 2) леммы 14 достаточно показать, что в G_K имеет место стандартное описание нормальных делителей. Это получается из теоремы 13 при помощи индукции по степени m рассматриваемой группы. Так как указанные в теореме 4 типы в точности отвечают условию $m \geqslant m_0 + 1$, то индуктивный шаг очевиден, и остается дать обоснование базы индукции в каждом случае. Другими словами, нужно в m-мерном пространстве W над D при $m = m_0 + 1$ найти такой анизотропный относительно f вектор x, что в группе $G(x)$ имеет место стандартное описание нормальных делителей. Но в случае 1) из списка классических групп (см. § 2.4, п. 4) при $D = L$, $m = m_0 + 1 = 3$ и в случае 4) при $m = m_0 + 1 = 2$ для любого анизотропного вектора $x \in W$ группа $G(x)$ имеет тип A_1, и поэтому в $G(x)_K$ имеет место стандартное описание нормальных делителей (утверждение 3) леммы 14). Аналогично, в случае 2) при $m = m_0 + 1 = 5$ группа $G(x)$ имеет тип $D_2 = A_1 + A_1$, и опять применима лемма 1. Немного сложнее разбираться со случаем 5), $m = m_0 + 1 = 4$. Здесь группа $H = G(x)$ имеет тип $D_3 = A_3$. Покажем, что вектор $x \in W$ можно выбрать таким образом, чтобы группа H оказалась либо

K-изотропной (и тогда отсутствие собственных нецентральных нормальных делителей в H_K вытекает из теоремы 1), либо группой вида $\boldsymbol{SU}_4(f)$, где f — эрмитова форма над квадратичным расширением L/K, которые мы уже рассмотрели. При этом используется следующий признак:

Лемма 19. *Пусть H — простая односвязная K-группа типа A_3. Предположим, что H становится разложимой над некоторым квадратичным расширением L/K. Тогда H есть одна из следующих групп: $\boldsymbol{SL}_4$; $\boldsymbol{SL}_2(D)$, D — тело кватернионов над K; $\boldsymbol{SU}_4(f)$, где f — невырожденная эрмитова форма над L.*

Доказательство легко получается из описания всех групп типа A_n (см. § 2.3).

Тем самым остается построить такой анизотропный вектор $x \in W$, что для группы $H = G(x)$ выполняются условия леммы 19. Сначала покажем, что в пространстве W найдутся векторы e_1, e_2, удовлетворяющие условиям

$$e_1 \perp e_2, \quad f(e_1) = f(e_2) \neq 0. \tag{8}$$

С этой целью для каждого $v \in V_\infty^K$ найдем такие регулярные векторы s^v, $t^v \in W \otimes_K K_v$, что $s^v \perp t^v$, $f(s^v) = f(t^v)$. Используя слабую аппроксимацию в пространстве W и процесс ортогонализации, можно построить такие векторы s, $t \in W$, что $s \perp t$ и

$$f(s) \in f(s^v D_v^*), \quad f(t) \in f(t^v D_v^*) \tag{9}$$

для всех $v \in V_\infty^K$. Положим $e_1 = s$ и покажем, что в ортогональном дополнении W_0 к вектору e_1 найдется вектор e_2, для которого $f(e_2) = f(e_1)$. В силу утверждения 3 из § 6.6 достаточно для каждого $v \in V_\infty^K$ найти вектор $e^v \in W_0 \otimes_K K_v$ такой, что $f(e^v) = f(e_1)$. Но согласно (9) $f(s) = f(s^v d_1)$, $f(t) = f(t^v d_2)$ для подходящих d_1, $d_2 \in D_v^*$. Тогда вектор $e^v = t d_2^{-1} d_1 \in W_0 \otimes_K K_v$ является искомым, ибо $f(e^v) = f(t^v d_1) = f(s^v d_1) = f(s)$. Таким образом, существование векторов e_1, e_2, удовлетворяющих (8), установлено.

Положим $U = e_1 D + e_2 D$ и обозначим через h ограничение формы f на U. Тогда группа $F = \boldsymbol{SU}_2(h)$ относится к типу $D_2 = A_1 \times A_1$. С другой стороны, F становится разложимой над квадратичным расширением $P = K(a)$ поля K, где $a = f(e_1) = f(e_2)$. Действительно, обозначим через T_i специальную унитарную группу пространства, натянутого на e_i. Тогда $T_i \simeq \mathbf{R}_{P/K}^{(1)}(\boldsymbol{G}_m)$, и $T = T_1 \times T_2$ является максимальным тором в F, откуда и следует требуемое. Из отмеченных фактов вытекает, что $F = F_1 \times F_2$ — прямое произведение групп типа A_1 над K. Имеем $F_i = \boldsymbol{SL}_1(D_i)$, где D_i — алгебра кватернионов над K. Сейчас мы установим существование такого вектора $e_3 \in U^\perp$, что $b = f(e_3) \neq 0$ и поле $L = K(b)$ расщепляет алгебры D_1 и

D_2. Утверждается, что тогда в качестве x можно взять любой вектор, ортогональный e_1, e_2, e_3. В самом деле, положим $H = G(x)$ и покажем, что группа H является L-разложимой. Очевидно, H содержит произведение $F \times T_3$, где $T_3 \simeq \mathbf{R}^{(1)}_{L/K}(\boldsymbol{G}_m)$ — одномерный тор, являющийся специальной унитарной группой пространства, натянутого на e_3. Но по построению L расщепляет группу F и тор T_3, и все доказано, ибо ранги H и произведения $F \times T_3$ совпадают.

Для построения e_3 обозначим через S конечное подмножество в V^K, состоящее из таких v, что хотя бы одна из алгебр D_{1v}, D_{2v} является телом. Пусть $v \in S$; тогда в пространстве $U^\perp \otimes_K K_v$ найдется такой регулярный вектор u^v, что для $b^v = f(u^v)$ алгебра $K_v[b^v]$ является полем. Действительно, если D_v — тело, то в качестве u^v можно взять произвольный анизотропный вектор; в противном случае следует воспользоваться тем фактом, что 4-мерная квадратичная форма над K_v всегда содержит анизотропную бинарную подформу (отметим, что поскольку $v \in S$, то заведомо $K_v \neq \mathbb{C}$). Возьмем в качестве e_3 вектор из $U^\perp$, который настолько близок к векторам u^v для $v \in S$, что для $b = f(e_3)$ алгебры $K_v[b]$ и $K_v[b^v]$ изоморфны при всех $v \in S$ (существование такой аппроксимации легко устанавливается, например, при помощи леммы Краснера, см § 6.4). Тогда из наших построений и сказанного в п. 1 § 1.5 вытекает, что поле $L = K(b)$ является искомым. Теорема 5 полностью доказана.

Нам осталось провести доказательство теоремы 6. Итак, пусть G — простая алгебраическая K-группа типа G_2. Хорошо известно (см. Джекобсон [1]), что G реализуется как группа всех автоморфизмов алгебры $C \otimes_K K$, где C — некоторая алгебра октав над K. На алгебре C имеется «норменное» отображение N: $C \to K$, которое является невырожденной квадратичной формой степени 8 от координат в базисе C/K. Обозначим через W пространство «чистых» октав, т. е. ортогональное дополнение к единице алгебры C относительно билинейной формы $(|)$, ассоциированной с N, и пусть f — ограничение N на W. Пространство $\overline{W} = W \otimes_K \overline{K}$ и форма f инвариантны относительно G, причем, ограничивая действие группы G на W, мы получаем ее известное 7-мерное K-определенное представление.

Доказательство теоремы 6 использует следующие свойства этого представления:

Предложение 6 (теорема Витта). *Пусть $a, b \in \overline{W}$ — два анизотропных вектора такие, что $f(a) = f(b)$. Тогда существует $g \in G$ со свойством $g(b) = a$. Далее, если a_1, a_2 и b_1, b_2 — две пары векторов из $\overline{W}$, порождающих невырожденные относительно f подпространства, причем $f(a_i) = f(b_i)$ $(i = 1, 2)$, $(a_1 | a_2) = (b_1 | b_2)$, то существует $g \in G$ со свойством $g(b_i) = a_i$ $(i = 1, 2)$.*

Предложение 7. *Для любого анизотропного относительно f вектора $x \in W$ стабилизатор $G(x)$ изоморфен либо группе $\boldsymbol{SL}_3$, либо группе $\boldsymbol{SU}_3(\varphi)$, где φ — невырожденная эрмитова форма над квадратичным расширением L/K, а для пары векторов $x, y \in W$, порождающих невырожденное относительно f подпространство, стабилизатор $G(x, y)$ есть либо $\boldsymbol{SL}_2$, либо $\boldsymbol{SU}_2(\varphi)$. Таким образом, группы $G(x)$ и $G(x, y)$ являются полупростыми и односвязными.*

Из предложения 7 и теоремы 5 вытекает, что для анизотропного $x \in W$ в группе $G(x)_K$ имеет место стандартное описание нормальных делителей, поэтому достаточно установить в нашей ситуации аналог теоремы 13. Этот аналог действительно имеет место, причем его доказательство полностью повторяет доказательство самой теоремы 13. Вся необходимая для этого арифметическая информация сосредоточена в следующем результате, который непосредсетвенно вытекает из утверждения 1′ в § 6.6 и следствия 2 из предложения 7.4: пусть $z \in W$ — анизотропный вектор, W_0 — ортогональное дополнение к z и $Z = \{x \in W_0 \otimes_K R \mid f(x) = c\}$, где $c \in K^*$; если $Z_{K_v} \neq \varnothing$ для $v \in V_\infty^K$, то $Z_K \neq \varnothing$, причем в этом случае Z обладает слабой аппроксимацией относительно любого конечного подмножества $S \subset V^K$. Восстановить детали рассуждений мы оставляем читателю в качестве упражнения.

Существует еще одно доказательство проективной простоты группы G_K для K-анизотропной группы G типа G_2, принадлежащее В. И. Черноусову (неопубликовано)*). Оно основано на уже использованном нами при доказательстве принципа Хассе для G факте, что любой максимальный K-определенный тор $T \subset G$ лежит в K-определенной подгруппе $H \subset G$ типа A_2 (см. § 6.8). Рассмотрим произвольную нецентральную нормальную подгруппу $N \subset G_K$ и покажем, что $N = G_K$. Пусть $x \in G_K$. Так как группа G предполагается K-анизотропной, то элемент x является полупростым и, следовательно, содержится в некотором K-определенном максимальном торе $T \subset G$. Рассмотрим содержащую T K-определенную подгруппу $H \subset G$ типа A_2. В силу теоремы 8 индекс $[G_K : N]$ конечен, откуда, в частности, вытекает, что пересечение $H_K \cap N$ является нецентральной нормальной подгруппой в H_K. Поэтому, чтобы установить включение $x \in N$ и тем самым завершить доказательство требуемого факта, достаточно установить проективную простоту группы H_K. Но это будет следовать из теоремы 5, если показать, что H имеет вид $\boldsymbol{SU}_3(f)$ для подходящей эрмитовой формы f над некоторым квадратичным расширением L/K. Для этого воспользуемся тем

*) Можно показать, что любая K-группа типа G_2 является либо K-разложимой, либо K-анизотропной, тем самым мы получаем другое доказательство теоремы 6.

фактом (см. предложение 6.17), что группа G становится разложимой над квадратичным расширением L/K. Пусть $B \subset G$ — — L-определенная подгруппа Бореля. Имеем $\dim G = 14$, $\dim H = 8$ и $\dim B = 8$, так что $\dim(B \cap H) \geqslant 2$. Отсюда следует, что группа H над L становится изотропной. С другой стороны, список всех возможностей для H выглядит следующим образом:

$$^1A_2 = \begin{cases} \text{(i)} & \boldsymbol{SL}_3, \\ \text{(ii)} & \boldsymbol{SL}_1(D),\ D \text{ — тело индекса } 3; \end{cases}$$

$$^2A_2 = \begin{cases} \text{(iii)} & \boldsymbol{SU}_3(f), \\ \text{(iv)} & \boldsymbol{SU}_1(D),\ D \text{ — тело индекса } 3, \end{cases}$$

и ни одна из групп в случаях (ii) и (iv) L-изотропной быть не может. Доказательство завершено.

§ 9.4. Группы, разложимые над квадратичным расширением

Настоящий параграф посвящен доказательству теоремы 7. Мы будем вести рассуждения индукцией по рангу l группы G. При $l = 2$ группа G относится к одному из следующих трех типов: A_2, $B_2 = C_2$ или G_2. Для групп типов B_2 или G_2 отсутствие нецентральных нормальных делителей в G_K вытекает из теорем 5 и 6. Изучение нормального строения произвольных групп типа A_2 пока не завершено, однако в нашей ситуации встречаются лишь группы этого типа, разложимые над квадратичным расширением L/K. Такие группы имеют вид $G = \boldsymbol{SU}_3(f)$, где f — невырожденная трехмерная эрмитова форма над L (см. рассуждения в конце предыдущего параграфа), и проективная простота G_K снова вытекает из теоремы 5.

Предположим, что утверждение теоремы справедливо для всех указанных в ее формулировке групп ранга, меньшего l ($l \geqslant 3$), и покажем, что оно верно, если ранг группы G равен l. С этой целью мы установим существование такого открытого подмножества $U \subset G_\infty$, что любой элемент $g \in G_K \cap U$ представим в виде

$$g = g_1 \cdots g_m, \tag{1}$$

где элемент g_i ($i = 1, \ldots, m$) лежит в группе G_{iK} для подходящей простой односвязной K-определенной подгруппы $G_i \subset G$, разложимой над L и имеющей ранг от 2 до $l - 1$. Тогда если $N \subset G_K$ — нецентральная нормальная подгруппа, то $[G_K : N] < \infty$ (теорема 8), и, в частности, пересечение $G_{iK} \cap N$ является нецентральной нормальной подгруппой в G_{iK}. Поэтому по предположению индукции $G_{iK} \cap N = G_{iK}$, откуда $g \in N$, и, значит, $G_K \cap U \subset N$. Но согласно лемме 1 $N_\infty = G_\infty$, так что $NU = G_\infty$

и $N(G_K \cap U) = G_K$. Поэтому окончательно получаем, что $N = G_K$, и теорема доказана.

Чтобы установить существование разложения (1), нам понадобится структурная информация о группе G. Согласно лемме 6.20 существует максимальный K-определенный тор $T \subset G$, разложимый над расширением L/K. Как мы отмечали после доказательства леммы 6.20 (§ 6.6), нетривиальный автоморфизм $\sigma \in \mathrm{Gal}(L/K)$ действует на группе характеров $\mathbf{X}(T)$ умножением на (-1), так что для любого корня $\alpha \in R = R(T, G)$ корневая подгруппа $G_\alpha \subset G$, порожденная одномерными унипотентными подгруппами U_α и $U_{-\alpha}$, определена над K (отметим, что $G_\alpha \simeq \boldsymbol{SL}_2$ над полем L). Зафиксируем, далее, некоторую подсистему простых корней $\Pi \subset R$ и для любого подмножества $\Sigma \subset \Pi$ обозначим через G_Σ подгруппу в G, порожденную группами G_α для $\alpha \in \Sigma$. Положим, наконец, $T_\Sigma = T \cap G_\Sigma$ (в частности, $T_\alpha = T \cap G_\alpha$). Нам понадобятся следующие хорошо известные свойства (см., например, Стейнберг [2]):

$$\left.\begin{array}{l} 1)\ \text{для любого подмножества } \Sigma \subset \Pi \text{ группа } G_\Sigma \text{ является} \\ \text{полупростой односвязной } K\text{-группой ранга, равного } [\Sigma]; \\ 2)\ \text{если } \Sigma_1 \cap \Sigma_2 = \varnothing, \text{ то } G_{\Sigma_1} \cap G_{\Sigma_2} = (1); \\ 3)\ T = \prod\limits_{\alpha \in \Pi} T_\alpha. \end{array}\right\} \quad (2)$$

В каждой группе $(G_\alpha)_L (\alpha \in \Pi)$ выберем элемент w_α, который является представителем нетривиального элемента $\bar{w}_\alpha$ группы Вейля $W(T_\alpha, G_\alpha)$, и обозначим через X'_α соответствующую «большую клетку» в разложении Брюа группы G_α, т. е. положим $X'_\alpha = B_\alpha w_\alpha B_\alpha$, где $B_\alpha = T_\alpha U_\alpha$ — подгруппа Бореля в G_α. Так как $\sigma(B_\alpha) = B_{-\alpha} = T_\alpha U_{-\alpha}$ и $\sigma(w_\alpha) = w_\alpha t$ для подходящего $t \in T_\alpha$, то $\sigma(X'_\alpha) = B_{-\alpha} w_\alpha B_{-\alpha}$; следовательно, многообразие

$$X_\alpha = X'_\alpha \cap \sigma(X'_\alpha) = B_\alpha w_\alpha B_\alpha \cap B_{-\alpha} w_\alpha B_{-\alpha} \quad (3)$$

определено над K и является открытым плотным подмножеством в G_α. В частности, $\dim X_\alpha = 3$. Положим также $Y_\alpha = X_\alpha T = TX_\alpha$ и заметим, что в действительности $Y_\alpha \simeq X_\alpha \times T_{\Pi \setminus \{\alpha\}}$ в силу свойства 2) в (2).

В § 2.1, п. 10 мы отмечали, что множество $S = \{\bar{w}_\alpha \mid \alpha \in \Pi\}$ порождает группу Вейля $W = W(T, G)$, причем пара (W, S) является группой Кокстера. Рассмотрим элемент $\bar{w} \in W$, имеющий максимальную длину относительно множества образующих S. Известно (см. Бурбаки [4]), что такой элемент единствен и характеризуется тем свойством, что переводит положительные корни в отрицательные, причем длина r его приведенного разложения $\bar{w} = \bar{w}_{\alpha_1} \ldots \bar{w}_{\alpha_r}$ $(\alpha_i \in \Pi)$ совпадает с числом положительных корней (отметим, что среди корней α_i заведомо имеются совпадающие). Положим $X = X_{\alpha_1} \times \ldots \times X_{\alpha_r}$, $Y = Y_{\alpha_1} \times \ldots$

$\ldots \times Y_{\alpha_r}$, и пусть $\varphi\colon Y \to G$ — морфизм-произведение. Определим, кроме того, действие тора T^{r-1} на Y следующим образом: если $t=(t_1, \ldots, t_{r-1}) \in T^{r-1}$, $y=(y_1, \ldots, y_r) \in Y$, то

$$yt=\left(y_1t_1, t_1^{-1}y_2t_2, \ldots, t_{r-2}^{-1}y_{r-1}t_{r-1}, t_{r-1}^{-1}y_r\right) \tag{4}$$

(в этом параграфе нам удобно рассматривать «правое» действие, а не «левое», как обычно). Из равенств $Y_\alpha = X_\alpha T = TX_\alpha$ вытекает, что правая часть (4) попадает в Y, и, следовательно, действие определено корректно. При этом из (4) непосредственно видно, что стабилизатор в T^{r-1} любой точки $y \in Y$ тривиален.

Лемма 20. 1) *Для любого расширения P/K имеем $\varphi(X_P) = \varphi(Y_P)$.*

2) *Морфизм φ является доминантным, а его непустые слои совпадают с орбитами тора T^{r-1}.*

(В современной терминологии утверждение 2), в частности, означает, что Y является торсером с базой $\varphi(Y)$ и структурной группой T^{r-1}.)

Доказательство. 1) Поскольку $Y_\alpha \simeq X_\alpha \times T_{\Pi \setminus \{\alpha\}}$, то $(Y_\alpha)_P = (X_\alpha)_P\,(T_{\Pi \setminus \{\alpha\}})_P$. Но, как мы отмечали выше, T нормализует X_α, и поэтому T_P нормализует $(X_\alpha)_P$. С другой стороны, $(X_\alpha)_P(T_\alpha)_P = (X_\alpha)_P$. Используя эти факты, легко показать, что $\varphi((Y_{\alpha_1})_P \times \ldots \times (Y_{\alpha_r})_P) = \varphi((X_{\alpha_1})_P \times \ldots \times (X_{\alpha_r})_P)$.

2) Для $m \leqslant r$ рассмотрим морфизм-произведение $\varphi^{(m)}\colon Y^{(m)} = Y_{\alpha_1} \times \ldots \times Y_{\alpha_m} \to G$ и индукцией по m покажем, что слои морфизма $\varphi^{(m)}$ совпадают с орбитами действия тора T^{m-1} на $Y^{(m)}$, задаваемого формулой, аналогичной (4):

$$(y_1, \ldots, y_m)(t_1, \ldots, t_{m-1}) = \left(y_1t_1, t_1^{-1}y_2t_2, \ldots, t_{m-2}^{-1}y_{m-1}t_{m-1}, t_{m-1}^{-1}y_m\right). \tag{5}$$

Из (5) вытекает, что $\varphi^{(m)}(yT^{m-1}) = \varphi^{(m)}(y)$ для любой точки $y \in Y^{(m)}$. Поэтому остается показать, что если $\varphi^{(m)}(y) = \varphi^{(m)}(z)$, то $z = yt$ для подходящего $t \in T^{m-1}$. Для $m=1$ утверждение очевидно. Пусть $m > 1$ и для $y_i, z_i \in Y_{\alpha_i}$ $(i = 1, \ldots, m)$ имеем

$$y_1 \ldots y_m = z_1 \ldots z_m. \tag{6}$$

Положим $g = y_m z_m^{-1}$ и покажем, что $g \in T$. Из (3) вытекает, что $Y_\alpha \subset Bw_\alpha B \cap B^- w_\alpha B^-$, где B — подгруппа Бореля в G, ассоциированная с системой простых корней Π, B^- — противоположная подгруппа Бореля. Покажем, что $g \in B$; аналогично показывается, что $g \in B^-$, и тогда $g \in B \cap B^- = T$, что и требовалось. Так как группа G_{α_m} нормализуется тором T, то $g \in G_{\alpha_m}T$. Если предположить, что $g \notin B$, то из разложения Брюа $G_{\alpha_m} = B_{\alpha_m} \cup B_{\alpha_m} w_{\alpha_m} B_{\alpha_m}$ в группе G_{α_m} вытекает, что $g \in$

$\in (B_{\alpha_m} w_{\alpha_m} B_{\alpha_m}) T \subset B w_{\alpha_m} B$. Поскольку произведение $\bar{w}_{\alpha_1}, \ldots, \bar{w}_{\alpha_m}$, будучи отрезком приведенного разложения $\bar{w}$, несократимо, то $(B w_{\alpha_1} \ldots w_{\alpha_i} B)(B w_{\alpha_{i+1}} B) = B w_{\alpha_1} \ldots w_{\alpha_{i+1}} B$ для любого $i < m$ (см. Стейнберг [2]), откуда получаем, что

$$z' = z_1 \ldots z_{m-1} \in B w_{\alpha_1} \ldots w_{\alpha_{m-1}} B,$$

$$y' = y_1 \ldots y_{m-1} g \in B w_{\alpha_1} \ldots w_{\alpha_m} B.$$

Но в силу (6) $y' = z'$, что противоречит тому факту, что двойные смежные классы в разложении Брюа для группы G не пересекаются. Итак, $g \in T$. Тогда $y_{m-1} g \in Y_{\alpha_{m-1}}$, и из соотношения $y' = z'$ по предположению индукции вытекает существование таких $t_1, \ldots, t_{m-2} \in T$, что

$$z_1 = y_1 t_1,\ z_2 = t_1^{-1} y_2 t_2,\ \ldots,\ z_{m-1} = t_{m-2}^{-1} y_{m-1} g.$$

Тогда, полагая $t_{m-1} = g$ и $t = (t_1, \ldots, t_{m-1})$, будем иметь $(y_1, \ldots, y_m) t = (z_1, \ldots, z_m)$.

Таким образом, слои морфизма φ совпадают с орбитами тора T^{r-1} и поэтому имеют размерность $l(r-1)$, где l — ранг группы G. Поэтому из теоремы о размерности слоев и образа морфизма вытекает, что

$$\dim \overline{\varphi(Y)} = r \dim Y_\alpha - (r-1) l =$$
$$= r(3 + (l-1)) - (r-1) l = 2r + l = \dim G,$$

ибо $2r$ совпадает с числом всех корней группы G. Таким образом, морфизм φ доминантен, и лемма 20 доказана.

Из доминантности морфизма $\varphi\colon Y \to G$ и предложения 3.3 вытекает, что $\varphi(Y_\infty)$ содержит открытое в G_∞ подмножество U. Покажем, что для $g \in G_K \cap U$ имеет место разложение (1). Пусть $y \in \varphi^{-1}(g)_{\bar{K}}$. Тогда для любого $\theta \in \mathrm{Gal}(\bar{K}/K)$ имеем $\varphi(y) = \varphi(\theta(y)) = g$, так что в силу леммы 20 найдется единственный элемент $t_\theta \in T_{\bar{K}}^{r-1}$ со свойством $\theta(y) = y t_\theta$. Легко проверяется, что семейство $\xi = \{t_\theta \mid \theta \in \mathrm{Gal}(\bar{K}/K)\}$ определяет коцикл со значениями в T^{r-1}, причем для произвольного расширения P поля K включения $g \in \varphi(Y_P)$ и $\xi \in \mathrm{Ker}(H^1(K, T^{r-1}) \to H^1(P, T^{r-1}))$ равносильны. По построению тор T разложим над L, так что $H^1(L, T^{r-1}) = 1$, и, следовательно, $g \in \varphi(Y_L)$. Но $\varphi(Y_L) = \varphi(X_L)$ (утверждение 1) леммы 20), поэтому элемент $x = (x_1, \ldots, x_r)$ со свойством $\varphi(x) = g$ можно выбрать уже в X_L. Обозначим через $\xi = \{t_\theta\}$ такой коцикл в $H^1(K, T^{r-1})$, что $\theta(x) = x t_\theta$. Основное для дальнейшего свойство коцикла ξ состоит в том, что $\xi \in \mathrm{Ker}\left(H^1(K, T^{r-1}) \to \prod_{v \in V_\infty^K} H^1(K_v, T^{r-1})\right)$, ибо по построению $g \in \varphi(Y_\infty)$. Кроме того, $g \in \varphi(Y_L)$, и поэтому ξ

попадает в подгруппу $H^1(L/K, T^{r-1})$, т. е. задается одним элементом $t = t_\sigma \in T_L^{r-1}$ таким, что $t\sigma(t) = 1$. Используя эти факты, мы покажем, как перейти от разложения

$$g = x_1 \ldots x_r \tag{7}$$

к разложению вида (1). Пусть $\alpha \in \Pi$ — «крайний» корень в диаграмме Дынкина системы корней R, β — (единственный) соседний с ним корень

Положим $\Sigma = \Pi \setminus \{\alpha\}$. Нам достаточно установить существование таких элементов $g_i \in G_{iK}$ $(i = 1, \ldots, d)$, где G_i — простая односвязная L-разложимая K-подгруппа в G ранга 2, что элемент $g' = g_d \ldots g_1 g$ допускает представление вида

$$g' = h_1 h_2, \tag{8}$$

где $h_1 \in (G_\Sigma)_L$, $h_2 \in (G_\alpha)_L$. Действительно, поскольку $g' \in G_K$, а $G_\Sigma \cap G_\alpha = (1)$, то из (8) вытекает, что $h_1 \in (G_\Sigma)_K$, $h_2 \in (G_\alpha)_K \subset \subset (G_{\{\alpha, \beta\}})_K$, и поэтому эквивалентное (8) разложение $g = g_1^{-1} \ldots g_d^{-1} h_1 h_2$ удовлетворяет всем требованиям, предъявляемым к разложению (1). Для осуществления перехода от разложения (7) к разложению (8), нужно в (7) «переставить» сомножители таким образом, чтобы собрать отдельно все x_i, для которых $\alpha_i \in \Sigma$, и все x_i, для которых $\alpha_i = \alpha$, компенсируя перестановку умножением на подходящие g_i. Это легко достигается при помощи очевидного индуктивного рассуждения, построенного на следующем утверждении:

Предложение 8. *Пусть элемент $z \in G_K$ имеет вид $z = z_1 z_2 x_i \ldots x_r$, где $z_1 \in (G_\Sigma)_L$, $z_2 \in (G_\alpha)_L$, а x_i — сомножители из разложения (7). Тогда найдется такая простая односвязная L-разложимая K-подгруппа $H \subset G$ ранга 2 и такие элементы $g \in H_K$, $z_3 \in (G_\Sigma)_L$, $z_4 \in (G_\alpha)_L$, что $gz = z_3 z_4 x_{i+1} \ldots x_r$.*

Доказательство. Если $\alpha_i = \alpha$, то можно положить $z_3 = z_1$, $z_4 = z_2 x_i$. Если $\alpha_i \neq \alpha, \beta$, то корней вида $j\alpha_i + k\alpha$, $(j, k \in \mathbb{Z} \setminus (0))$ не существует, поэтому из соотношений коммутирования (см. Стейнберг [2]) вытекает, что группы G_{α_i} и G_α перестановочны. В частности, перестановочны элементы z_2 и x_i, и можно положить $z_3 = z_1 x_i$, $z_4 = z_2$. Поэтому остается рассмотреть случай $\alpha_i = \beta$. Пусть $t = (t_1, \ldots, t_{r-1}) \in T_L^{r-1}$ — введенный выше элемент со свойствами $t\sigma(t) = 1$ и $\sigma(x) = xt$. Тогда

$$\sigma(x_1) = x_1 t_1, \quad \sigma(x_2) = t_1^{-1} x_2 t_2, \ \ldots, \ \sigma(x_r) = t_{r-1}^{-1} x_r. \tag{9}$$

Мы будем работать с «частями» элемента t, а именно, положим $u = t_i$ и обозначим через s проекцию элемента t_{i-1} на T_Σ в смысле прямого разложения $T = T_\Sigma \times T_\alpha$. Из соотношения

$t\sigma(t)=1$ вытекает, что $s\sigma(s)=u\sigma(u)=1$, т. е. элементы s и u определяют коциклы в $H^1(L/K, T_\Sigma)$ и $H^1(L/K, T)$ соответственно. Отметим, что эти коциклы становятся тривиальными при переходе к вещественным локализациям, ибо по построению коцикл $\xi \in H^1(L/K, T^{r-1})$, определяемый элементом t, лежит в

$$\operatorname{Ker}\Big(H^1(K, T^{r-1}) \to \prod_{v \in V_\infty^K} H^1(K_v, T^{r-1})\Big).$$

Положим $a=z_1$, $b=z_1z_2x_i$.

Лемма 21. $\sigma(a)=as$, $\sigma(b)=bu$.

Доказательство. Поскольку $z = bx_{i+1} \ldots x_r \in G_K$, то $b^{-1}\sigma(b)=(x_{i+1} \ldots x_r)\sigma(x_{i+1} \ldots x_r)^{-1}=t_i=u$ в силу (9). Аналогично показывается, что $\sigma(az_2)=az_2t_{i-1}$. По построению $t_{i-1}=ss'$ для некоторого $s' \in T_\alpha$, откуда $s^{-1}a^{-1}\sigma(a)=(s^{-1}z_2s)s'\sigma(z_2)^{-1} \in G_\Sigma \cap G_\alpha=(1)$ и $\sigma(a)=as$, как и утверждалось.

Лемма 22. *Пусть $f \in G_L$ — такой элемент, что $e=f^{-1}\sigma(f) \in T_L$, $\delta=\operatorname{Int} f$ — соответствующий внутренний автоморфизм. Тогда для любого подмножества $\Delta \subset \Pi$ группа $\delta(G_\Delta)$ и ограничение $\delta|_T$: $T \to \delta(T)$ определены над K.*

Доказательство. Группа $\delta(G_\Delta)$ и морфизм $\delta|_T$ заведомо определены над полем L, поэтому для доказательства их K-определенности достаточно установить их инвариантность относительно σ. Имеем $\sigma(fG_\Delta f^{-1})=\sigma(f)G_\Delta\sigma(f)^{-1}=feG_\Delta e^{-1}f^{-1}=fG_\Delta f^{-1}$, ибо T нормализует G_Δ. Аналогично, для любого $t \in T_L$ получаем $\sigma(ftf^{-1})=fe\sigma(t)e^{-1}f^{-1}=f\sigma(t)f^{-1}$, что и требовалось.

Завершим доказательство предложения 8. Положим $\delta=\operatorname{Int} a$, $H=\delta(G_{\{\alpha,\beta\}})$. Из лемм 21, 22 вытекает, что группа H определена над K и, очевидно, имеет ранг 2. Нам достаточно найти также элементы $h \in H_K$, $y_1 \in (H_\beta)_L$, $y_2 \in (H_\alpha)_L$, где $H_\alpha=\delta(G_\alpha)$, $H_\beta=\delta(G_\beta)$, что

$$h\delta(z_2x_i)=y_1y_2, \tag{10}$$

ибо тогда

$$hz=h\delta(z_2x_i)ax_{i+1} \ldots x_r=y_1y_2ax_{i+1} \ldots x_r=$$
$$=a\delta^{-1}(y_1)\delta^{-1}(y_2)x_{i+1} \ldots x_r,$$

и можно положить $z_3=a\delta^{-1}(y_1)$, $z_4=\delta^{-1}(y_2)$.

Имеем

$$\sigma(\delta(z_2x_i))=\sigma(ba^{-1})=bus^{-1}a^{-1}=\delta(z_2x_i)\delta(us^{-1}). \tag{11}$$

Поэтому наша задача сводится к отысканию таких y_1, y_2, что

$$\sigma(y_1y_2)=y_1y_2\delta(us^{-1}). \tag{12}$$

Действительно, в этом случае из (11) и (12) получаем, что элемент $h=\delta(z_2x_i)(y_1y_2)^{-1}$ лежит в H_K и, очевидно, удовлетворяет (10).

Лемма 23. *Пусть* $\gamma \in \Pi$, $d \in (T_\gamma)_L$ — *такой элемент, что* $d\sigma(d) = 1$. *Предположим, что коцикл в* $H^1(L/K, T_\gamma)$, *определяемый элементом* d, *лежит в* $\operatorname{Ker}\left(H^1(K, T_\gamma) \to \prod_{v \in V_\infty^K} H^1(K_v, T_\gamma)\right)$. *Тогда для любого* $f \in G_L$ *такого, что* $f^{-1}\sigma(f) \in T_L$, *найдется элемент* $g \in f(G_\gamma)_L f^{-1}$ *со свойством* $g^{-1}\sigma(g) = fdf^{-1}$.

Доказательство. Положим $\delta = \operatorname{Int} f$. Тогда согласно предыдущей лемме группа $\delta(G_\gamma)$ и ограничение $\delta|_T$ определены над K. Отсюда следует, что элемент $t = \delta(d)$ определяет коцикл $\xi \in H^1(L/K, \delta(T_\gamma))$, который лежит в $\operatorname{Ker}\left(H^1(K, \delta(T_\gamma)) \to \prod_{v \in V_\infty^K} H^1(K_v, \delta(T_\gamma))\right)$. Но тогда из справедливости принципа Хассе для группы $\delta(G_\gamma)$ получаем, что $\xi \in \operatorname{Ker}(H^1(K, \delta(T_\gamma)) \to H^1(K, \delta(G_\gamma)))$, т. е. $t = g^{-1}\sigma(g)$ для подходящего $g \in \delta(G_\gamma)_L$, и лемма доказана.

В нашей ситуации имеем $\delta(us^{-1}) \in H \cap \delta(T) = \delta(T_{\{\alpha, \beta\}})$, так что $d = us^{-1} \in T_{\{\alpha, \beta\}}$, и можно записать $d = d_1 d_2$, где $d_1 \in (T_\beta)_L$, $d_2 \in (T_\alpha)_L$. Из наших построений вытекает, что элементы d_1 и d_2 определяют коциклы соответственно в $H^1(L/K, T_\beta)$ и $H^1(L/K, T_\alpha)$, которые становятся тривиальными при переходе к вещественным локализациям. Тогда из леммы 23 непосредственно вытекает существование такого $y_1 \in (H_\beta)_L$, что $y_1^{-1}\sigma(y_1) = ad_1a^{-1}$. Положим $f = y_1 a$. Тогда $f^{-1}\sigma(f) = a^{-1}y_1^{-1}\sigma(y_1)a = d_1 \in T_L$. Применяя лемму 23 еще раз, найдем элемент $p \in f(H_\alpha)_L f^{-1}$ со свойством $p^{-1}\sigma(p) = fd_2f^{-1}$. Полагая $y_2 = y_1^{-1}py_1$, будем иметь $\sigma(y_1y_2) = \sigma(y_1)\sigma(y_1)^{-1}\sigma(p)\sigma(y_1) = pfd_2f^{-1}y_1ad_1a^{-1} = pfd_2d_1a^{-1} = y_1y_2\sigma(d_1d_2)$, и соотношение (12) доказано. Таким образом, доказательство предложения 8 и теоремы 7 завершено.

Как мы уже отмечали в § 9.1, из предложения 6.17 вытекает применимость теоремы 7 к любой односвязной K-анизотропной группе, относящейся к одному из типов B_n, C_n, E_7, E_8, F_4, G_2, так что группы K-рациональных точек таких групп всегда являются проективно простыми.

§ 9.5. Конгруэнц-проблема (обзор)

Пусть G — простая односвязная K-группа, $N \subset G_K$ — нецентральный нормальный делитель. Если $S \subset V^K$ — конечное подмножество, содержащее $T \cup V_\infty^K$ *) и такое, что группа G_S

*) Напомним, что через T обозначается совокупность таких $v \in V_f^K$, что группа G является K_v-анизотропной, см. § 9.1.

некомпактна $\left(\text{т. е. } \operatorname{rang}_S G = \sum_{v \in S} \operatorname{rang}_{K_v} G \geqslant 1\right)$, то группа $\Gamma = G_{\mathcal{O}(S)}$ бесконечна, и, как показывает доказательство теоремы 8,

$$G_K/N \simeq \Gamma/\Gamma \cap N. \tag{1}$$

Мы вывели конечность факторгруппы, стоящей в левой части, из конечности факторгруппы, стоящей справа, которая имеет место при выполнении условий: $\operatorname{rang}_S G \geqslant 2$; $\Gamma \cap N \not\subset Z(G)$. Эту связь между нормальным строением группы K-рациональных точек G_K и ее S-арифметических подгрупп (для произвольного $S \subset V^K$, содержащего лишь V^K_∞) естественно изучать дальше. В частности, естественно спросить: какое свойство нормальных делителей группы Γ гарантирует выполнение для группы G_K гипотез 1, 2? Группа Γ всегда обладает обширным семейством нормальных подгрупп конечного индекса, состоящим из конгруэнц-подгрупп

$$\Gamma(\mathfrak{a}) = \{g \in \Gamma \mid g \equiv e \pmod{\mathfrak{a}}\}, \tag{2}$$

отвечающих ненулевым идеалам $\mathfrak{a}$ кольца $\mathcal{O}(S)$. (Как обычно, когда речь идет о целых или S-целых точках, мы фиксируем матричную реализацию G; в частности, сравнение в (2) рассматривается относительно этой реализации.) Таким образом, говоря о нормальном строении Γ, естественно спрашивать, будут ли конгруэнц-подгруппами в определенном смысле исчерпываться *все* нормальные подгруппы в Γ конечного индекса? Некоторый дополнительный анализ показывает, что корректная постановка здесь должна выглядеть следующим образом:

будет ли любая нормальная подгруппа в Γ конечного индекса содержать подходящую конгруэнц-подгруппу $\Gamma(\mathfrak{a})$? (3)

Этот вопрос получил название *конгруэнц-проблемы*. Связь конгруэнц-проблемы с проблемой изучения нормального строения групп рациональных точек раскрывает

Предложение 9. *Пусть G — простая односвязная K-группа, $S \subset V^K$ — конечное подмножество, содержащее V^K_∞. Предположим, что $\operatorname{rang}_S G \geqslant 1$ и конгруэнц-проблема* (3) *для группы $\Gamma = G_{\mathcal{O}(S)}$ решается положительно. Тогда для группы G_K выполняется гипотеза* 2 (*см.* § 9.1).

Доказательство. Обозначим через $\bar{N}$ замыкание N в группе S-аделей G_{A_S}. Тогда, рассуждая как при доказательстве леммы 1 и теоремы 8, легко показать, что

$$\bar{N} = N_{T \setminus (T \cap S)} \times G_{A_{S \cup T}}. \tag{4}$$

Покажем, что $N = G_K \cap N_{T \setminus (T \cap S)} = G_K \cap H$, где $H = N_{T \setminus (T \cap S)} \times G_{T \cap S}$ — открытый нормальный делитель в G_T. По условию для подходящего ненулевого идеала $\mathfrak{a} \in \mathcal{O}(S)$ справедливо

включение $\Gamma(\mathfrak{a}) \subset \Gamma \cap N$. Из определения адельной топологии вытекает существование такой открытой подгруппы $U \subset G_{A_S}$, что $U \cap G_K = \Gamma(\mathfrak{a})$. Тогда $U_0 = U \cap \bar{N}$ является открытой подгруппой в G_{A_S}, содержащейся в $\bar{N}$, и поэтому $\bar{N} = U_0 N$. Пересекая с G_K, в силу (4) будем иметь

$$G_K \cap N_{T \setminus (T \cap S)} = (U_0 \cap G_K) N.$$

Но по построению $U_0 \cap G_K \subset U \cap G_K = \Gamma(\mathfrak{a}) \subset N$, откуда $G_K \cap N_{T \setminus (T \cap S)} = N$, что и требовалось.

Отметим, что приведенное рассуждение показывает, что для справедливости конгруэнц-проблемы для группы Γ необходимо выполнение условия $S \cap T = \varnothing$. В самом деле, пусть $v_0 \in S \cap T$ и $W \subset G_{K_{v_0}}$ — произвольный собственный открытый нормальный делитель. Тогда из слабой аппроксимационной теоремы вытекает выполнение для нормального делителя $N = G_K \cap W$ следующих свойств:

1) $$G_K/N \simeq G_{K_{v_0}}/W \neq 1,$$

2) $$N_{T \setminus (T \cap S)} = G_{T \setminus (T \cap S)}.$$

Предположим теперь, что для группы $\Gamma = G_{\mathcal{T}(S)}$ выполняется утверждение конгруэнц-проблемы (3). Тогда из доказательства предложения 9 и свойства 2) вытекает, что $N = G_K$, а это противоречит свойству 1).

Таким образом, решение проблемы описания нормальных делителей в группе G_K можно получить, положительно решив для группы $\Gamma = G_{\mathcal{O}(S)}$ конгруэнц-проблему (3). В этом смысле конгруэнц-проблема является априори более общей и более сложной задачей. В действительности именно так и обстоит дело. Скажем, отсутствие нормальных делителей в группе $SL_n(\mathbb{Q})$ $(n \geqslant 2)$ было известно очень давно, в то время как полностью решить конгруэнц-проблему для групп $SL_n(\mathbb{Z})$ $(n \geqslant 3)$ удалось лишь в 1964 г., а для группы $SL_2(\mathbb{Z})$ она вообще решается отрицательно! Для того чтобы у читателя сформировалось правильное впечатление о соотношении этих задач, мы дадим краткий исторический обзор исследований по конгруэнц-проблеме, который рекомендуем сопоставить с историческим материалом из § 7.2 и 9.1.

Тот факт, что для группы $\Gamma = SL_2(\mathbb{Z})$ конгруэнц-проблема решается отрицательно, был отмечен Ф. Клейном [1] еще в 1880 г. в связи с исследованиями по модулярным функциям. Однако исследовать конгруэнц-проблему уже для группы $\Gamma = SL_3(\mathbb{Z})$ долгое время не удавалось. Прогресс был достигнут в 1964—65 годах в работах Басса — Лазара — Серра [1] и Меннике [1], содержащих положительное решение конгруэнц-проблемы для групп $SL_n(\mathbb{Z})$ $(n \geqslant 3)$. В ходе дальнейших исследований (см. Басс — Милнор — Серр [1]) выяснилось, что ответ на

конгруэнц-проблему для группы $\Gamma = SL_n(\mathcal{O})$, где $\mathcal{O}$ — кольцо целых поля алгебраических чисел K, определяется не только алгебраическими свойствами самой группы SL_n, но и арифметикой основного поля K. Так, если поле K не является вполне мнимым, то конгруэнц-проблема по-прежнему решается положительно. Напротив, если поле K — вполне мнимое, то ответ на (3) отрицательный, однако существует подгруппа $\Gamma' \subset \Gamma$ конечного индекса, для которой (3) уже решается положительно. Можно показать, что для группы $\Gamma = SL_2(\mathbb{Z})$ такая подгруппа отсутствует. Тем самым возникает необходимость в случае отрицательного ответа на вопрос (3) характеризовать степень нарушения указанного в (3) свойства (называемого конгруэнц-свойством). Так возникает важное в методологическом отношении понятие конгруэнц-ядра (см. Серр [6], Хамфри [3]), которое мы сейчас определим.

Пусть G — определенная над K алгебраическая группа, $S \subset V^K$ — конечное подмножество, содержащее V_∞^K. Тогда несложная проверка, использующая предложение 1 из книги Бурбаки [2] гл. III, § 1, n°2, показывает, что на группе G_K можно определить две хаусдорфовы топологии τ_a и τ_c, относительно которых G_K является топологической группой. Первая из них называется арифметической и имеет в качестве фундаментальной системы окрестностей единицы совокупность всех подгрупп конечного индекса группы Γ, вторая — так называемая конгруэнц-топология — соответственно совокупность всех конгруэнц-подгрупп $\Gamma(\mathfrak{a})$. Используя результаты loc cit. гл. III, § 3, n°4, можно показать, что существуют пополнения $\hat{G}$ и $\bar{G}$ группы G_K относительно этих топологий. При этом, поскольку τ_a сильнее τ_c, возникает непрерывный гомоморфизм $\pi\colon \hat{G} \to \bar{G}$, ядро $C^S(G) = \operatorname{Ker} \pi$ которого называется *конгруэнц-ядром*. Можно рассмотреть также пополнения $\hat{\Gamma}$ и $\bar{\Gamma}$ группы Γ относительно индуцированных топологий, которые совпадают с замыканиями Γ в $\hat{G}$ и $\bar{G}$ соответственно. Тогда π индуцирует непрерывный гомоморфизм $\pi_0\colon \hat{\Gamma} \to \bar{\Gamma}$, причем легко видеть, что $\operatorname{Ker} \pi = \operatorname{Ker} \pi_0 \subset \hat{\Gamma}$. Пополнение $\hat{\Gamma}$ совпадает с *проконечным пополнением* группы Γ, т. е. с проективным пределом $\varprojlim \Gamma/N$ по всем нормальным делителям конечного индекса. Отсюда легко получается следующее утверждение (см. Серр [2], Хамфри [3]):

Предложение 10. *Проекция π сюръективна, а ее ядро $C^S(G)$ является проконечной группой. При этом $C^S(G)$ тривиально в том и только том случае, если для группы $\Gamma = G_{\mathcal{O}(S)}$ выполняется конгруэнц-проблема в форме* (3)*).

---

*) В настоящем параграфе большинство утверждений будет приведено без доказательства.

Таким образом, конгруэнц-ядро $C^S(G)$ измеряет степень отклонения от положительного решения конгруэнц-проблемы в форме (3). Поэтому под конгруэнц-проблемой в современной постановке понимают проблему вычисления конгруэнц-ядра $C^S(G)$, в отличие от постановки в форме (3), которую принято называть классической. Используя понятие конгруэнц-ядра, результат Басса — Милнора — Серра [1] можно сформулировать следующим образом:

Теорема 14. *Пусть G есть либо $\mathbf{SL}_n$ $(n \geqslant 3)$, либо $\mathbf{Sp}_{2n}$ $(n \geqslant 2)$ над полем алгебраических чисел K. Тогда для $S = V_\infty^K$ имеем*

$$C^S(G) = \begin{cases} 1, & \text{если } K \text{ не является вполне мнимым,} \\ E(K) & \text{в противном случае,} \end{cases} \tag{5}$$

где $E(K)$ — группа всех корней из единицы в K.

Таким образом, для рассматриваемых групп конгруэнц-ядро конечно. С другой стороны, можно показать, что для группы $SL_2(\mathbb{Z})$ оно является свободной проконечной группой счетного ранга (см. Мельников [1]).

Развивая методы работы Басса — Милнора — Серра [1], Мацумото [2] получил аналогичное вычисление конгруэнц-ядра для универсальных групп Шевалле ранга $\geqslant 2$. В оставшемся случае $G = SL_2$ сначала Меннике [2] положительно решил конгруэнц-проблему (3) для группы $SL_2(\mathbb{Z}[1/p])$, а затем Серр [6] рассмотрел общую ситуацию, показав, что при $|S| > 1$ конгруэнц-ядро $C^S(G)$ тривиально, если S не является вполне мнимым, и изоморфно $E(K)$ в противном случае (ср. (10) ниже). Анализируя полученные к тому времени результаты, Серр [6] сформулировал следующую конгруэнц-гипотезу:

пусть G — простая односвязная алгебраическая K-группа;

$$\text{тогда конгруэнц-ядро } C^S(G) \text{ конечно, если } \operatorname{rang}_S G = \sum_{v \in S} \operatorname{rang}_{K_v} G \geqslant 2 \text{ и } \operatorname{rang}_{K_v} G \geqslant 1 \tag{6}$$

*для $v \in S \setminus V_\infty^K$ *), и бесконечно, если $\operatorname{rang}_S G = 1$.*

(Читателю может показаться странным, что определяя конгруэнц-ядро $C^S(G)$ для произвольных алгебраических групп, мы ведем речь о его вычислении только для простых односвязных групп. В действительности это не ограничивает общности, ибо можно показать (см. Платонов [6], Платонов, Шаромет [1]), что вычисление $C^S(G)$ сводится к полупростому случаю, а для полупростой неодносвязной K-группы G такой, что односвязная

---

*) Заметим, что условие $\operatorname{rang}_{K_v} G \geqslant 1$ для $v \in S \setminus V_\infty^K$ отсутствовало у Серра, но как мы видели выше, оно необходимо.

накрывающая $\tilde{G}$ обладает сильной аппроксимацией относительно S, конгруэнц-ядро $C^S(G)$ всегда бесконечно (см. Серр [2], Платонов [20]).)

Нас будет интересовать, в основном, первая часть конгруэнц-гипотезы, относящаяся к конечности $C^S(G)$, и сейчас мы изложим схему рассуждений, которая применялась во всех работах по этому вопросу.

По определению конгруэнц-ядро $C = C^S(G)$ входит в точную последовательность

$$1 \to C \to \hat{G} \to \bar{G} \to 1. \tag{7}$$

Рассмотрим отвечающий (7) начальный отрезок спектральной когомологической последовательности Хохшильда — Серра

$$H^1(\bar{G}) \xrightarrow{\varphi} H^1(\hat{G}) \to H^1(C)^{\bar{G}} \xrightarrow{\psi} H^2(\bar{G}), \tag{8}$$

где $H^i(*)$ обозначает i-ю группу непрерывных когомологий с коэффициентами в одномерном торе $\mathbb{R}/\mathbb{Z}$. Легко видеть, что

$$\operatorname{Coker}\varphi = [\overline{G_K, G_K}]/[G_K, G_K],$$

где черта означает замыкание в G_K относительно S-арифметической топологии. Далее замечается, что S-конгруэнц-топология на G_K совпадает с индуцированной топологией при вложении $G_K \hookrightarrow G_{A_S}$ в группу S-аделей. Поэтому если предположить, что начиная с этого места мы находимся в условиях конгруэнц-гипотезы, то из сильной аппроксимационной теоремы вытекает, что группу $\bar{G}$ можно отождествить с G_{A_S}. С другой стороны, по построению группа G_K вкладывается как в $\bar{G}$, так и в $\hat{G}$, т. е. последовательность (7) расщепляется над G_K и в действительности является «универсальной» последовательностью с этим свойством (см. Прасад, Рагунатан [2]). Отсюда следует, что

$$\operatorname{Im}\psi = M(G, S),$$

где $M(G, S) = \operatorname{Ker}(H^2(G_{A_S}) \to H^2(G_K))$ — так называемое *метаплектическое ядро* (группа G_K считается наделенной дискретной топологией). Таким образом, из (8) получаем следующую точную последовательность:

$$1 \to \operatorname{Coker}\varphi \to H^1(C)^{\bar{G}} \to M(G, S) \to 1. \tag{9}$$

К сожалению, член $H^1(C)^{\bar{G}}$ в общем случае несет информацию только о части конгруэнц-ядра C. Полностью восстановить C по $H^1(C)^{\bar{G}}$ можно лишь в том случае, когда C центрально, т. е. лежит в центре группы $\hat{G}$, ибо тогда $H^1(C)^{\bar{G}} = H^1(C)$ совпадает с группой C^*, двойственной по Понтрягину к C.

Теорема 15. *Если конгруэнц-ядро C центрально, то оно конечно. Кроме того, если* $\operatorname{Coker}\varphi = 1$, *то* $C^* = M(G, S)$.

В самом деле, метаплектическое ядро $M(G, S)$ всегда конечно (см. Рагунатан [4], Прасад, Рагунатан [2]). С другой стороны, в силу теоремы 8 коммутант $[G_K, G_K]$ имеет конечный индекс в G_K; в частности, $\operatorname{Coker}\varphi$ также конечно. Поэтому утверждение о конечности C вытекает из точной последовательности (9) и последующих замечаний. Второе утверждение теоремы очевидно.

Следует отметить, что конечность C фактически эквивалентна его центральности. Более точно, если C конечно, а группа G_K проективно проста, то C центрально. Таким образом, качественный аспект определения C (т. е. доказательство его конечности) сводится к доказательству его центральности.

Следующий этап исследований, естественно, связан с получением точных вычислений для C. Для этого прежде всего надо выяснить, тривиально $\operatorname{Coker}\varphi$ или нет. Ясно, что $\operatorname{Coker}\varphi = 1$, если группа G_K не имеет собственных нецентральных нормальных делителей. Поэтому, в силу результатов § 9.1, $\operatorname{Coker}\varphi = 1$, если группа G либо K-изотропна и не является группой типа ${}^2E_6$, либо принадлежит к одному из типов B_l $(l \geqslant 2)$, C_l $(l \geqslant 2)$, D_l $(l \geqslant 4$, кроме ${}^3D_4$, ${}^6D_4)$, E_7, E_8, F_4, G_2 или является специальной унитарной группой $\boldsymbol{SU}_m(L, f)$ $(m \geqslant 3)$ невырожденной эрмитовой формы f над квадратичным расширением L/K. Пусть теперь G является K-анизотропной внутренней формой типа A_n, $T = \{v \in V_f^K \mid G \quad K_v\text{-анизотропна}\}$. Из условия конгруэнц-гипотезы вытекает, что $S \cap T = \varnothing$, так что в силу теоремы 4 коммутант $[G_K, G_K]$ замкнут в S-арифметической топологии, и опять $\operatorname{Coker}\varphi = 1$. Таким образом, тривиальность $\operatorname{Coker}\varphi$ не установлена лишь для некоторых форм типов ${}^2A_n$, ${}^3D_4$, ${}^6D_4$ и E_6, т. е. в большинстве случаев вычисление C (в случае его центральности) сводится к вычислению метаплектического ядра $M(G, S)$.

В основополагающих работах Мура [1] и Мацумото [1] содержится вычисление $M(G, S)$ для групп Шевалле. Их результат напоминает (5) и выглядит следующим образом.

Теорема 16. *Пусть G — простая односвязная K-разложимая группа, $S \subset V^K$ — конечное подмножество, содержащее V_∞^K. Тогда*

$$M(G, S) = \begin{cases} 1, & \text{если } \exists v \in S \mid K_v \neq \mathbb{C}, \\ E(K) & \text{в противном случае.} \end{cases} \tag{10}$$

Случай квазиразложимых групп был рассмотрен Деодером [1].

В целом период активных исследований в этой области конца 60-х годов сменился более чем десятилетним периодом забвения. Возрождение этой тематики относится уже к 80-м годам, когда Прасад и Рагунатан [2], [3] (для классических групп см. также Бак, Рехман [1], [2]) вычислили $M(G, S)$ для всех K-изотропных групп.

Теорема 17. *Пусть G — простая односвязная K-изотропная группа. Тогда*

$$M(G, S) = \begin{cases} 1, & \text{если } S \neq V_\infty^K, \\ \subset E(K) & \text{в противном случае.} \end{cases}$$

Доказательство Прасада и Рагунатана основано на использовании некоторых K-определенных подгрупп в G типа $\boldsymbol{SL}_2$, которые строятся, исходя из предположения о K-изотропности G. По этой причине их рассуждения не переносятся в K-анизотропную ситуацию, исследование которой, выполненное Рапинчуком [3—4, 6], потребовало привлечения иных средств. К сожалению, результаты здесь пока не обрели унифицированную форму типа теоремы 17, и их приходится формулировать отдельно для разных типов групп.

Внутренние формы типа $\boldsymbol{A}_{n-1}$. Здесь $G = \boldsymbol{SL}_1(D)$, где D — тело индекса n над K. Положим $S_e = \{v \in V^K \setminus S \mid D \otimes_K K_v \simeq M_2(F_v),\ F_v$ — алгебра с делением над $K_v\}$ и $s = [S_e]$ (число s — конечно, если $n > 2$, и бесконечно, если $n = 2$).

Теорема 18. *Предположим, что S содержит неархимедово нормирование v_0 такое, что $D \otimes_K K_{v_0} \simeq M_n(K_{v_0})$. Тогда $M(G, S)$ является конечной подгруппой группы $B(D, S) = (\mathbb{Z}/2\mathbb{Z})^s$. В общем случае $M(G, S)$ изоморфно конечной подгруппе расширения группы $B(D, S)$ при помощи группы $E(K)$ всех корней из единицы в K.*

Следствие. *Если $S_e = \varnothing$, в частности, если n нечетно, то*

$$M(G, S) = \begin{cases} 1, & \text{если } \exists v_0 \in S \mid K_{v_0} \neq \mathbb{C} \text{ и } D_{v_0} \simeq M_n(K_{v_0}), \\ \subset E(K) & \text{в противном случае.} \end{cases}$$

(Последний результат фактически аналогичен классическому результату (10).)

Доказательство теоремы получается путем редукций к исследованию законов взаимности на максимальных K-торах группы G. Редукционная часть рассуждений в общих чертах аналогична классическим рассуждениям Мацумото [2] с той лишь разницей, что при работе с анизотропными группами, естественно, появляются анизотропные торы. Затем возникающие законы взаимности исследуются средствами алгебраической теории чисел. (Отметим, что аналогичные результаты о законах взаимности были получены независимо, но несколько позже Прасадом [3].)

Внешние формы типа $\boldsymbol{A}_{n-1}$. Это специальные унитарные группы $G = \boldsymbol{SU}_m(D, f)$, где D — конечномерное тело с инволюцией σ второго рода, причем поле неподвижных относительно σ элементов центра D совпадает с K, f — невырожденная σ-эрмитова форма степени m над D (см. § 2.3).

Теорема 19. *Пусть $G = \boldsymbol{SU}_m(D, f)$ и $m \geqslant 3$. Если S содержит неархимедово нормирование, то $M(G, S)$ имеет экспоненту,*

не превосходящую 2. В общем случае $M(G, S)$ является конечной группой, представимой в виде расширения группы экспоненты $\leqslant 2$, при помощи подгруппы группы $E(K)$.

Доказательство использует теорему 18, свойства эрмитовых форм и локальные вычисления Прасада — Рагунатана [2].

Остальные классические типы. Используя теорему 18 и геометрическую реализацию групп классических типов, можно получить следующую теорему:

Теорема 20. *Пусть G — простая односвязная K-группа одного из следующих типов: B_n $(n \geqslant 2)$, C_n $(n \geqslant 2)$, D_n $(n \geqslant 5)$. Предположим, что S содержит неархимедово нормирование v_0 и что выполняются следующие условия:*

1) *если G принадлежит типу B_n, то либо $n \geqslant 3$, либо $n = 2$ и G является K_{v_0}-разложимой;*

2) *если G принадлежит типу C_n, то G является K_{v_0}-разложимой.*

Тогда $M(G, S)$ имеет экспоненту $\leqslant 2$. В общем случае $M(G, S)$ является конечной группой, которая представима в виде расширения группы экспоненты $\leqslant 2$ при помощи подгруппы группы $E(K)$.

Исключительные типы.

Теорема 21. *Пусть G — простая K-группа одного из следующих типов: E_8, F_4, G_2. Тогда $M(G, S)$ тривиально, если S содержит неархимедово нормирование, и изоморфно подгруппе $E(K)$ в противном случае.*

Для групп типа E_7 получается результат, аналогичный теореме 20. Таким образом, остается исследовать метаплектическое ядро для некоторых групп типов ${}^2A_n$, D_4 и E_6.

Мы не имеем здесь возможности более подробно останавливаться на основных моментах доказательства теорем 18—21, из которых наиболее фундаментальной является теорема 18, а приведем лишь доказательство так называемой *слабой метаплектической гипотезы* (см. теорему 12), которую мы использовали при выводе теоремы 3 и которая в действительности является одной из составляющих доказательства теоремы 18.

Доказательство теоремы 12. Пусть $G = \mathbf{SL}_1(D)$, где D — тело индекса $n > 2$ над K, $T = \{v \in V_f^K \mid D_v$ — тело$\}$. Нам надо показать, что отображение ограничения θ: $H^2(G_T) \to H^2(G_K)$ инъективно. (Здесь и ниже рассматриваются непрерывные когомологии с коэффициентами в тривиальном дискретном модуле $J = \mathbb{Q}/\mathbb{Z}$. Можно, однако, показать, что в нашей ситуации те же результаты получаются, если модуль коэффициентов J заменить на одномерный тор $\mathbb{R}/\mathbb{Z}$.) Для этого рассмотрим такое максимальное подполе $L \subset D$, что все локальные расширения L_v/K_v неразветвлены для $v \in T$, и пусть $F = \mathbf{R}^{(1)}_{L/K}(\mathbf{G}_m)$ — соответствующий максимальный K-тор группы G. Мы покажем, что

уже отображение μ: $H^2(G_T) \to H^2(F_K)$ инъективно. Очевидно, μ раскладывается в композицию двух отображений ограничения

$$H^2(G_T) \xrightarrow{\zeta} H^2(F_T) \xrightarrow{\eta} H^2(F_K),$$

и достаточно установить инъективность каждого из них.

Лемма 24. *Отображение η инъективно.*

Доказательство. В силу п. 1, § 1.3 каждому коциклу $\alpha \in H^2(H)$ отвечает центральное расширение

$$1 \to J \to E \xrightarrow{\rho} H \to 1, \tag{11}$$

с которым для любых двух перестановочных подгрупп $A, B \subset H$ можно связать бимультипликативное отображение $\delta: A \times B \to J$, $\delta(a, b) = [\tilde{a}, \tilde{b}] = \tilde{a}\tilde{b}\tilde{a}^{-1}\tilde{b}^{-1}$, где $\tilde{a} \in \rho^{-1}(a)$, $\tilde{b} \in \rho^{-1}(b)$. При этом если H — топологическая группа и коцикл α непрерывен, то расширение (11) также является топологическим, а функция δ — непрерывной. После этих предварительных замечаний перейдем непосредственно к доказательству инъективности η.

Пусть $\alpha \in \operatorname{Ker} \eta$ и

$$1 \to J \to E \xrightarrow{\rho} F_T \to 1 \tag{12}$$

— отвечающее α центральное расширение. Коцикл α тривиален в том и только том случае, если это расширение тривиально (т. е. расщепляется), а последнее в силу абелевости F_T и делимости J эквивалентно абелевости E (лемма 1.1). Чтобы установить абелевость E, рассмотрим определенное выше бимультипликативное отображение δ: $F_T \times F_T \to J$ и покажем, что оно тривиально. Условие $\alpha \in \operatorname{Ker} \eta$ сводится к тому, что расширение (12) расщепляется над F_K, т. е. существует сечение φ: $F_K \to E$ гомоморфизма ρ. Отсюда без труда следует, что ограничение $\delta|_{F_K \times F_K}$ тривиально. Но из предложения 7.8 вытекает плотность F_K в F_T, поэтому из соображений непрерывности получаем, что δ также тривиально. Лемма 24 доказана.

Лемма 25. *ζ инъективно.*

Доказательство легко получается из следующего результата Прасада и Рагунатана [4].

Теорема 22. *Для каждого $v \in T$ отображение $H^2(G_{K_v}) \to H^2(F_{K_v})$ инъективно.*

Пусть $\alpha \in \operatorname{Ker} \zeta$ и

$$1 \to J \to E \xrightarrow{\rho} G_T \to 1 \tag{13}$$

— соответствующее центральное расширение. Легко видеть, что для каждого $v \in T$ коцикл α_v, отвечающий индуцированному расширению

$$1 \to J \to \rho^{-1}(G_{K_v}) \to G_{K_v} \to 1, \tag{14}$$

лежит в ядре отображения $H^2(G_{K_v}) \to H^2(F_{K_v})$ и поэтому в силу теоремы 22 тривиален, т. е. последовательность (14) расщепляется. Другими словами, для каждого $v \in T$ существует непрерывный гомоморфизм φ_v: $G_{K_v} \to E$, являющийся сечением ρ над группой G_{K_v}. Для того чтобы произведение $\varphi = \prod_{v \in T} \varphi_v$ доставляло сечение ρ над всей группой G_T, необходимо и достаточно, чтобы подгруппы $\rho^{-1}(G_{K_v})$ $(v \in T)$ в E были попарно перестановочны. Пусть v_1, $v_2 \in T$ и δ: $G_{K_{v_1}} \times G_{K_{v_2}} \to J$ — отвечающее подгруппам $G_{K_{v_1}}$, $G_{K_{v_2}} \subset G_T$ бимультипликативное отображение, определяемое коммутированием. Наша цель — показать, что δ тривиально. В силу бимультипликативности, δ можно рассматривать как отображение $G_{K_{v_1}}/[G_{K_{v_1}}, G_{K_{v_1}}] \times G_{K_{v_2}}/[G_{K_{v_2}}, G_{K_{v_2}}] \to J$. С другой стороны, поскольку $\alpha \in \operatorname{Ker} \xi$, то ограничение δ на $F_{K_{v_1}} \times F_{K_{v_2}}$ тривиально. Поэтому тривиальность δ является следствием соотношения $G_{K_{v_i}} = F_{K_{v_i}}[G_{K_{v_i}}, G_{K_{v_i}}]$, которое вытекает из теоремы 1.8. Тем самым лемма 25, а вместе с тем и теорема 12 доказаны.

Нам осталось убедиться в справедливости теоремы 22. Чтобы не переусложнять обозначений, положим $C = G_{K_v}$, $B = F_{K_v}$, и для каждого $i = 1, 2$, обозначим через C_i конгруэнц-подгруппу $G_{K_v} \cap (1 + \mathfrak{P}_v^i)$, где $\mathfrak{P}_v$ — идеал нормирования в D_v; будем также считать C_0 равным C. Таким образом, наши обозначения будут полностью соответствовать обозначениям п. 4 § 1.4, результаты которого используются в рассуждениях. Доказывать, что отображение ξ: $H^2(C) \to H^2(B)$ инъективно, мы будем следующим образом. Легко видеть, что $H^2(C) = \varinjlim H^2(C/C_i)$, где прямой предел берется относительно естественных гомоморфизмов инфляции $H^2(C/C_i) \to H^2(C/C_j)$ для $i \geqslant j$. Обозначим через $H^2(C)_i$ образ $H^2(C/C_i)$ в $H^2(C)$. Тогда $H^2(C) = \bigcup_i H^2(C)_i$. Так как группа C/C_1 — циклическая (см. предложение 1.8), то $H^2(C/C_1) = 1$. Поэтому для любого нетривиального элемента $\alpha \in H^2(C)$ можно найти такое минимальное число $i \geqslant 2$, что $\alpha \in H^2(C)_i$. Взяв $\alpha \in \operatorname{Ker} \xi$ и выбрав такое минимальное i, мы покажем, что на самом деле $\alpha \in H^2(C)_{i-1}$, откуда $\alpha = 1$. Наметим основную линию рассуждений, оставляя детали читателю в качестве упражнения.

Пусть $r \geqslant 2$, $\alpha \in H^2(C/C_r)$ и

$$1 \to J \to E \to C/C_r \to 1$$

— отвечающее α центральное расширение. Для $s \leqslant r$ положим $E(s) = \rho^{-1}(C_s/C_r)$. Всюду ниже предполагаем выполненным условие теоремы 12 о том, что $n > 2$.

Лемма 26. 1) *$E(2)$ централизует $E(r-1)$.*

2) *α лежит в образе отображения инфляции $H^2(C/C_{r-1}) \to H^2(C/C_r)$ в том и только том случае, если $E(1)$ централизует $E(r-1)$.*

Доказательство легко вытекает из коммутационных соотношений между конгруэнц-подгруппами (см. § 1.4, п. 4) и оставляется читателю.

Нам удобно несколько переформулировать утверждение леммы. Поскольку $E(2)$ действует на $E(r-1)$ тривиально, коммутирование $(x, y) \to [x, y]$ задает корректно определенное отображение

$$\Lambda^\alpha\colon E(1)/E(2) \times E(r-1)/E(r) \to J.$$

Но, очевидно, $E(1)/E(2) = C_1/C_2 = F(1)$, $E(r-1)/E(r) = C_{r-1}/C_r = F(r)$ в обозначениях п. 4 § 1.4 (с. 46). Легко видеть, что Λ^α является биаддитивным отображением, инвариантным относительно естественного действия на $F(1)$ и $F(r)$ группы $\Delta = E/E(1) = C/C_1$. Поскольку экспонента $F(i)$ равна соответствующему v простому числу p, то

$$\operatorname{Im} \Lambda^\alpha \subset \frac{1}{p}\mathbb{Z}/\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z}.$$

Таким образом, Λ^α можно рассматривать как биаддитивное Δ-инвариантное отображение $F(1) \times F(r) \to F_p = \mathbb{Z}/p\mathbb{Z}$. При этом

$$\alpha \in \operatorname{Im}\left(H^2(C/C_{r-1}) \to H^2(C/C_r)\right) \Leftrightarrow \Lambda^\alpha = 0. \tag{15}$$

Отсюда следует, что соответствие $H^2(C/C_r) \to B(F(1), F(r-1))$, $\alpha \mapsto \Lambda^\alpha$ (где $B(F(1), F(r-1))$, как и в § 1.4, обозначает множество биаддитивных Δ-инвариантных отображений $F(1) \times F(r-1) \to F_p$) является гомоморфизмом абелевых групп, ядром которого служит $\operatorname{Im}(H^2(C/C_{r-1}) \to H^2(C/C_r))$. (Отметим, что на самом деле этот гомоморфизм связан с одной из «стрелок» в спектральной последовательности Хохшильда — Серра, отвечающей расширению $1 \to C_{r-1}/C_r \to C/C_r \to C/C_{r-1} \to 1$.) Наряду с отображениями Λ^α нам понадобятся «высшие» биаддитивные Δ-инвариантные отображения Λ_i^α $(i < r)$:

$$\Lambda_i^\alpha\colon F(i) = E(i)/E(i+1) \times E(r-i)/E(r-i+1) = F(r-i) \to \mathbb{Z}/p\mathbb{Z},$$

которые индуцируются коммутированием $(x, y) \to [x, y]$. Для обоснования корректности Λ_i^α нужно показать, что $E(i+1)$ централизует $E(r-i)$ для любого $i = 1, \ldots, r-1$.

Предложение 11. 1) *$E(i+1)$ централизует $E(r-i)$ для любого $i = 1, \ldots, r-1$; тем самым отображения Λ_i^α корректно определены. При этом Λ_i^α являются биаддитивными и Δ-инвариантными.*

2) *Если r кратно n, то для любого $\alpha \in H^2(C/C_r)$ отображение Λ^α задается формулой $\Lambda^\alpha(x, y) = \mathrm{Tr}_{l/F_p}(\lambda^\alpha x\sigma(y))$, где λ^α — подходящий элемент поля вычетов l тела D_v, σ — каноническая образующая группы Галуа $\mathrm{Gal}(l/k_v)$, а группы $F(i)$ отождествляются с подгруппами аддитивной группы поля l* (см. § 1.4, п. 4). *В этом случае $\Lambda_i^\alpha(x, y) = \mathrm{Tr}_{l/F_p}(\lambda_i^\alpha x\sigma^i(y))$, где $\lambda_i^\alpha = \sum_{j=0}^{i-1} \sigma^j(\lambda^\alpha)$.*

Доказательство использует тождество Ф. Холла:

$$[[a, b], {}^b c]\,[[b, c], {}^c a]\,[[c, a], {}^a b] = 1,$$

справедливое для любых элементов a, b, c некоторой группы, где ${}^x y$ обозначает элемент xyx^{-1}. Утверждение 1) будем доказывать индукцией по i. Случай $i = 1$ разобран в лемме 26. Предположим, что перестановочность $E(i)$ и $E(r-i+1)$ уже доказана, и пусть $a \in E(1)$, $b \in E(i)$, $c \in E(r-i)$. Тогда из тождества Холла и предположения индукции вытекает, что

$$[[a, b], {}^b c] = 1,$$

т. е. $[a, b]$ и ${}^b c$ перестановочны. Поскольку ${}^b cc = [b, c] \in E(r-i+1)$, то элементы $[a, b]$ и ${}^b cc$ также перестановочны по предположению индукции, поэтому перестановочны и элементы $[a, b]$ и c. Но из коммутаторных соотношений между конгруэнц-подгруппами (см. § 1.4, п. 4) вытекает, что $[E(1), E(i)] \subset E(i+1)$, следовательно, $E(i+1)$ коммутирует с $E(r-i)$, что и требовалось. Утверждения о биаддитивности и Δ-инвариантности Λ_i^α очевидны.

Пусть теперь r кратно n. Тогда если $F(1)$ является простым Δ-модулем, то при соответствующих отождествлениях отображение Λ^α задается формулой

$$\Lambda^\alpha(x, y) = \mathrm{Tr}_{l/F_p}(\lambda^\alpha x\sigma(y)) \tag{16}$$

для подходящего $\lambda^\alpha \in l$ (теорема 1.11). Немного позже мы покажем, что отображение Λ^α имеет вид (16) всегда, а пока, используя (16), получим формулу для $\Lambda_i^\alpha(x, y)$. Здесь снова проводится индукция по i.

Предположим, что уже установлена формула для Λ_{i-1}^α и докажем ее для Λ_i^α. Рассмотрим произвольные $a \in E(1)$, $b \in E(i-1)$, $c \in E(r-i)$. Тогда, зафиксировав униформизующий элемент $\Pi \in D_v$, будем иметь

$$\rho(a) = 1 + s\Pi,$$
$$\rho(b) = 1 + t\Pi^{i-1},$$
$$\rho(c) = 1 + u\Pi^{r-i}$$

для подходящих s, t, u из кольца целых $\mathcal{O}_{D_v}$. Тогда из леммы 1.8 вытекает, что

$$\begin{aligned}
&\rho([a, b]) = 1 + x\Pi^i, && \text{причем } \bar{x} = \bar{s}\sigma(\bar{t}) - \sigma^{i-1}(\bar{s})\bar{t},\\
&\rho([b, c]) = 1 + y\Pi^{r-1}, && \text{причем } \bar{y} = \bar{t}\sigma^{i-1}(\bar{u}) - \sigma^{r-i}(\bar{t})\bar{u},\\
&\rho([c, a]) = 1 + z\Pi^{r-i+1}, && \text{причем } \bar{z} = \bar{u}\sigma^{r-i}(\bar{s}) - \sigma(\bar{u})\bar{s},
\end{aligned} \tag{17}$$

где черта обозначает вычет соответствующего элемента в l. Учитывая тривиальность действия C_1 на $F(i)$, из тождества Холла получим $\Lambda_i^\alpha(\bar{x}, \bar{u}) = \Lambda_{r-1}^\alpha(\bar{y}, \bar{s}) + \Lambda_{r-i+1}^\alpha(\bar{z}, \bar{t}) = 0$. Далее, из очевидного тождества $[a, b]^{-1} = [b, a]^{-1}$ вытекает, что $\Lambda_i^\alpha(x, y) = -\Lambda_{r-i}^\alpha(y, x)$ для всех $x \in F(i)$, $y \in F(r-i)$, откуда

$$\Lambda_i^\alpha(\bar{x}, \bar{u}) = \Lambda_1^\alpha(\bar{s}, \bar{y}) + \Lambda_{i-1}^\alpha(\bar{t}, \bar{z}). \tag{18}$$

Воспользовавшись теперь предположением индукции, получим

$$\begin{aligned}
\Lambda_i^\alpha(\bar{x}, \bar{u}) &= \mathrm{Tr}_{l/F_p}\left(\lambda^\alpha \bar{s}\sigma(\bar{t}\sigma^{i-1}(\bar{u}) - \sigma^{r-i}(\bar{t})\bar{u}\right) +\\
&+ \mathrm{Tr}_{l/F_p}\left((\lambda^\alpha + \ldots + \sigma^{i-r}(\lambda^\alpha)) \cdot \bar{t}\sigma^{i-1}(\bar{u}\sigma^{r-i}(\bar{s}) - \sigma(\bar{u})\bar{s})\right) =\\
&= \mathrm{Tr}_{l/F_p}\left((\lambda^\alpha + \sigma(\lambda^\alpha) + \ldots + \sigma^{i-1}(\lambda^\alpha))\bar{s}\sigma(\bar{t})\sigma^i(\bar{u})\right) -\\
&- \mathrm{Tr}_{l/F_p}\left((\lambda^\alpha + \sigma(\lambda^\alpha) + \ldots + \sigma^{i-1}(\lambda^\alpha))\sigma^{i-1}(\bar{s})\sigma^r(\bar{t})\sigma^i(\bar{u})\right) =\\
&= \mathrm{Tr}_{l/F_p}\left((\lambda^\alpha + \ldots + \sigma^{i-1}(\lambda^\alpha))(\bar{s}\sigma(\bar{t}) - \sigma^{i-1}(\bar{s})\bar{t})\sigma^i(\bar{u})\right) =\\
&= \mathrm{Tr}_{l/F_p}\left(\lambda_i^\alpha \bar{x}\sigma^i(\bar{u})\right),
\end{aligned}$$

ибо r кратно n.

Таким образом, мы видим, что два биаддитивных отображения $\Lambda_i^\alpha(x, y)$ и $\mathrm{Tr}_{l/F_p}\left(\lambda_i^\alpha x\sigma^i(y)\right)$ совпадают на тех элементах $x \in F(i)$, $y \in F(r-i)$, где x имеет вид $x = s\sigma(t) - \sigma^{i-1}(s)t$ для некоторых $s \in F(1)$, $t \in F(i-1)$. Однако, как мы видели при доказательстве теоремы 1.9, элементы такого вида порождают всю группу $F(i)$, поэтому тождественно

$$\Lambda_i^\alpha(x, y) = \mathrm{Tr}_{l/F_p}\left(\lambda_i^\alpha x\sigma^i(y)\right).$$

Нам осталось показать, что в случае, когда $F(1)$ не является простым Δ-модулем, отображение Λ^α также имеет вид (16). Поскольку $n > 2$, то в силу предложения 1.9 нам надо рассмотреть ситуацию, когда расширение l/k_v есть расширение F_{64}/F_4. Как мы знаем (теорема 1.11), в этом случае можно гарантировать, что

$$\Lambda^\alpha(x, y) = \mathrm{Tr}_{l/F_p}\left(\lambda x\sigma(y) + \mu x\sigma(y)^8\right)$$

для некоторых $\lambda, \mu \in l$, и наша цель — показать, что $\mu = 0$. Из (17), (18) получаем, что для любых $s, t, u \in l$ должно выполняться равенство (заметим, что $r \geqslant n = 3$)

$$\Lambda_2^\alpha(s\sigma(t) - \sigma(s)t, u) = \Lambda_1^\alpha(s, t\sigma(u) - \sigma^{r-2}(t)u) + \\ + \Lambda_1^\alpha(t, u\sigma^{r-2}(s) - \sigma(u)s). \quad (19)$$

Пусть $t = \zeta s$, $\zeta \in k_v$. Тогда из (19) получаем, что

$$0 = \Lambda^\alpha(s, \zeta(s\sigma(u) - \sigma^{r-2}(s)u)) + \Lambda^\alpha(\zeta s, u\sigma^{r-2}(s) - \sigma(u)s) = \\ = \mathrm{Tr}_{l/F_p}(\mu(\zeta + \zeta^8)s\sigma(s\sigma(u) - \sigma^{r-2}(s)u)^8). \quad (20)$$

Лемма 27. *В рассматриваемой ситуации элементы вида* $s\sigma(s\sigma(u) - \sigma^{r-2}(s)u)^8$ $(s, u \in l)$ *порождают* l *как абелеву группу.*

Доказательство оставляется читателю.

Из леммы и равенства (20) вытекает, что $\mu(\zeta + \zeta^8) = 0$, и так как можно выбрать $\zeta \in k_v$ со свойством $\zeta + \zeta^8 \neq 0$ $(k_v = F_4 \not\subset F_8!)$, то $\mu = 0$. Предложение 11 полностью доказано.

Завершим доказательство теоремы 22. Пусть $\beta \in \mathrm{Ker}\,\xi$, где ξ: $H^2(C) \to H^2(B)$ — отображение ограничения и $\beta \neq 0$. Выберем такое минимальное число $r > 1$, что $\beta \in H^2(C)_r$, и пусть $\alpha \in H^2(C/C_r)$ — такой элемент, который при отображении $H^2(C/C_r) \to H^2(C)$ переходит в β. Утверждается, что r кратно n. В самом деле, если r не кратно, то из теоремы 1.11 вытекает, что $B(F(1), F(r-1)) = 0$, и в силу (15) отображение $H^2(C/C_{r-1}) \to H^2(C/C_r)$ сюръективно. Таким образом, из минимальности r вытекает, что r кратно n. Тогда согласно теореме 1.11 соответствующее отображение Λ^α задается формулой

$$\Lambda^\alpha(x, y) = \mathrm{Tr}_{l/F_p}(\lambda^\alpha x\sigma(y)), \quad x \in F(1), \ y \in F(r-1),$$

для некоторого $\lambda^\alpha \in l$. Наша цель — показать, что $\omega = \mathrm{Tr}_{l/k_v}(\lambda^\alpha) = 0$. Заметим, что согласно предложению 11

$$\Lambda_n^\alpha(x, y) = \mathrm{Tr}_{l/F_p}(\omega xy), \quad x \in F(n), \ y \in F(r-n). \quad (21)$$

Далее воспользуемся тем обстоятельством, что β становится тривиальным при ограничении на B. Отсюда следует, что прообраз $\rho^{-1}(BC_r/C_r)$ (где ρ — расширение, отвечающее α) коммутативен. С другой стороны, согласно предложению 1.8 $C_n = (C_n \cap B)C_{n+1}$ и $C_{r-n} = (C_{r-n} \cap B)C_{r-n+1}$. Поэтому из определения Λ_n^α вытекает, что $\Lambda_n^\alpha = 0$. Так как при каноническом отождествлении $F(n)$ и $F(r-n)$ переходят в $l^{(0)} = \{x \in l \mid \mathrm{Tr}_{l/k_v}(x) = 0\}$, то окончательно получаем, что

$$\mathrm{Tr}_{l/F_p}(\omega xy) = 0 \quad \text{для всех} \quad x, y \in l^{(0)}. \quad 22))$$

Но $(l^{(0)})^{\perp} = \{z \in l \mid \mathrm{Tr}_{l/k_v}(zl^{(0)}) = 0\}$ совпадает с k_v, так что из (22) вытекает, что $\omega l^{(0)} \subset k_v$. Последнее невозможно, если $\omega \neq 0$, ибо $\dim_{k_v} l^{(0)} = n - 1 > 1$. Итак,

$$\omega = \mathrm{Tr}_{l/k_v}(\lambda^{\alpha}) = 0.$$

Заключительный этап рассуждений выглядит следующим образом. Мы построим такой $\gamma \in \mathrm{Ker}(H^2(C/C_r) \to H^2(C/C_{r+1}))$, что $\Lambda^{\alpha} = \Lambda^{\gamma}$. Тогда в силу (15) $\alpha - \gamma \in \mathrm{Im}(H^2(C/C_{r-1}) \to H^2(C/C_r))$, и поэтому образ $\alpha - \gamma$ в $H^2(C)$ лежит в $H^2(C)_{r-1}$; с другой стороны, образ $\alpha - \gamma$ в $H^2(C)$ по построению совпадает с образом α, откуда $\beta \in H^2(C)_{r-1}$ — противоречие.

Для построения γ представим λ^{α} в виде $\lambda^{\alpha} = \delta - \sigma\delta$ $(\delta \in l)$, что возможно в силу условия $\mathrm{Tr}_{l/k_v}(\lambda^{\alpha}) = 0$, и определим $\varphi \in \mathrm{Hom}(F(r), F_p)$ формулой $\varphi(x) = \mathrm{Tr}_{l/F_p}(\delta x)$. Используя отождествление $\mathbb{Z}/p\mathbb{Z} \simeq \frac{1}{p}\mathbb{Z}/\mathbb{Z} \subset J$, будем считать, что $\varphi \in \mathrm{Hom}(F(r), J)$. Рассмотрим тривиальное расширение

$$1 \to J \to E' = (C/C_{r+1}) \times J \to C/C_{r+1} \to 1$$

и обозначим через Φ подгруппу в E', состоящую из элементов вида $(g, -\varphi(g))$, где $g \in C_r/C_{r+1}$. Поскольку r кратно n, то C_r/C_{r+1} лежит в центре группы C/C_{r+1}, откуда следует, что подгруппа Φ нормальна в E'. Пусть $\gamma \in H^2(C/C_r)$ — коцикл, отвечающий расширению

$$1 \to J \to E = E'/\Phi \xrightarrow{\varepsilon} C/C_r = C/C_{r+1}/C_r/C_{r+1} \to 1.$$

В силу наших построений $\gamma \in \mathrm{Ker}(H^2(C/C_r) \to H^2(C/C_{r+1}))$, и остается показать, что

$$\Lambda^{\gamma}(x, y) = \mathrm{Tr}_{l/F_p}(\lambda^{\alpha} x\sigma(y)) = \mathrm{Tr}_{l/F_p}((\delta - \sigma\delta)\, x\sigma(y))$$

для всех $x \in F(1)$, $y \in F(r-1)$. Для этого заметим, что коммутатор двух элементов $a \in E(1)$ и $b \in E(r-1)$ можно вычислить следующим образом: взять произвольные прообразы c и d элементов $\varepsilon(a)$ и $\varepsilon(b)$ в группе C/C_{r+1} и рассмотреть коммутатор $[c, d] \in C_r/C_{r+1} = F(r)$; тогда $[a, b] = \varphi([c, d])$. Поэтому из формул коммутирования (см. лемму 1.8) вытекает, что

$$\Lambda^{\gamma}(x, y) = \varphi(x\sigma(y) - \sigma^{r-1}(x)\, y) =$$
$$= \mathrm{Tr}_{l/F_p}(\delta(x\sigma(y) - y\sigma^{r-1}(x))) = \mathrm{Tr}_{l/F_p}((\delta - \sigma\delta)\, x\sigma(y)) = \Lambda^{\alpha}(x, y).$$

Теорема 22 доказана.

Завершая наш обзор исследований по конгруэнц-проблеме, укажем на имеющиеся к настоящему времени результаты о центральности конгруэнц-ядра. Прежде всего центральность конг-

руэнц-ядра может быть установлена путем манипуляций с унипотентными элементами в группе G_K (если они существуют). Эта идея восходит к фундаментальным работам Басса — Милнора — Серра [1], Меннике [1], [2], Мацумото [1] и Серра [6]. Окончательный результат принадлежит Рагунатану [4], [6], который показал, что для простой односвязной K-группы G существование унипотентных элементов в G_K (т. е. K-изотропность G) вместе с условием $\operatorname{rang}_S G \geqslant 2$ действительно обеспечивает центральность конгруэнц-ядра $C^S(G)$. В его рассуждениях наличие унипотентных элементов в G_K играет существенную роль, и поэтому они не могут быть распространены на анизотропные группы. До недавнего времени единственным результатом о центральности $C^S(G)$, в котором допускаются также анизотропные группы, была теорема Кнезера [14], касающаяся спинорных групп квадратичных форм. Оказалось, однако, что рассуждения Кнезера имеют общую природу и применимы к другим группам с удобной геометрической реализацией. Вначале Рагунатан и Томанов рассмотрели случай групп типа C_n, а затем Рапинчук [9] доказал следующую общую теорему:

Теорема 23. *Пусть G — простая односвязная K-группа одного из следующих типов: $B_n (n \geqslant 2)$, $C_n (n \geqslant 2)$, $D_n (n \geqslant 5)$, G_2, либо специальная унитарная группа $\boldsymbol{SU}_m(L, f)$ $(m \geqslant 4)$ невырожденной эрмитовой формы f над квадратичным расширением L поля K, относящаяся к типу ${}^2A_{m-1}$. Тогда, если $\operatorname{rang}_S G \geqslant 2$, то конгруэнц-ядро $C^S(G)$ центрально.*

Доказательство базируется на развитии метода Кнезера [14] и использует технику § 9.3. Рассуждения здесь, как и в § 9.3, имеют общую природу и применимы к другим группам с удобной геометрической реализацией; их схема для групп типа G_2 приведена в работе Рапинчука [8].

Геометрический метод, при помощи которого получена теорема 23, по-видимому, не применим к исключительным группам, ибо эти группы не обладают подходящими геометрическими реализациями. Здесь решение конгрунэц-проблемы было получено при помощи нового подхода, использующего внутреннюю структуру группы.

Теорема 24 (Рапинчук [9]). *Пусть G — простая односвязная K-анизотропная группа одного из следующих типов: E_7, E_8, F_4. Если $\operatorname{rang}_S G \geqslant 2$, то конгруэнц-ядро $C^S(G)$ центрально.*

Доказательство использует тот факт, что группы рассматриваемых типов разложимы над квадратичным расширением поля K (по этой причине среди перечисленных типов отсутствует E_6).

Отметим, что при доказательстве практически всех результатов по конгруэнц-проблеме, в частности, теорем 23 и 24 используется проективная простота группы рациональных точек.

К сожалению, на сегодняшний день мы не имеем никакой информации по конгруэнц-проблеме для анизотропных внутрен-

них форм типа A_n. Уже долгие годы не поддается исследованию даже минимальный случай групп типа A_1, хотя нормальное строение групп рациональных точек здесь известно (теорема 2). В частном случае $G = \boldsymbol{SL}_1(D)$, где D — тело неопределенных кватернионов над $\mathbb{Q}$, $S = \{\infty, p\}$, причем простое число p выбрано таким образом, что поле $\mathbb{Q}_p$ расщепляет D, эта задача принадлежит Ихаре (см. Коуровскую тетрадь, выпуск 1978 г., задача 5.33). Отметим, что результаты Серра [9] позволяют определить точную алгебраическую структуру $G_{\mathbf{Z}(S)}$. Повидимому, основные результаты здесь еще впереди.

ДОПОЛНЕНИЕ

На стадии прохождения корректур представилась возможность написать небольшое дополнение к основному тексту книги с изложением некоторых результатов, появившихся уже после сдачи книги в печать. За это время в арифметической теории алгебраических групп был получен ряд новых важных результатов, однако ограниченность объема дополнения не позволяет нам дать их систематический обзор. В то же время мы сочли неуместным подменять такой обзор простым перечислением фактов, ибо это явилось бы сильным контрастом с основной частью книги. По этой причине мы приняли решение включить в дополнение краткое, но концептуальное изложение двух результатов, которые вплотную примыкают к проблематике книги. Первый из них связан с теоремами конечности некоторого нового типа (§ Д.1), второй — с гипотезой В. П. Платонова об арифметичности (§ Д.2).

§ Д.1. Теоремы конечности для дискретных подгрупп в полупростых группах с ограниченным объемом факторпространства

В § 4.6 мы установили, что для полупростой $\mathbb{Q}$-определенной алгебраической группы G любая арифметическая подгруппа $\Gamma \subset G_{\mathbb{R}}$ является решеткой, т. е. дискретной подгруппой с конечным объемом факторпространства $G_{\mathbb{R}}/\Gamma$. Точная величина объема $G_{\mathbb{R}}/\Gamma$ была вычислена нами только для случая группы $G = \boldsymbol{SL}_2$. До недавнего времени такие вычисления имелись лишь для разложимых (Лэнглэндс [1]) и квазиразложимых (Лэй [2]) групп. Не было также ответа на ряд естественных качественных вопросов, связанных с объемом $G_{\mathbb{R}}/\Gamma$, в частности, на вопрос о том, может ли этот объем быть произвольно малым. Решение многих из этих вопросов содержится в глубоких работах Бореля — Прасада [1] и Прасада [4], о которых пойдет речь в настоящем параграфе.

Уже довольно давно было известно*), что в случае простой $\mathbb{R}$-определенной группы G с условием $\operatorname{rang}_{\mathbb{R}} G > 1$ существует лишь конечное число классов сопряженности таких решеток $\Gamma \subset G_{\mathbb{R}}$, что объем факторпространства $G_{\mathbb{R}}/\Gamma$ относительно фиксированной меры Хаара на группе $G_{\mathbb{R}}$ ограничен некоторой константой. Впоследствии Титс поставил вопрос о справедливости аналогичного результата для решеток Γ в группах G_K точек простых алгебраических групп G над неархимедовыми локальными полями K, причем в его постановке фиксировалась только константа, ограничивающая объем факторпространства G_K/Γ, но допускалась вариация поля K и K-группы G (при

*) См. Wang H. C. Topics on totally discontinuous groups//Symmetric spaces. — New York: Marcel Dekker, 1972. P. 460—472.

некотором «универсальном» определении меры Хаара на G_K). Ясно, что в такой постановке этот вопрос приобретает новый смысл и для решеток в вещественных группах, а также обобщается на решетки в произведениях вещественных и p-адических групп (в частности, на S-арифметические подгруппы, см. § 5.4). Исследованию этой проблемы для S-арифметических подгрупп и посвящена работа Бореля — Прасада [1]. Прежде чем формулировать ее основные результаты, введем некоторые обозначения.

Пусть G — простая односвязная алгебраическая группа над числовым полем K, G' — некоторая группа, изогенная G над K. Для $v \in V^K$ обозначим через μ'_v меру Хаара на группе G'_{K_v} (см. § 3.5), которая нормализуется следующим образом. При $v \in V_f^K$ мы должны иметь $\mu'_v(I_v) = 1$, где I_v — подгруппа Ивахори в G'_{K_v} (см. § 3.4). Для $v \in V_\infty^K$ рассмотрим группу $H = \mathbf{R}_{K_v/\mathbb{R}}(G')$. Тогда $G'_{K_v} \simeq H_\mathbb{R}$, и достаточно определить меру μ'_v на $H_\mathbb{R}$. Пусть H_0 — такая $\mathbb{C}/\mathbb{R}$-форма группы H, что группа $H_{0\mathbb{R}}$ компактна (она всегда существует). Поскольку алгебра Ли $L(H) \simeq \simeq L(H_0)$, то любой инвариантной дифференциальной форме степени $n = \dim H$ на H отвечает аналогичная форма на H_0, и поэтому любой мере Хаара на $H_\mathbb{R}$ отвечает мера Хаара на $H_{0\mathbb{R}}$ (см. § 3.5). Тогда мера μ'_v нормализуется таким образом, чтобы объем $H_{0\mathbb{R}}$ относительно соответствующей меры равнялся 1. Для любого конечного подмножества $S \subset V^K$, содержащего V_∞^K, обозначим через μ'_S меру Хаара на группе G'_S, которая является произведением мер μ'_v, $v \in S$. В этих обозначениях имеет место

Теорема Д.1. *Зафиксируем константу $c > 0$. Имеется лишь конечное число таких возможностей для выбора числового поля K, конечного подмножества $S \subset V^K$, содержащего V_∞^K, и (с точностью до K-изоморфизма) K-группы G' абсолютного ранга $\geqslant 2$, что существует S-арифметическая подгруппа $\Gamma' \subset \subset G'_S$, для которой $\mu'_S(G'_S/\Gamma') \leqslant c$. При этом число классов сопряженности таких Γ' в G'_S также конечно.*

Теорема Д.1 представляет собой теорему конечности принципиально нового типа. Действительно, все варианты теорем конечности, рассмотренные в книге, утверждают конечность некоторых множеств ($H^1(K, G)$, Ш(G), $G_{A(\infty)}\backslash G_A/G_K$ и т. д.), связанных с индивидуальной алгебраической группой G. Здесь же мы имеем конечность некоторого класса объектов (S-арифметических подгрупп с ограниченным объемом факторпространства) в произвольных простых группах ранга $\geqslant 2$. Другими словами, доказывается не только конечность числа классов сопряженности таких подгрупп в каждой отдельной группе,

но и их отсутствие во всех группах за исключением конечного числа.

Методы, развитые для доказательства теоремы Д.1, позволяют также получить один интересный результат о равномерном росте чисел классов простых односвязных алгебраических групп компактного типа. Для его точной формулировки условимся о некоторых обозначениях. Пусть $S \subset V^K$ — конечное подмножество, содержащее V^K_∞, и для каждого $v \in V^K \setminus S$ задана парахорическая подгруппа $P_v \subset G_{K_v}$. Тогда набор $P = (P_v)_{v \in V^K \setminus S}$ называется *согласованным*, если $P_v = G_{\mathcal{C}_v}$ для почти всех $v \in V^K \setminus S$. В этом случае подгруппа $U(S, P) = G_S \times \prod_{v \in V^K \setminus S} P_v$ является открытой в G_A. Предположим теперь, что $S = V^K_\infty$ и для согласованного набора $P = (P_v)_{v \in V^K_f}$ будем писать $U(P)$ вместо $U(V^K_\infty, P)$. Тогда из теоремы 5.1 вытекает конечность числа двойных смежных классов $U(P) \backslash G_A / G_K$, которое мы обозначим через $c(P)$.

Теорема Д.2. *Зафиксируем константу $C > 0$. Существует лишь конечное число таких числовых полей K, простых односвязных K-групп G компактного типа и классов сопряженности относительно группы G_{A_f} согласованных семейств $P = (P_v)_{v \in V^K_f}$ парахорических подгрупп, что $c(P) \leqslant C$.*

Отметим, что для произвольной решетки L, задающей реализацию группы G, найдется такой согласованный набор P парахорических подгрупп, что $G^L_{A(\infty)} \subset U(P)$. Тогда $\mathrm{cl}(G^L) \geqslant c(P)$, и поэтому из теоремы Д.2 вытекает

Следствие. *Для любого $C > 0$ существует конечное число таких пар (G_i, L_i), $i = 1, \ldots, d$, состоящих из простой односвязной алгебраической группы $G_i \subset \boldsymbol{GL}_{n_i}$, определенной над числовым полем K_i, и решетки $L_i \subset K_i^{n_i}$, что выполняется следующее утверждение: если $G \subset \boldsymbol{GL}_n$ — простая односвязная алгебраическая группа компактного типа над некоторым числовым полем K и $L \subset K^n$ — такая решетка, что $\mathrm{cl}(G^L) \leqslant C$, то для подходящего $i \in \{1, \ldots, d\}$ имеем $K = K_i$, $G \simeq G_i$ над K и группа $G^L_{A(\infty)}$ изоморфна подгруппе, сопряженной в G_{iA} с подгруппой $G^{L_i}_{iA(\infty)}$.*

Другими словами, имеется лишь конечное число простых односвязных групп компактного типа, имеющих реализации с ограниченным числом классов, и для каждой группы имеется лишь конечное число таких существенно различных реализаций. Тем самым теорема Д.2 устанавливает существование некоторой системы табу внутреннего характера, которые «запрещают» почти всем простым односвязным группам компактного типа

иметь реализации с малым числом классов (в частности одноклассные, ср. с теоремой 8.4). Было бы интересно выявить чисто арифметический механизм этого явления. Кроме того, хотелось бы иметь теорему, аналогичную теореме Д.2, для всех полупростых групп, а не только для простых и односвязных. В связи с этим укажем, что для ортогональных групп положительно определенных квадратичных форм вопрос об одноклассных реализациях решает следующая теорема Пфейфера *): одноклассные положительно определенные квадратичные формы от трех и более переменных существуют лишь над конечным числом полей алгебраических чисел; при этом над каждым полем K имеется только конечное число классов эквивалентности таких форм f, для которых идеал $\mathfrak{d}(f)$ имеет ограниченную норму (здесь $\mathfrak{d}(f)$ — идеал в кольце целых $\mathcal{O}_K$ поля K, порожденный значениями соответствующей билинейной формы на решетке $\mathcal{O}_K^n$; в частности, условие $\mathfrak{d}(f)=\mathcal{O}_K$ выделяет примитивные формы).

Остановимся кратко на основных узловых моментах доказательства теорем Д.1 и Д.2. Одним из таких моментов является формула Прасада [4] для вычисления объема $\mu_S(G_S/\Gamma)$, где Γ — так называемая главная S-арифметическая подгруппа, т. е. подгруппа вида $\Gamma=G_K\cap\left(\prod_{v\in V^K\setminus S}P_v\right)$, где $(P_v)_{v\in V^K\setminus S}$ — некоторый согласованный набор парахорических подгрупп. Приведем общий вид этой формулы, опуская определение некоторых явно указываемых констант. Пусть L — минимальное расширение поля K, над которым G становится внутренней формой, если тип G отличен от ${}^6D_4$, и подполе степени 3 над K в таком расширении, если G — группа типа ${}^6D_4$. Пусть также $m_1\leqslant\ldots\leqslant m_r$ — показатели системы корней группы G (см. Бурбаки [4], гл. VI, § 1, n° 11).

Теорема Д.3. *Имеет место формула*

$$\mu_S(G_S/\Gamma)=D_K^{\frac{1}{2}\dim G}\left(D_L/D_K^{[L:K]}\right)^{\frac{1}{2}s}\left(\prod_{i=1}^{r}\frac{m_i!}{(2\pi)^{m_i+1}}\right)^{[K:\mathbb{Q}]}\tau(G)\varepsilon,$$

где D_K (соответственно D_L) — дискриминант поля K (соответственно L), s — некоторая константа, зависящая только от внутреннего типа группы G, $\tau(G)$ — число Тамагавы группы G, ε — некоторая константа, зависящая от набора парахорических подгрупп $(P_v)_{v\in V^K\setminus S}$.

Далее используется тот факт, что в действительности $\tau(G)=1$ (см. с. 294), и поэтому этот множитель может быть опу-

*) Pfeuffer H. Einklassige Geschlechter totalpositiver quadratischer Formen in totalreelen algebraischen Zahlkörpern//J. Number Theory. 1971. V. 3. P. 371—411.

щен. Анализируя формулу из теоремы Д.3 с помощью различных теоретико-числовых оценок, в частности, оценок для дискриминантов числовых полей, Борель и Прасад получают конечность числа таких троек (K, S, G), что для подходящей группы G', изогенной G над K, существует S-арифметическая подгруппа $\Gamma' \subset G'_S$, для которой $\mu'_S(G'_S/\Gamma') \leqslant c$. Заключительный этап доказательства теоремы Д.1 связан с обоснованием конечности числа классов сопряженности S-арифметических подгрупп с ограниченным объемом факторпространства для фиксированной группы. Здесь используются теоремы конечности для когомологий Галуа и оценки индексов S-арифметических подгрупп в своих нормализаторах, которые получаются из подходящего обобщения результатов Рольфса [3].

Отметим, что большинство результатов этого параграфа при некоторых незначительных ограничениях сохраняет силу и для групп над глобальными полями положительной характеристики.

§ Д.2. Представления групп конечной ширины

Пусть Γ — абстрактная группа с конечным числом образующих. В этом параграфе мы будем рассматривать представления Γ исключительно над полями нулевой характеристики, причем в большинстве случаев основным полем будет поле $\mathbb{C}$ комплексных чисел. Обозначим через $R_n(\Gamma)$ и $\mathbf{X}_n(\Gamma)$ многообразия n-мерных представлений Γ и их характеров. В § 7.5 мы уже обсуждали группы так называемого конечного представленческого типа, т. е. группы, удовлетворяющие условию

$$\dim \mathbf{X}_n(\Gamma) = 0 \quad \text{для всех } n \geqslant 1. \tag{1}$$

В настоящее время основные усилия по изучению таких групп направлены на доказательство гипотезы об арифметичности, выдвинутой первым из авторов (см. с. 477). К сожалению, продвижения в этом направлении пока не слишком значительны. Тем не менее все известные примеры групп, удовлетворяющих (1), действительно получаются из S-арифметических групп. Но даже для этих групп проверка условия (1) отнюдь не является тривиальной, а использует либо положительное решение конгруэнц-проблемы, либо результаты Маргулиса [6] о супержесткости. Однако оба этих метода не позволяют раскрыть связь условия (1) со структурными свойствами группы Γ. С другой стороны, ясно, что без выявления такой связи далеко продвинуться в анализе групп конечного представленческого типа нельзя. Один пример «структурного» подхода к проверке условия (1) мы уже привели в § 7.5, а именно, там мы показали, что условие (1) для группы $\Gamma = SL_n(\mathbb{Z})$ $(n \geqslant 3)$ выводится из ограниченной порождаемости группы Γ

относительно множества элементарных матриц (см. предложение 7.14). Недавно вторым автором *) была получена абстрактная версия этого результата, а именно, показано, что (1) выводится из такого чисто комбинаторного свойства Г, как конечность ширины.

Напомним, что группа Г называется группой конечной (или ограниченной) ширины, не превосходящей t, если существуют такие элементы $\gamma_1, \ldots, \gamma_t \in \Gamma$, что $\Gamma = \langle\gamma_1\rangle \ldots \langle\gamma_t\rangle$, где $\langle\gamma_i\rangle$ — порожденная элементом γ_i циклическая подгруппа. Введем также следующее условие:

$$\text{для любой подгруппы } \Gamma_1 \subset \Gamma \text{ конечного индекса группа } \Gamma_1^{ab} = \Gamma_1/[\Gamma_1, \Gamma_1] \text{ конечна.} \tag{2}$$

Теорема Д.4. *Пусть* Γ — *группа конечной ширины, удовлетворяющая условию* (2). *Тогда* $\dim \mathbf{X}_n(\Gamma) = 0$ *для всех* $n \geqslant 1$.

Отметим, что условие (2) является необходимым для выполнения (1). Укажем также на ряд следствий из теоремы Д.4.

Следствие 1. *Пусть* $\Gamma \subset GL_n(\mathbb{C})$ — *вполне приводимая подгруппа конечной ширины, удовлетворяющая условию* (2). *Тогда существует такой элемент* $g \in GL_n(\mathbb{C})$, *что* $g\Gamma g^{-1} \subset GL_n(K)$, *где* K — *подходящее поле алгебраических чисел.*

Следствие 2. *Пусть* $G \subset GL_n(\mathbb{C})$ — *простая* $\mathbb{R}$-*определенная алгебраическая группа. Если* $\operatorname{rang}_{\mathbb{R}} G \geqslant 2$ *и* $\Gamma \subset G_{\mathbb{R}}$ — *решетка, имеющая конечную ширину как абстрактная группа, то существует такая матрица* $g \in GL_n(\mathbb{R})$, *что* $g\Gamma g^{-1} \subset GL_n(K)$, *где* K — *некоторое поле алгебраических чисел.*

Один из ключевых моментов доказательства теоремы Д.4 содержится в следующем утверждении.

Предложение Д.1. *Пусть* Γ — *абстрактная группа конечной ширины* $\leqslant t$. *Тогда для любой подгруппы* $\Gamma_1 \subset \Gamma$ *конечного индекса про-p-пополнение* $\widehat{\Gamma}_1^{(p)}$ *является аналитической про-p-группой* (*т. е. компактной группой Ли над* $\mathbb{Q}_p$) *размерности* $\leqslant t$.

Доказательство получается при помощи одного из критериев аналитичности (см. Лазар [1], с. 206).

Как заметил О. И. Тавгень [3], из предложения Д.1 вытекает, что группа Г конечной ширины является линейной в том и только том случае, если существует подгруппа $\Gamma_1 \subset \Gamma$ конечного индекса, которая для некоторого простого p аппроксимируется конечными p-группами. Таким образом, из справедливости гипотезы В. П. Платонова об арифметичности получалась бы следующая абстрактная характеризация арифметических групп: если группа Г имеет конечную ширину, удовлетворяет

*) Rapinchuk A. S. Combinatorial theory of arithmetic groups//Preprint of the Institute of Mathematics of the Academy of Sciences of BSSR 20(420). Minsk, 1990.

(2) и существует такая подгруппа $\Gamma_1 \subset \Gamma$ конечного индекса, которая для некоторого простого p аппроксимируется конечными p-группами, то Γ — группа арифметического типа.

Из предложения Д.1 вытекает, что для подходящей подгруппы $\Gamma_1 \subset \Gamma$ конечного индекса про-p-пополнение $\hat{\Gamma}_1^{(p)}$ является аналитической про-p-группой максимальной возможной размерности. Тогда соответствующая алгебра Ли $\mathfrak{g}_1$ над $\mathbb{Q}_p$ с точностью до изоморфизма не зависит от выбора подгруппы $\Gamma_1 \subset \Gamma$ с описанными свойствами. Мы будем называть $\mathfrak{g}_1$ p-алгеброй Ли данной группы Γ, $\operatorname{adim}_{\mathbb{Q}_p} \mathfrak{g}_1$ — аналитической p-размерностью Γ и обозначать через $\dim_p \Gamma$. Укажем на следующий интересный вопрос: пусть Γ — линейная группа конечной ширины; верно ли, что для почти всех p число $\dim_p \Gamma$ не зависит от p? Если нет, то может ли образ отображения $p \mapsto \dim_p \Gamma$ (p — простое) быть бесконечным?

Дадим набросок доказательства теоремы Д.4. Как и при доказательстве предложения 7.14, достаточно показать, что для любого представления $\rho\colon \Gamma \to GL_n(\mathbb{C})$ множество следов $X = \{\operatorname{tr} \rho(\gamma) \mid \gamma \in \Gamma\}$ целиком состоит из алгебраических чисел. Оказывается, при этом можно заменять группу Γ на подгруппу конечного индекса.

Лемма Д.1. *Пусть $\Gamma_1 \subset \Gamma$ — подгруппа конечного индекса, $X_1 = \{\operatorname{tr} \rho(\gamma) \mid \gamma \in \Gamma_1\}$. Тогда поле $\mathbb{Q}(X)$ является алгебраическим (и даже конечным) расширением поля $\mathbb{Q}(X_1)$.*

Имеем $\rho(\Gamma) \subset GL_n(A)$, где $A \subset \mathbb{C}$ — некоторое конечно порожденное подкольцо. Далее используется следующее утверждение, доказательство которого базируется на конструкции вложений в локально компактные поля из работы Платонова [10].

Лемма Д.2. *Существует такое бесконечное множество Π простых чисел, что для каждого $p \in \Pi$ имеется бесконечно много вложений $\sigma_1, \sigma_2, \ldots$ кольца A в $\mathbb{Z}_p$, удовлетворяющих следующему свойству: при $i \neq j$ пересечение $\sigma_i(A) \cap \sigma_j(A)$ состоит из алгебраических чисел.*

Беря композицию представления ρ с вложениями σ_i, мы получаем представления $\rho_i\colon \Gamma \to GL_n(\mathbb{Z}_p)$. Пусть $\mathfrak{g}$ — p-алгебра Ли группы Γ. Имеем $\mathfrak{g} = \mathfrak{s} \oplus \mathfrak{r}$, где $\mathfrak{r}$ — радикал $\mathfrak{g}$, а алгебра $\mathfrak{s}$ полупроста. Существует лишь конечное число (скажем, d) неэквивалентных представлений $\tau\colon \mathfrak{s} \to \mathfrak{gl}_n(\mathbb{Q}_p)$. Рассмотрим представления $\rho_1, \ldots, \rho_{d+1}$. Переходя к подгруппе конечного индекса, можно без ограничения общности считать, что образы $\rho_i(\Gamma)$ $(i = 1, \ldots, d+1)$ лежат в конгруэнц-подгруппе $GL_n(\mathbb{Z}_p, p)$, следовательно, ρ_i продолжаются до аналитических представлений $\hat{\rho}_i\colon \hat{\Gamma}^{(p)} \to GL_n(\mathbb{Z}_p)$, и, кроме того, $\hat{\Gamma}^{(p)}$ является полупрямым произведением $S \rtimes R$, где S и R — аналитические про-p-группы с алгебрами Ли $\mathfrak{s}$ и $\mathfrak{r}$

соответственно. Из наших построений вытекает, что для подходящих двух индексов $i, j \in \{1, \ldots, d+1\}$ представления $\hat{\rho}_i$ и $\hat{\rho}_j$ индуцируют эквивалентные представления алгебры Ли $\mathfrak{s}$, поэтому, переходя к подгруппе конечного индекса, можно считать, что ограничения $\hat{\rho}_i|_S$ и $\hat{\rho}_j|_S$ эквивалентны; в частности $\operatorname{tr}\hat{\rho}_i(x) = \operatorname{tr}\hat{\rho}_j(x)$ для всех $x \in S$. С другой стороны, из условия (2) вытекает, что для любого представления $\lambda\colon \Gamma \to GL_n(\mathbb{C})$ разрешимый радикал связной компоненты G^0 алгебраической группы G, получаемой замыканием $\lambda(\Gamma)$, совпадает с ее унипотентным радикалом, поэтому, переходя снова к подгруппе конечного индекса, можно считать, что $\operatorname{tr}\hat{\rho}_k(xy) = \operatorname{tr}\hat{\rho}_k(x)$ для всех $x \in S$, $y \in R$ $(k = i, j)$. Но тогда $\operatorname{tr}\hat{\rho}_i(x) = \operatorname{tr}\hat{\rho}_j(x)$ для всех $x \in \hat{\Gamma}^{(p)}$. В частности, $\sigma_i(\operatorname{tr}\rho(\gamma)) = \sigma_j(\operatorname{tr}\rho(\gamma))$ для любого $\gamma \in \Gamma$. Поэтому из леммы Д.2 вытекает, что $\operatorname{tr}\rho(\gamma)$ — алгебраическое число, что и требовалось.

Теорема Д.4 дает качественное описание совокупности всевозможных представлений группы Γ. Оказывается, что для S-арифметических подгрупп конечной ширины можно дать полное описание самих представлений.

Теорема Д.5. *Пусть G — простая односвязная алгебраическая группа над полем алгебраических чисел K, $S \subset V^K$ — конечное подмножество, содержащее V^K_∞, и $\Gamma \subset G_K$ — плотная по Зарисскому S-арифметическая подгруппа. Предположим, что для G над K выполняется гипотеза 2 из § 9.1. Тогда если Γ имеет конечную ширину, то для любого представления $\rho\colon \Gamma \to GL_n(\mathbb{C})$ существует такой рациональный гомоморфизм $\rho'\colon \mathbf{R}_{K/\mathbb{Q}}(G) \to GL_n(\mathbb{C})$, что ρ и ρ' совпадают на некоторой подгруппе $\Gamma' \subset \Gamma$ конечного индекса.*

Следствие 3. *В условиях теоремы Д.5 Γ не содержит таких нецентральных нормальных делителей N бесконечного индекса, что факторгруппа Γ/N — линейная. В частности, выполняется условие (2).*

Доказательство теоремы Д.5 содержится в указанном препринте А. С. Рапинчука. Там же показано, что для S-арифметической подгруппы Γ свойство конечности ширины связано также с конечностью конгруэнц-ядра $C^S(G)$. В связи с этим естественно сформулировать следующую гипотезу, которая на сегодняшний день представляется одной из наиболее существенных в теории арифметических групп: пусть Γ — S-арифметическая подгруппа простой алгебраической группы G; тогда если $\operatorname{rang}_S G = \sum_{v \in S} \operatorname{rang}_{K_v} G \geqslant 2$, то Γ имеет конечную ширину (ослабленный вариант: проконечное пополнение $\hat{\Gamma}$ имеет конечную ширину как проконечная группа).

СПИСОК ЛИТЕРАТУРЫ

Абельс (Abels H.)

1. Finite presentability of S-arithmetic groups//London Math. Soc. Lect. Notes Ser. 1986. N 121. P. 128—134.
2. Finite presentability of S-arithmetic groups, compact presentability of solvable groups//Lect. notes math. 1987. N 1261. P. 1—176.

Алгебраическая теория чисел/Под ред. Дж. Касселса и А. Фрелиха. — М.: Мир, 1969. (Цитируется как АТЧ.)

Аллан (Allan N. D.)

1. The problem of the maximality of arithmetic groups//Proc. Symp. Pure Math 1966. V. 9. P. 104—109.
2. Maximality of some arithmetic groups//An. Acad. Brasil. Siens. 1966. V. 38, N 2. P. 223—227.
3. Arithmetic subgroups of some classical groups//An. Acad. Brasil. Siens. 1967. V. 39, N 1. P. 15—18.
4. On commensurability class of the Siegal modular group//Bull. Amer. Math. Soc. 1968. V. 74, N 1. P. 115—118.
5. Some non-maximal arithmetic groups//Rev. Colomb. Math. 1968. V. 2. N 1. P. 21—28.
6. On the maximality of $Sp(L)$ in $Sp_n(K)$//Rev. Colomb. Math. 1970. V. 4, N 1. P. 7—15.
7. Maximal open compact subgroup of the projective symplectic group over a locally compact discrete valuation field//Rev. Colomb. Math. 1971. V. 5, N 3. P. 31—58.
8. A note on the arithmetic of the orthogonal groups//Rev. Colomb. Math. 1973. V. 7, N 2. P. 53—66.
9. A note on the arithmetic of the orthogonal groups. II//Port. Math. 1974. V. 33, N 3—4. P. 193—197.

Алберт (Albert A.)

1. Structure of algebras. New York: Amer. Math. Soc. Colloq. Publ. 1939.

Аппельгейт, Ониаши (Appelgate H., Oniahi H.)

1. Similarity problem over $SL(n, Z_p)$//Proc. Amer. Math. Soc. 1983. V. 87, N 2. P. 233—238.

Арасон (Arason J. Kr.)

1. Cohomologische Invarianten quadratischer Formen//J. Algebra. 1975. V. 36. P. 448—491.

Артин (Artin M.)

1. Brauer groups in ring theory and algebraic geometry//Lect. Notes Math. 1982. V. 917. P. 194—210.

Артин Э.

1. Геометрическая алгебра. — М.: Наука, 1969.

Артин, Тейт (Artin E., Tate J.)

1. Class field theory. Harvard, 1961.

Аш (Ash A.)

1. Cohomology of congruence subgroups of $SL(n, Z)$//Math. Ann. 1980. Bd 249, N 1. S. 55—73.
2. On the top Betti number of subgroups of $SL(n, Z)$//Math. Ann. 1983. Bd 264, N 3. S. 277—281.

3. Small-dimensional classifying spaces for arithmetic subgroups of general linear groups//Duke Math. J. 1984. V. 51, N 2. P. 459—468.

Аш, Грейсон, Грин (Ash A., Grayson D., Green P.)
1. Computations of cuspidal cohomology of congruence subgroups of $SL(3, Z)$//J. Number Theory. 1984. V. 19, N 3. P. 412—436.

Аш, Стивенс (Ash A., Stevans G.)
1. Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues//J. reine und angew. Math. 1986. Bd 365. S. 192—220.

Бак (Bak A.)
1. Le problème des sous-groupes de congruence et le problème métaplectique pour les groupes classiques de rang > 1//C. r. Acad. sci. 1981, ser. 1. V. 292, N 5. P. 307—310.

Бак, Рехман (Bak A., Rehman N.)
1. The congruence subgroup problem for skew field//C. r. Acad. Sci. 1979. V. 289, N 3. P. A151.
2. The congruence subgroup and metaplectic problems for $SL_{n\geqslant 2}$ of division algebras//J. Algebra. 1982. V. 78, N 2. P. 475—547.
3. K_2-analogs of Hasse's norm theorem//Comment. math. helv. 1984. V. 59, N 1. P. 1—11.

Бартельс (Bartels H.-J.)
1. Invarianten hermitescher Formen über Schiefkörpern//Math. Ann. 1975. V. 215, N 3. S. 269—288.
2. Zur Klassifikation schiefhermitescher Formen über Zahlkörpern//Math. Ann. 1976. B. 219, N 1. S. 13—19.
3. Definite arithmetische Gruppen//J. reine und angew. Math. 1978. Bd 301. S. 27—29.
4. Zur Galoiskohomologie definiter arithmetischer Gruppen//J. reine und angew. Math. 1978. Bd 278. S. 89—97.
5. Zur Arithmetik von Konjugationsklassen in algebraischen Gruppen//J. Algebra. 1981. V. 70, N 1. P. 179—199.
6. Zur Arithmetik von Diedergruppenerweiterungen//Math. Ann. 1981. B. 256. S. 465—473.

Бартельс, Китаока (Bartels H.-J., Kitaoka Y.)
1. Endliche arithmetische Untergruppen der GL_n//J. reine und angew. Math. 1980. V. 313, S. 151—156.

Басс (Bass H.)
1. The congruence subgroup problem//Proc. Conf. Local Fields. Dribergen, 1966. Berlin — Heidelberg — New York: Springer, 1967. P. 16—22.
2. Алгебраическая K-теория. — М.: Мир, 1973.

Басс, Лазар, Серр (Bass H., Lazard M., Serre J.-P.)
1. Sous groupes d'indices finis dans $SL(n, Z)$//Bull. Amer. Math. Soc. 1964. V. 70. P. 385—392.

Басс Х., Милнор Дж., Серр Ж.-П.
1. Решение конгруэнц-проблемы для SL_n $(n \geqslant 3)$ и Sp_{2n} $(n \geqslant 2)$//Математика. 1970. Т. 14, № 6. С. 64—128; Математика. 1971. Т. 15, № 1. С. 44—60.

Бейер-Флюкигер (Bayer-Fluckiger E.)
1. Intersections de groupes orthogonaux et principe de Hasse faible pour les systèmes de formes quadratiques sur un corps global//C. r. Acad. sci. 1985. Ser. 1. V. 301, N 20. P. 911—914.
2. Principe de Hasse faible pour les systemes de formes quadratiques//J. reine und angew. Math. 1987. Bd 378. P. 53—59.

Бейль (Beyl F.)
1. The Schur multiplicator of $SL(2, Z/mZ)$ and congruence subgroup property//Math. Z. 1986. Bd 191, N 1. S. 23—42.

Бейль, Таппе (Beyl F. R., Tappe J.)
1. Group extensions, representations and the Shur multiplicator//Lect. Notes Math. 1982. V. 958.

Бер (Behr H.)
1. Über die endliche Definierbarkeit von Gruppen//J. reine und angew. Math. 1962. Bd 211. S. 116—122.
2. Über die endliche Definierbarkeit verallgemeinerter Einheitengruppen. II// Invent. Math. 1967. Bd 4, N 4. S. 265—274.
3. Zur starken Approximation in algebraischen Gruppen über globalen Körpern//J. reine und angew. Math. 1968. Bd 229. S. 107—116.
4. Endliche Erzeugbarkeit arithmetischer Gruppen über Funktionenkörpern// Invent. Math. 1969. Bd 7, N 1. S. 1—32.
5. Explizite Präsentation von Chevalleygruppen über Z//Math. Z. 1975. Bd 141. S. 235—241.
6. $SL_3(F_q[t])$ is not finitely presentable//London Math. Soc. Lect. Notes Ser. 1979. N 36. P. 213—224.
7. Finite presentability of arithmetic groups over global function fields// Proc. Edinburgh Math. Soc. 1987. V. 30, N 1. P. 23—39.

Бертран (Bertrand D.)
1. Endomorphismes de groupes algebriques: applicationes arithmetiques// Approxim. diophant. et nombres transcendents. Colloq. Luminy. 13—19 Juin, 1982. Boston, 1983. P. 1—45.

Бёге (Böge S.)
1. Eine Bemerkung zur Reduktiontheorie in orthogonalen Gruppen//Math. Ann. 1971. Bd 193, N 1. S. 38—48.

Бондаренко А. А.
1. К проблеме максимальности арифметических подгрупп в ортогональных группах типа B_n//Мат. заметки. 1974. Т. 16, № 1. С. 151—161.
2. К классификации максимальных арифметических подгрупп в ортогональных группах типа (D_l)//ДАН БССР. 1974. Т. 18, № 9. С. 773—776.
3. Классификация максимальных арифметических подгрупп в ортогональных группах типа (D_l)//ДАН БССР. 1975. Т. 19, № 11. С. 969—972.
4. К классификации максимальных арифметических подгрупп в разложимых группах//Мат. сборник. 1977. Т. 102, № 2. С. 155—172.
5. Классификация максимальных арифметических подгрупп неопределенных ортогональных групп типа (B_l)//Мат. сб. 1985. Т. 127, № 1. С. 72—91.

Бондаренко А. А., Рапинчук А. С.
1. К оценке числа двойных смежных классов групп аделей алгебраических групп//ДАН БССР. 1978. Т. 22, № 5. С. 397—400.

Боревич З. И., Шафаревич И. Р.
1. Теория чисел. — М.: Наука, 1985.

Борель А.
1. Some finiteness properties of adele groups over number fields//Publ. Math. I. H. E. S. 1963. V. 16. P. 101—126.
2. Арифметические свойства алгебраических групп//Математика. 1964. Т. 8, № 2. С. 3—17.
3. Некоторые свойства групп аделей, связанных с алгебраическими группами//Математика. 1964. Т. 8, № 2. С. 73—75.
4. Фундаментальные множества арифметических групп//Математика. 1965. Т. 9, № 1. С. 127—139.
5. Density and maximality of arithmetic subgroups//J. reine und angew. Math. 1966. Bd 224. S. 78—89.
6. Фундаментальные множества арифметических групп и автоморфные формы//Математика. 1968. Т. 12, № 4. С. 80—103; 1968. Т. 12, № 5. С. 34—90; 1968. Т. 12, № 6. С. 3—30.
7. Introduction aux groupes arithmetiques. — Paris: Hermann, 1969.
8. Линейные алгебраические группы. — М.: Мир, 1972.
9. Cohomologie reele stable des groupes S-arithmetiques classiques//C. R. Acad. Sci. 1972. V. 274. P. A1700—A1702.
10. Stable real cohomology of arithmetic groups//Ann. Sci. Ecole Norm Sup. 1974. V. 7. P. 235—272.

11. Cohomology of arithmetic groups//Proc. Intern. Congr. Math. Vancouver, 1974. V. 1. P. 435—442.
12. Admissible representations of a semi-simple group over a local field with vectors, fixed under Iwahori subgroup//Invent. Math. 1976. Bd 35. S. 233—259.
13. Cohomologie des sous-groupes discrete et representations des groupes semisimples//Asterisque. 1976. V. 32—33. P. 73—112.
14. Stable and L^2-cohomology of arithmetic groups//Bull. Amer. Math. Soc. 1980. V. 3, N 3. P. 1025—1027.
15. On free subgroups of semi-simple groups//Enseign. Math. 1983. V. 29, N 1—2. P. 151—164.
16. Oeuvres collected papers. Vol. 1: 1948—1958. — Berlin: Springer, 1983.
17. Oeuvres collected papers. Vol. 2: 1959—1968. — Berlin: Springer, 1983.
18. Oeuvres collected papers. Vol. 3: 1969—1982. — Berlin: Springer, 1983.

Борель, Касельман (Borel A., Casselman W.)
1. Cohomologie d'intersection et L^2-cohomologie de varietes arithmetiques de rang rationnel 2//C. r. Acad. sci. 1985. Ser. I. V. 301, N 7. P. 369—373.

Борель, Мостов (Borel A., Mostow G. D.)
1. Algebraic groups and discontinuous subgroups//Proc. Symp Pure Math. 1966. v. 9. 426 p.

Борель, Прасад (Borel A., Prasad G.)
1. Finiteness theorems for discrete subgroups of bounded covolume in semi-simple groups//Publ. Math. I. H. E. S. 1989. V. 69. P. 119—171.

Борель, Серр (Borel A., Serre J.-P.)
1. Theoremes de finitude en cohomologie galoisienne//Comment. Math. Helv. 1964. V. 39, N 2. P. 111—164.
2. Adjonction de coins aux espaces symmetriques; applications a la cohomologie des groupes arithmetiques//C. r. Acad. Sci. 1970. V. 271, N 23. P. A1156.
3. Cohomologie a supports compacts des immeubles de Bruhat—Tits; applications a la cohomologie des groupes S-arithmetiques//C. r. Acad. Sci. 1971. V. 272, N 2. P. A110—A113.
4. Corners and arithmetic group//Comment. Math. helv. 1973. V. 48, P. 436—491.
5. Cohomologie d'immeubles et de groupes S-arithmetiques//Topology. 1976. V. 15, N 3. P. 211—232.

Борель, Спрингер (Borel A., Springer T. A.)
1. Rationality properties of linear algebraic groups//Tohôku Math. J. 1968. V. 20. P. 443—497.

Борель, Титс (Borel A., Tits J.)
1. Редуктивные группы//Математика. 1967. Т. 11, № 1. С. 43—111; Т. 11, № 2. С. 3—31.
2. Complements a l'article «Groupes reductifs»//Publ. Math. I. H. E. S. 1972. N 41. P. 253—276.
3. Унипотентные элементы и параболические подгруппы редуктивных групп. I//Математика. 1972. Т. 16, № 3. С. 3—12.

Борель, Уоллах (Borel A., Wallach N.)
1. Continuous cohomology, discrete subgroups and representation of reductive groups//Ann. Math. Stud. 1980. N 94.

Борель, Хардер (Borel A., Harder G.)
1. Existence of discrete compact subgroups of reductive groups over local fields//J. reine und angew. Math. 1978. Bd 298. S. 53—64.

Борель, Харишь-Чандра (Borel A., Harish-Chandra)
1. Arithmetic subgroups of algebraic groups//Bull. Amer. Math. Soc. 1961. V. 67, N 6. P. 579—583.
2. Арифметические подгруппы алгебраических групп Ли//Математика. 1964. Т. 8, № 2. С. 19—71.

Боровой М. В.
1. Абстрактная простота некоторых простых анизотропных алгебраических групп над числовыми полями//ДАН СССР. 1985. Т. 283, № 4. С. 794.

2. Когомологии Галуа вещественных редуктивных групп и вещественные формы простых алгебр Ли//Функц. анал. и его прил. 1988. Т. 22, № 2. С. 63—64.
3. Абстрактная простота групп типа D_n над числовыми полями//Успехи матем. наук. 1988. Т. 43, № 5. С. 179—180.
4. Слабая аппроксимация в однородных пространствах//ДАН СССР (в печати).

Браун К.
1. Когомологии групп. — М.: Наука, 1987.

Бритто (Britto J.)
1. On defining a subgroup of the special linear group by a congruence//J. Indian Math. Soc. 1976. V. 40, N 1—4, P. 235—243.
2. On the construction of non-congruence subgroups//Acta arithm. 1977. V. 33, N 3. P. 261—267.

Брюа (Bruhat F.)
1. Sur les representations des groupes classiques *p*-adiques. I//Amer. J. Math. 1961. V. 83, N 2. P. 321—338.
2. Sur les representations des groupes classiques *p*-adiques. II//Amer. J. Math. 1961. V. 83, N 2. P. 343—368.
3. Sur une classe de sous-groupes compacts maximaux de groupes de Chevalley sur un corps *p*-adique//Publ. Math. I. H. E. S. 1964. V. 23. P. 621—650.
4. Groupes algebriques semisimples sur un corps local//Actes Congr. intern. math. Paris, 1970. P. 285—290.

Брюа, Тите (Bruhat F., Tits J.)
1. Groupes algebriques simples sur un corps local//Proc. Conf. Local Fields. Driebergen, 1966. Berlin — Heidelberg — New York: Springer, 1967. P. 23—36.
2. Строение полупростых алгебраических групп над локальными полями// Математика. 1968, Т. 12, № 5. С. 19—33.
3. Groupes reductifs sur un corps local//Publ. Math. I. H. E. S. 1972. V. 41. P. 5—252.
4. Groupes reductifs sur un corps local. Chap II. Schemas en groupes. Existence d'une donnée radicielle valuée//Publ. Math. I. H. E. S. 1984. V. 60.
5. Schemas en groupes et immeubles des groupes classiques sur un corps local//Bull. Soc. Math. Fr. 1984. V. 112, N 2. P. 259—301.
6. Groupes algebriques sur un corps local. Chap. III. Complements et applications a la cohomologie galoisienne//J. Fac. Sci. Univ. Tokyo. 1987. Sec IA. V. 34, N 3. P. 671—688.

Бурбаки Н.
1. Алгебра. — М.: Физматгиз, гл. I—III — 1962, гл. IV—VI — 1965, гл. VII—IX — 1966.
2. Общая топология. — М.: Наука, гл. I—II — 1968, гл. III—VIII — 1969, гл. IX—X — 1975.
3. Интегрирование. — М.: Наука, гл. I—V — 1967, гл. VI—VII — 1970.
4. Группы и алгебры Ли. — М.: Мир, гл. I—III — 1976, гл. IV—VI — 1972, гл. VII—VIII — 1978.
5. Коммутативная алгебра. — М.: Мир, 1971.

Бюргисер (Bürgisser B.)
1. On the projective class group of arithmetic groups//Math. Z. 1983. Bd 184, N 3. S. 339—357.

Вайсман (Weisman C. S.)
1. On the connected identity component of adele class group of an algebraic torus//Proc. Amer. Math. Soc. 1969. V. 21. N 1. P. 155—160.

Ванг (Wang S.)
1. On the commutator group of a simple algebra//Amer. J. Math. 1950. V. 72, N 2. P. 323—334.

2. A note on free subgroups in linear groups//J. Algebra 1981. V. 71, N 1. P. 232—234.
3. On anisotropic solvable linear algebraic groups//Proc. Amer. Math. Soc. 1982. V. 84, N 1. P. 11—15.

Ван дер Варден Б. Л.
1. Алгебра. — М.: Наука, 1976.

Вассерштейн (Vaserstein L. N.)
1. О группе SL_2 над дедекиндовыми кольцами арифметического типа// Матем. сборник. 1972. Т. 89, № 2. С. 313—322.
2. On full subgroups of Chevalley groups//Tohôku Math. J. 1985. V. 37, N 4. P. 423—454.
3. On arithmetic subgroups of simple algebraic groups//Linear algebra and Appl. 1985. V. 72. P. 93—96.

Вейль (Weil A.)
1. Sur la theorie des formes quadratiques//Coll. Theorie Groupes Algebr. Bruxelles. — Paris. 1962. P. 9—22.
2. On the arithmetic theory of the classical groups//Proc. Conf. Arithm. Algebr. Geom. 1963. New-York. P. 1—3.
3. Алгебры с инволюцией и классические группы//Математика. 1963. Т. 7, № 4. С. 31—56.
4. Адели и алгебраические группы//Математика. 1964. Т. 8, № 4. С. 3—74.
5. О некоторых группах унитарных операторов//Математика. 1969. Т. 13, № 25. С. 33—94.
6. О формуле Зигеля в теории классических групп//Математика. 1969. Т. 13, № 6. С. 18—98.
7. Основы теории чисел. — М.: Мир, 1972.
8. Adeles and algebraic groups. — Boston: Birkhäuser, 1982.

Вейсфейлер (Weisfeiler B.)
1. Принцип Хассе для алгебраических групп, разложимых над квадратичным расширением//Функц. анализ и его приложения. 1972. Т. 6, № 2. С. 21—23.
2. Strong approximation for Zariski-dense subgroups of semi-simple algebraic groups//Ann. Math. 1984. V. 120, N 2. P. 271—315.

Венкатарамана (Venkataramana T. N.)
1. Sur la super-rigidity et l'arithmeticite des reseaux dans les groupes sur des corps locaux de caracteristique quelconque//C. r. Acad. sci. 1986. V. 302, N 10. P. 371—373.
2. Zariski dense subgroups of arilhmetic groups//J. Algebra. 1987. V. 108, N 2. P. 325—339.

Верфритц (Wehrfritz B. A. E.)
1. The conjugacy of tori//Bull. London Math. Soc. 1986. V. 18, N 1. P. 11—16.

Винберг Э. Б.
1. О группах единиц некоторых квадратичных форм//Матем. сб. 1972. Т. 87, № 1. С. 18—36.

Винберг Э. Б., Горбацевич В. В., Шварцман О. В.
1. Дискретные подгруппы группы Ли//Итоги науки и техн. ВИНИТИ. Совр. пробл. мат.: Фундам. направления. 1988. № 21. С. 5—120.

Винберг Э. Б., Онищик А. Л.
1. Семинар по группам Ли и алгебраическим группам. — М.: Наука, 1988.
2. Основы теории групп Ли//Итоги науки и техн. ВИНИТИ. Совр. пробл. мат.: Фундам. направления. 1988. № 20. С. 5—101.

Винберг Э. Б., Шварцман О. В.
1. Дискретные группы движений пространств постоянной кривизны//Итоги науки и техн. ВИНИТИ. Соврем. пробл. мат.: Фундам. направления. 1988. № 29. С. 147—259.

Витт (Witt E).
1. Schiefkörper über diskret Bewertung Körpern//J. reine und angew. Math. 1936. Bd 176. S. 153—156.

Воронович И. И.
1. Локально-глобальный принцип для алгебр над полями рациональных функций//ДАН БССР. 1987. Т. 31, № 10. С. 877—880.
2. Линейный локально-глобальный принцип для алгебр над полями рациональных функций: Препринт № 25/295. Минск: Ин-т мат. АН БССР, 1987.

Воскресенский В. Е.
1. Бирациональные свойства линейных алгебраических групп//Изв. АН СССР. Сер. мат. 1970. Т. 34, № 1. С. 3—19.
2. О слабой аппроксимации в алгебраических группах//Исследов. по теории чисел. — Саратов: изд-во Саратов. ун-та, 1972. Вып. 4. С. 3—7.
3. Алгебраические торы. — М.: Наука, 1977.
4. Целочисленные структуры в алгебраических торах и группы классов числовых полей//Семинар по арифметике алгебр. многообразий. Саратов, 1979. С. 8—15.
5. Проективные инвариантные модели Демазюра//Изв. АН СССР. Сер. мат. 1982. Т. 46, № 2. С. 195—210.
6. Арифметика алгебраических групп и однородных пространств//Исследования по теории чисел. Саратов. 1987. № 9. С. 7—38.

Гарланд (Garland H.)
1. The spectrum of non-compact G/T and the cohomology of arithmetic groups//Bull. Amer. Math. Soc. 1969. V. 75, N 4. P. 807—811.
2. A finiteness theorem for K_2 of a number field//Ann. of Math. 1971. V. 94. P. 534—548.
3. On the cohomology of discrete subgroups of p-adic groups//Proc. Intern. Congr. Math. Vancouver. 1974. v. 1. P. 449—453.

Гарланд, Рагунатан (Garland H., Raghunathan M. S.)
1. Fundamental domains for lattices in (R)-rank one semi-simple Lie groups//Ann. of Math. 1970. V. 92. P. 354—360.

Гарланд, Сия (Garland H., Hsiang W. C.)
1. A square integrability criterion for the cohomology of arithmetic groups// Proc. Nat. Acad. Sci. USA. 1968. V. 59, N 2. P. 354—360.

Гаусс К. Ф.
1. Арифметические исследования//Труды по теории чисел. — М.: Изд-во АН СССР, 1959. С. 7—583.

Герстейн (Gerstein L. J.)
1. On the proper spinor genus of a quadratic form//Lin. and Mult. Algebra. 1982. V. 11, N 2. P. 203—208.

Годеман (Godement R.)
1. Domaines fondamentaux des groupes arithmetiques//Sem. Bourbaki (1962—1963). Paris. 1964. V. 15, N 3. P. 257/01—257/25.
2. Formes automorphes et produite euleriens d'apres R. P. Langlands//Lect. Notes. Math. 1971. V. 179. P. 37—53.

Гото М., Гроссханс Ф.
1. Полупростые алгебры Ли. — М.: Мир, 1981.

Громов (Gromov M.)
1. Hyperbolic groups//Essays Group Theory. N. Y., 1987. P. 75—263.

Громов, Пятецкий-Шапиро (Gromov M., Piatetski-Shapiro I.)
1. Non-arithmetic groups in Lobachevsky spaces//Publ. I. H. E. S. 1988. N 66. P. 93—103.

Гротендик (Grothendieck A.)
1. Representations lineaires et compactification profinie des groupes discretes//Manusc. Math. 1970. V. 2. P. 375—396.

Грюневальд, О'Хэллори (Grunewald F. Y., O'Halloran J.)
1. Nilpotent groups and unipotent algebraic groups//J. Pure and Appl. Algebra. 1985. V. 37, N 3. P. 299—313.

Грюневальд, Сегал (Grunewald F. J., Segal D.)
1. A note on arithmetic groups//Bull. London Math. Soc. 1978. V. 10. P. 297—302.

2. The solubility of certain decision problems in arithmetic and algebra// Bull. Amer. math. soc. 1979. V. 1, N 6. P. 915—918.
3. Some general algorithms. I. Arithmetic groups//Ann. of Math. 1980. V. 112, N 3. P. 531—583.
4. Some general algorithms. II. Nilpotent groups//Ann. of Math. 1980. V. 112, N 3. P. 585—617.
5. Decision problems concerning S-arithmetic groups//J. Symbol. Log. 1985. V. 50, N 3. P. 743—772.

Грюневальд, Швермер (Grunewald F. J., Schwermer J.)
1. Free non-abelian quotients of SL_2 over orders of imaginary quadratic number fields//J. Algebra. 1981. V. 69, N 2. P. 298—304.

Гурак (Gurak S.)
1. On the rational equivalence of full decomposable forms//J. Number Theory. 1982. V. 14, N 2 P. 251—259.
2. On the Hasse norm principle//J. reine und angew. Math. 1978. V. 299/300. P. 16—27.

Дансе (Danset R.)
1. Methode du cercle adelique et principe de Hasse fin pour certain systemes de formes//Enseign. Math. 1985. V. 31, N 1—2. P. 1—66.

Делинь (Deligne P.)
1. Extensions centrales non residuellement finies de groupes arithmetiques// C. r. Acad. Sci. Paris. Ser. A. 1978. V. 287. P. 203—208.

Делоне Б. Н., Галиулин Р. В., Штогрин Н. И.
1. О типах Бравэ решеток//Итоги науки и техники. ВИНИТИ. Соврем. пробл. мат.; Фундам. направления. 1973. № 2. С. 119—254.

Демазюр (Demazure M.)
1. Sous-groupes arithmetiques des groupes algebriques lineaires//Sem. Bourbaki (1961—1962). Paris. 1962. V. 3. P. 235/1—235/12.

Деодер (Deodhar V. V.)
1. On central extensions of rational points of algebraic groups//Amer. J. Math. 1978. V. 100. N 2. P. 303—386.
2. On central extensions of rational points of algebraic groups//Contemp. Math. 1982. V. 9. P. 319—322.

Джеймс (James D.)
1. On the normal subgroups of integral orthogonal groups//Pacif. J. Math. 1974. V. 52, N 1. P. 107—114.
2. Orthogonal groups of three dimensional anisotropic quadratic forms//J. Algebra. 1975. V. 37, N 1. P. 121—136.

Джейн (Jehne W.)
1. Der Hassesche Normensatz und seine Entwicklung//Mitt. math. Ges. Hamburg 1982. V. 11, N 1. S. 143—153.

Джекобсон (Jacobson N.)
1. Cayley numbers and simple Lie algebras of type G_2//Duke Math. J. 1939. V. 5. P. 775—783.
2. Composition Algebra and Their Automorphisms//Rend Circolo math. Palermo. 1958. V. 7, N 1. P. 55—80.

Джонсон (Johnson F. E. A.)
1. On the existence of irreducible lattices//Arch. Math. 1984. Bd 43, N 5. S. 391—396.

Джонсон (Johnson R. P.)
1. Orthogonal groups of local anisotropic spaces//Amer. J. Math. 1969. V. 91, N 4. P. 1077—1105.

Дойл, Джеймс (Doyle C., James D.)
1. Discreteness criteria and high order generators for subgroups of $SL(2, R)$//Ill. J. Math. 1981. V. 15, N 2. P. 191—200.

Дойринг (Deuring M.)
1. Algebren. — Berlin: Springer, 1935.

Дракохруст Ю. А.
1. О полном препятствии к принципу Хассе//ДАН БССР. 1986. Т. 30, № 1. С. 5—8.
Дракохруст Ю. А., Платонов В. П.
1. Норменный принцип Хассе для полей алгебраических чисел//Изв. АН СССР. Сер. мат. 1986. Т. 50, № 5. С. 946—968.
Дракел, Кнезер (Draxl P., Kneser M.)
1. SK_1 von Schiefkörpern//Lect. Notes. Math. 1980. V. 778.
Дуайер (Dwyer W. G.)
1. Homology of integral upper-triangular matrices//Proc. Amer. Math. Soc. 1985. V. 94, N 3. P. 523—528.
Дьедонне (Diedonne J.)
1. On the structure of unitary groups//Trans. Amer. Math. Soc. 1952. V. 72. P. 367—385.
2. Геометрия классических групп. — М.: Мир, 1974.
Жентиль (Gentile E. R.)
1. Metodos locales-globales (aspectos historicos)//Trab. mat. Inst. argent. mat. 1986. N 96. P. 1—29.
Жиро (Giraud T.)
1. Cohomologie non abelienne. — Berlin — Heidelberg — New York: Springer, 1971.
Жук И. К.
1. О рациональности некоторых однородных пространств группы $SO(q)$// ДАН БССР. 1982. Т. 26, № 9. С. 773—775.
Закирьянов К. Х.
1. Конечность ширины симплектических групп над кольцами алгебраических чисел относительно элементарных матриц//Алгебра и логика. 1985. Т. 24. № 6. С. 667—673.
Зигель (Siegel C. L.)
1. Über die analytische Theorie der quadratischen Formen//Ann. of Math. 1935. V. 36. P. 527—606.
Ивасава К.
1. Локальная теория полей классов.— М.: Мир, 1983.
Ивахори, Мацумото (Iwahori N., Matsumoto H.)
1. On some Bruhat decomposition and the structure of the Hecke rings of p-adic Chevalley groups//Publ. Math. I. H. E. S. 1965. N 25. P. 5—48.
Игуза (Igusa J.-I.)
1. Some observations on metaplectic groups//Amer. J. Math. 1981. V. 103, N 6. P. 1343—1365.
Ихара (Ihara J.)
1. Дискретные подгруппы группы $PL(2, k_p)$// Математика. 1968. Т. 12, № 5. С. 131—138.
2. Congruence relations and fundamental groups//J. Algebra. 1982. V. 75, N 2. P. 445—451.
Иянага (Iyanaga K.)
1. Arithmetic of special unitary groups and their simplectic representations//J. Fac. Sci. Univ. Tokyo. 1968. Sec. 1. V. 15, N 1. P. 35—36.
2. On certain double coset spaces of algebraic groups//J. Math. Soc. Japan. 1971. V. 23. P. 103—122.
Каждан Д. А.
1. О связи дуального пространства группы со строением ее замкнутых подгрупп//ФАН. 1967. Т. 1, вып. 1. С. 71—74.
Канеда (Kaneda M.)
1. Generators and relations for special linear algebras and groups//J. Algebra. 1985. V. 94, N 1. P. 1—18.
Карияма (Kariyama K.)
1. On the conjugacy classes of anisotropic maximal tori of a Chevalley group over a local field//J. Algebra. 1986. V. 99. N 1. P. 22—49.

Картан А., Эйленберг С.
1. Гомологическая алгебра. — М.: ИЛ, 1960.
Картан (Cartan E.)
1. Sur certaines formes riemanniennes remarquable des geometries de groupe fondamental simple//Ann. Ec. Norm. Sup. 1927. V. 44. P. 345—467.
Картер, Келлер (Carter D., Keller G.)
1. Bounded elementary generation of $SL_n(O)$//Amer. J. Math. 1983. V. 105, N 3. P. 673—687.
Касселс Дж.
1. Рациональные квадратичные формы. — М.: Мир, 1982.
Катаяма (Katayama S.)
1. Class number relations of algebraic tori. I//Proc. Jap. Acad. 1986. A62, N 6. P. 216—218.
2. Class number relations of algebraic tori. II//Proc. Jap. Acad. 1986. A62, N 8. P. 321—322.
Квиллен (Quillen D. L.)
1. Classification of normal congruence subgroups of the modular group// Amer. J. Math. 1965. V. 87, N 2. P. 285—296.
Китаока (Kitaoka Y.)
1. Scalar extension of quadratic lattices//Nagoya Math. J. 1977. V. 66. P. 139—149.
2. Scalar extension of quadratic lattices II//Nagoya Math. J. 1977. V. 67. P. 159—164.
Клейн (Klein F.)
1. Zur Theorie der elliptischen Modulfunktionen//Math. Ann. 1880. Bd 17. S. 72—76.
Клозе (Klose J.)
1. Metaplektische Erweiterungen von Quaternionen-schiefkörpern//Math. Z. 1986. Bd 193, N 4. S. 625—649.
Кнезер (Kneser M.)
1. Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen//Arch. Math. 1956. Bd 7, N 5. S. 323—332.
2. Orthogonale Gruppen über algebraischen Zahkörpern//J. reine und angew. Math. 1956. Bd 196, N 3—4. S. 213—220.
3. Klassenzahlen definiter quadratischer Formen//Arch. Math. 1957. Bd 8, N 4. S. 241—250.
4. Einfach zusammenhängende algebraische Gruppen in der Arithmetik// Proc. Intern. Cong. Math. Djursholm, Uppsala. 1962. S. 260—263.
5. Schwache approximation in algebraische Gruppen//Colloq. Theor. Groupes Algebr. Bruxelles, Louvain — Paris. 1962. S. 41—52.
6. Approximationssätze für algebraische Gruppen//J. reine and angew. Math. 1962. Bd 209, N 1. S. 96—97.
7. Erzeugende und Relationen verallgemeinerter Einheitengruppen//J. reine und angew. Math. 1964. Bd. 214—215. S. 345—349.
8. Galois — Kohomologie halbenfacher algebraischer Gruppen über p-adischen Körpern I.//Math. Z. 1965. Bd 88, N 1. S. 40—47.
9. Galois-Kohomologie halbenfacher algebraischer Gruppen über p-adischen Körpern II.//Math. Z. 1965. Bd 89. S. 250—272.
10. Starke approximation in algebraischer Gruppen I.//J. reine und angew. Math. 1965. Bd 218. S. 190—203.
11. Strong approximation//Proc. Symp. Pure Math. 1966. V. 9. P. 187—197.
12. Lectures on Galois Cohomology of Classical Groups. — Bombay: Tata Inst. of Fund. Research, 1969.
13. Normal subgroups of integral orthogonal groups//Lect. Notes Math. 1969. V. 108. P. 67—71.
14. Normalteiler ganzzahliger Springruppen//J. reine und angew. Math. 1979. Bd 311—312. S. 191—214.

15. Erzeugung ganzzahlige orthogonaler Gruppen durch Spiegelungen//Ann. of Math. 1981. V. 255, N 4. P. 453—462.

Кнезер, Тамагава (Kneser M., Tamagawa T.)
1. Another formulation and proof of Siegel's theorems on quadratic forms// Abstr. Short Communs. Intern. Congr. Math. Edinburg. 1958. P. 32.

Кнопп, Нейманн (Knopp M. J., Newman M.)
1. Congruence subgroups of positive genus of the modular group//Ill. J. Math. 1965. V. 9, N 4. P. 577—583.

Кокс, Пэрри (Cox D., Parry W.)
1. Genera of congruence subgroups in Q-quaternion algebras//J. reine und angew. Math. 1984. Bd 351. S. 66—112.

Коксетер Г. С. М., Мозер У. О. Дж.
1. *Порождающие элементы и определяющие соотношения дискретных групп.* — М.: Наука, 1980.

Колывагин В. А.
1. Конечность E(Q) и Ш(E, Q) для подкласса кривых Вейля//Изв. АН СССР. Сер. мат. 1988. Т. 52, № 3. С. 522—540.
2. О группах Морделла — Вейля и Шафаревича — Тейта для эллиптических кривых Вейля//Изв. АН СССР. Сер. мат. 1988. Т. 52, № 6. С. 1154—1180.

Корэй (Coray D. F.)
1. The Hasse principle for pairs of quadratic forms//London Math. Soc. Lect. Note Ser. 1982. N 56. P. 237—246.

Костант (Kostant B.)
1. Groups over Z.//Proc. Symp. Pure Math. 1966. V. 9. P. 90—98.

Коттвиц (Kottwitz R.)
1. Stable trace formula: cuspidal tempered terms.//Duke Math. J. 1984. V. 51, N 3. P. 611—650.
2. Stable trace formula: Elliptic singular terms//Math. Ann. 1986. V. 275. P. 365—399.
3. Tamagawa numbers//Ann. Math. 1988. V. 127, N 3, P. 629—646.

Кох Х.
1. Теория Галуа p-расширений. — М.: Мир, 1973.

Крэм (Cram G.-M.)
1. Locally isomorphic algebras and a Hasse principle for split metacyclic groups//Arch. Math. 1986. Bd 47, N 4. S. 330—338.

Кунявский Б. Э.
1. Арифметические свойства трехмерных алгебраических торов//Зап. науч. сем. ЛОМИ АН СССР. 1982. Т. 116, С. 102—107.

Курсов В. В.
1. О коммутаторной длине групп Шевалле над полем//ДАН БССР. 1985. Т. 29, № 1. С. 27—30.

Курсов В. В., Янчевский В. И.
1. Скрещенные произведения простых алгебр и их групп автоморфизмов// ДАН БССР. 1988. Т. 32, № 9. С. 777—780.

Кэртис Ч., Райнер И.
1. Теория представлений конечных групп и ассоциативных алгебр. — М.: Наука, 1969.

Лабес, Швермер (Labesse J.-P., Schwermer J.)
1. On liftings and cusp cohomology of arithmetic groups//Invent. Math. 1986. V. 83, N 2. P. 383—401.

Лазар (Lazard)
1. Groupes analitiques p-adiques//Publ. Math. I. H. E. S. 1965. V. 26. P. 5—219.

Ламон (Lamont P.)
1. Approximations theorems for the group G_2//Indag. Math. 1964. V. 26, N 2. P. 187—192.

Ландер (Landherr W.)
1. Liesche Ringe vom Typus A über einen algebraischen Zahlkörper und hermitesche Formen über einem Schiefkörper//Abh. Math. Sem. Hamburg. 1938. B. 12. S. 200—241.

Ленг (Lang S.)
1. Algebraic groups over finite fields.//Amer. J. Math. 1958. V. 78, N 3. P. 553—563.
2. Алгебраические числа. — М.: Мир, 1966.
3. Алгебра. — М.: Мир. 1968.

Ленглендс (Langlands R. P.)
1. The volume of the fundamental domain for some arithmetical subgroups of Chevalley groups.//Proc. Symp. Pure Math. 1966. V. 9. P. 143—148.

Ли (Lee G.)
1. A geometric method for presenting subgroups of discrete groups.//Topol. and Appl. 1984. V. 18, N 2—3. P. 179—195.

Лиел (Liehl B.)
1. On the group SL_2 over orders of arithmetic type//J. reine und angew. Math. 1981. Bd. 323. S. 753—771.
2. Beschränkte Wortlänge in SL_2.//Math. Z. 1984. Bd 186, N 4. S. 509—524.

Линдон Р., Шупп П.
1. Комбинаторная теория групп. — М.: Мир, 1980.

Льюис (Lewis D. W.)
1. Quaternionic skew-hermitian forms over a number field.//J. Algebra. 1982. V. 74, N 1. P. 232—240.

Лэй (Lai K. F.)
1. On the Tamagawa number of quasi-split groups.//Bul. Amer. Math. Soc. 1976. V. 82, N 2. P. 300—302.
2. Tamagawa number of reductive algebraic groups.//Compos. Math. 1980. V. 41, N 2, P. 153—188.
3. On the cohomology of congruence subgroups of symplectic groups.// Nagoya Math. J. 1982. V. 85. P. 155—174.

Любоцки (Lubotzky A.)
1. Free quotients and the congruence kernel of SL_2.//J. Algebra. 1982. V. 77, N 2. P. 411—418.

Макдональд И. Г.
1. Сферические функции на группе p-адического типа//Успехи мат. наук. 1973. Т. 28, № 5. С. 155—224.

Маклахлан (Maclachlan C.)
1. On the structure of the certain arithmetic subgroups of $SL_2(\mathbf{R})$.//Math. Proc. Cambridge Phil. Soc. 1985. V. 97, N 2. P. 211—217.

Мальцев А. И.
1. О полупростых подгруппах групп Ли//Известия АН СССР, сер. матем. 1944. Т. 8, № 4. С. 143—174.
2. On the theory of the Lie groups in the large//Матем. сб. 1945. Т. 16, № 2. С. 163—189.

Маргулис Г. А.
1. Дискретные группы движений многообразий неположительной кривизны//Proc. Intern. Congr. Math. Vancouver, 1974. 1975. V. 2. P. 21—33.
2. Коограниченные подгруппы в алгебраических группах над локальными полями//Функц. анализ и его прилож. 1977. Т. 11, № 2. S. 45—57.
3. Факторгруппы дискретных подгрупп и теория меры//Функц. анализ и его приложения. 1978. Т. 12, № 4. С. 64—80.
4. Конечность факторгрупп дискретных подгрупп//Функц. анализ и его приложения. 1979. Т. 13, № 3. С. 28—39.
5. О мультипликативной группе алгебры кватернионов над глобальным полем//ДАН СССР. 1980. Т. 252, № 3, С. 542—546.
6. Arithmeticity of irreducible lattices of semisimple groups of rank greater than 1.//Invent. Math. 1984. V. 76, N 1. P. 93—120.

Маргулис, Сойфер (Margulis G. A., Soifer G. A.)
1. Maximal subgroups of infinite index in finitely generated linear groups.// J. Algebra. 1981. V. 69, N 1. P. 1—23.
Марс (Mars J. G.)
1. Les nombres de Tamagawa de certains groupes exeptionnels.//Bull. Soc. Math. France 1966. V. 94, N 2. P. 97—140.
2. Solution d'un probleme pose par A. Weil.//C. r. Acad. Sci. 1968. V. 266, N 9. P. A484—A486.
3. The Tamagawa number of ^2A_n//Ann. of Math. 1969. V. 89. N 3. P. 557—574.
4. Le nombres de Tamagawa de groupes semisimples.//Lect. Notes Math. 1971. N 179. P. 79—94.
Матвеев Г. В.
1. Род элементов ортогональной группы//Мат. заметки. 1973. Т. 13, № 5. С. 695—702.
2. Род элементов унитарных групп//ДАН БССР. 1974. Т. 18, № 5. С. 391—393.
3. Принцип Хассе для решеток в полной матричной алгебре//Мат. заметки. 1981. Т. 30, № 6. С. 801—805.
Матье (Mathieu P.)
1. Le principle de Hasse et les groupes semi-simples. I.//Bull. Soc. Math. Belg. 1983. B. 35, N 2. P. 119—125.
Матьюз (Matthews C. R.)
1. Counting points modulo p for some finitely generated subgroups of algebraic groups.//Bull. London Math. Soc. 1982. V. 14, N 2. P. 149—154.
Матьюз, Вассерштейн, Вейсфейлер (Matthews C. R., Vaserstein L. N., Weisfeiller B.)
1. Congruence properties of Zarisky-dense subgroups. I.//Proc. London Math. Soc. 1984. V. 48, N 3. P. 514—532.
Мацумото (Matsumoto M.)
1. Une theoreme de Sylow les groupes semisimple p-adiques.//C. R. Acad. Sci. 1966. V 262, N 8. P. A425—A427.
2. Sur les sous-groupes arithmetiques des groupes semisimples deployee// Ann. Sci. Ecole Norm. Sup. 1969. V. 2, N 1. P. 1—62.
Мельников О. В.
1. Конгруэнц-ядро группы $SL_2(Z)$//ДАН СССР. 1976. Т. 228, № 5. С. 1034—1036.
Мендоза (Mendoza E. R.)
1. Cohomology of PGL(2) over imaginary quadratic integers.//Bonn. Math. Schr. 1980. N 128.
Меннике (Mennicke J.)
1. Finite factor groups of the unimodular group.//Ann. of Math. 1965. V. 81, N 1. P. 31—37.
2. On Ihara's modular group//Invent. Math. 1967. V. 4, N 3. P. 202—228.
3. Discontinuous groups.//Lect. Notes Math. 1984. N 1098. P. 75—80.
Милн (Milne J. S.)
1. Этальные когомологии. — М.: Мир, 1983.
2. The Action of an Automorphism of $\bar{C}$ on a Shimura Variety and its Special Points//Arithmetic and Geometry. V. 1. — Boston: Birkhäuser, 1983. P. 239—264.
3. Arithmetic duality theorems. — Academic Press, 1986.
Мильсон, Рагунатан (Milson J. J., Raghunathan M. S.)
1. Geometric construction of cohomology for arithmetic groups//Proc. Indian Acad. Sci. Math. Sci. 1981. V. 90, N 2. P. 103—123.
Минковский (Minkowski H.)
1. Uber den arithmetischen Begriff der äquivalenz und über die endlichen Gruppen linearer ganzzahliger Substitutionenn//J. reine und angew. Math. 1887. Bd 109. S. 196—202.

2. Zur Theorie der positiven quadratischen Formen//J. reine und angew. Math. 1887. Bd 101. S. 196—202.
3. Geometrie der Zahlen. — Leipzig, 1910.

Минчев Х. П.
1. Сильная аппроксимация для многообразий над полем алгебраических чисел//ДАН БССР. 1989. Т. 33, № 1. С. 5—8.

Монастырный А. П., Янчевский В. И.
1. О группах Уайтхеда и гипотезе Кнезера — Титса для спинорных групп//ДАН СССР. 1989. Т. 307, № 1. С. 31—35.

Мос (Moss K.)
1. Homology of SL $\left(n, Z\left[\frac{1}{p}\right]\right)$ // Duke Math. J. 1980. V. 47, N 4, P. 803—818.

Мостов (Mostow G. D.)
1. Self-adjoint groups/Ann. Math. 1955. V. 62, N 1. P. 44—55.
2. Fully reducible subgroups of algebraic groups//Amer. J. Math. 1956. V. 78. P. 200—221.
3. Discrete subgroups of Lie groups//Asterisque. 1985. num. hors. ser. P. 289—309.

Мостов, Тамагава (Mostow G. D., Tamagawa T.)
1. On the compactness of arithmetically defined homogeneous spaces//Ann. of Math. 1962. V. 76, N 3. P. 446—464.

Мур (Moore C.)
1. Group extensions of p-adic and adelic linear groups//Publ. Math. I. H. E. S. 1968. V. 35. P. 5—70.

Нагата (Nagata M.)
1. Invariants of a group in an affine ring//J. Math. Kyoto Univ. 1964. V. 3. P. 369—377.

Накаяма, Мацусима (Nakayama T., Matsushima Y.)
1. Über die multiplikative Gruppe einer p-adischen Divisionsalgebra//Proc. Imperial Academy (Tokyo). 1943. V. 19. P. 622—628.

Нисневич (Nisnevich Y.)
1. Неабелевы когомологии и теоремы конечности для целочисленных орбит аффинных групповых схем//Изв. АН СССР. Сер. матем. 1975. Т. 39, № 4. С. 773—795.
2. Espaces homogenes principaux rationnellement triviaux et arithmetique des schemas en groupes reductifs sur les anneaux de Dedekind//C. R. Acad. Sci. 1984. V. 299, N 1. P. 5—8.

Нори (Nori M.)
1. Groupe de monodromie non arithmetique//C. r. Acad. Sci. 1986. ser. I. V. 302, N 2. P. 71—72.
2. On subgroups of $GL_n(F_p)$//Invent. Math. 1987. V. 88, N 2. P. 257—275.

Ньюмен (Newman M.)
1. Normal congruence subgroups of the modular group//Amer. J. Math. 1963. V. 85, N 3. P. 419—427.
2. Classification of normal subgroups of the modular group./Trans. Amer. Math. Soc. 1967. V. 126. P. 267—277.
3. The classical modular groups as a subgroup of GL(2, Z)//Glasgow Math. J. 1985. V. 27. P. 161—164.

О'Мира (O'Meara O. T.)
1. Introduction to quadratic forms. — Berlin — Heidelberg — New York: Springer, 1963.
2. On the finite generation of linear groups over Hasse domains//J. reine und angew. Math. 1965. Bd 217. S. 79—108.

Оно (Ono T.)
1. On the compacity of the orthogonal groups//Nagoya Math. J. 1954. V. 7. P. 111—114.

2. Arithmetic of orthogonal groups//Nagoya Math. J. 1955. V. 9. P. 129—146.
3. Принцип Хассе в ортогональных группах//Сугаку. 1956. Т. 7, № 1. С. 15—22.
4. Sur une propriete arithmetique des groupes algebriques commutatifs// Bull. Soc. Math. France, 1957. V. 85, N 3. P. 307—323.
5. Arithmetic of algebraic tori//Ann. of Math. 1961. V. 74, N 1. P. 101—139.
6. On the Tamagawa number of algebraic tori//Ann. of Math. 1963. V. 78, N 1. P. 47—73.
7. О числе Тамагава//Сугаку. 1963. Т. 15, № 2. С. 72—81.
8. On the relative theory of Tamagawa numbers//Bull. Amer. Math. Soc. 1964. V. 70, N 2. P. 325—326.
9. The Gauss-Bonnet theorem and the Tamagawa number//Bull. Amer. Math. Soc. 1965. V. 71, N 2. P. 345—348.
10. On the relative theory of Tamagawa numbers//Ann. of Math. 1965. V. 82, N 1. P. 88—111.
11. On algebraic groups and discontinuous groups//Nagoya Math. J. 1966. V. 27, N 1. P. 279—322.
12. A generalization of Gauss' theorem on the genera of quadratic forms// Proc. Jap. Acad. 1985. A61, N 4. P. 109—111.

Ополка (Opolka H.)
1. Zur Auflösung zahlentheoretischer Knoten//Math. Z. 1980. Bd 173, N 1. S. 95—103.
2. Geschlechter von zentralen Erweiterungen//Arch. Math. 1981. Bd 37, N. 5. S. 418—424.

Паримала, Шридхаран (Parimala R., Sridharan R.)
1. A local-global principle for quadratic forms over polynomial rings//J. Algebra. 1982. V. 74, N 1. P. 264—269.

Паршин А. Н.
1. Арифметика алгебраических многообразий//Алгебра. Топология. Геометрия. — М.: ВИНИТИ, 1971. С. 111—151.

Пизер (Pizer A.)
1. On the arithmetic of quaternion algebras//Acta arithm. 1976. V. 31, N 1. P. 61—89.
2. On the arithmetic of quaternion algebras. II//J. Math. Soc. Japan. 1976. V. 28, N 4. P. 676—688.

Пирс Р.
1. Ассоциативные алгебры. — М.: Мир, 1986.

Платонов В. П.
1. Группы аделей и проблема рода для целочисленных представлений// ДАН БССР. 1968. Т. 12, № 10. С. 866—868.
2. Группы аделей и целочисленные представления//Изв. АН СССР. Сер. матем. 1969. Т. 33, № 1. С. 155—162.
3. Сильная аппроксимация в алгебраических группах и гипотеза Кнезера — Титса//ДАН БССР. 1969. Т. 13, № 7. С. 585—587.
4. Проблема сильной аппроксимации и гипотеза Кнезера — Титса для алгебраических групп//Изв. АН СССР. Сер. матем. 1969. Т. 33, № 6. С. 1211—1219.
5. Дополнение к работе «Проблема сильной аппроксимации и гипотеза Кнезера — Титса для алгебраических групп»//Изв. АН СССР. Сер. матем. 1970, Т. 34, № 4. С. 775—777.
6. О конгруэнц-проблеме для разрешимых целочисленных групп//ДАН БССР. 1971. Т. 15, № 10. С. 869—872.
7. К проблеме максимальности арифметических групп//ДАН СССР. 1971. Т. 200, № 3. С. 530—533.
8. О проблеме рода в арифметических группах//ДАН СССР. 1971. Т. 200, № 4. С. 793—796.

9. Арифметическая теория линейных алгебраических групп и теория чисел//Труды Матем. ин-та АН СССР. 1973. Т. 132. С. 162—168.
10. Гипотеза Дьедонне и несюръективность накрытий алгебраических групп на k-точках//ДАН СССР. 1974. Т. 216, № 5. С. 986—989.
11. Арифметические и структурные проблемы в линейных алгебраических группах//Proc. Intern. Congr. Math. Vancouver, 1974. V. 1. 1975. P. 471—476.
12. Алгебраические группы//Алгебра. Топология. Геометрия. Итоги науки и техники. Т. 11. — М.: ВИНИТИ, 1974. С. 5—36.
13. О проблеме Таннака — Артина//ДАН СССР. 1975. Т. 221, № 5. С. 1038—1041.
14. Об аппроксимации в алгебраических группах над произвольными полями//ДАН СССР. 1976. Т. 229, № 4. С. 804—807.
15. Проблема Таннака — Артина и приведенная K-теория. Изв. АН СССР. Сер. матем. 1976. Т. 40, № 2. С. 227—261.
16. Приведенная K-теория и аппроксимация в алгебраических группах// Труды Матем. ин-та АН СССР. 1976. Т. 142, С. 198—207.
17. Бирациональные свойства приведенной группы Уайтхеда//ДАН БССР. 1977. Т. 21, № 3. С. 197—198.
18. К проблеме рациональности спинорных многообразий//ДАН СССР. 1979. Т. 248, № 3. С. 524—527.
19. Algebraic groups and reduced K-theory//Proc. Intern. Congr. Math. Helsinki, 1978. V. 1. 1980. P. 311—317.
20. Бирациональные свойства спинорных многообразий//Труды Матем. ин-та АН СССР им. В. А. Стеклова. 1981. Т. 157. Т. 161—169.
21. Арифметическая теория алгебраических групп//Успехи мат. наук. 1982. Т. 37, № 3. С. 3—54.
22. Группы аделей и числа классов//Труды матем. ин-та АН СССР. 1984. Т. 163. С. 205—214.
23. Кольца и многообразия представлений конечно-порожденных групп// Вопросы алгебры. Вып. 4. — Минск: Изд-во «Университетское», 1988. С. 36—40.
24. Geometric approach to the representation theory of finitely generated groups//Lect. Notes Math. (в печати).

Платонов В. П., Беняш-Кривец В. В.
1. Кольца характеров n-мерных представлений конечнопорожденных групп//ДАН СССР. 1986. Т. 289, № 2. С. 293—297.

Платонов В. П., Бондаренко А. А., Рапинчук А. С.
1. Числа классов алгебраических групп//ДАН СССР. 1979. Т. 245, № 1. С. 26—31.
2. Числа и группы классов алгебраических групп. I//Изв. АН СССР. Сер. мат. 1979. Т. 43, № 3. С. 603—627.
3. Числа и группы классов алгебраических групп. II//Изв. АН СССР. Сер. мат 1980. Т. 44, № 2. С. 395—414.

Платонов В. П., Дракохруст Ю. А.
1. О принципе Хассе для полей алгебраических чисел//ДАН СССР. 1985. Т. 281, № 4. С. 793—797.
2. Норменный принцип Хассе для примарных расширений полей алгебраических чисел//ДАН СССР. 1985 Т. 285, № 4. С. 812—815.

Платонов В. П., Матвеев Г. В.
1. Группы аделей и финитная аппроксимируемость линейных групп относительно сопряженности//ДАН БССР. 1970. Т. 14, № 9. С. 777—779.

Платонов В. П., Милованов М. В.
1. Определяемость алгебраических групп арифметическими подгруппами// ДАН СССР. 1973. Т. 209, № 1. С. 43—46.

Платонов В. П., Рапинчук А. С.
1. О группе рациональных точек трехмерных групп//ДАН СССР. 1979. Т. 247, № 2. С. 279—282.

2. Мультипликативная структура тел над числовыми полями и принцип Хассе//ДАН СССР. 1982. Т. 266, № 3. С. 560—564.
3. Алгебраические группы//Итоги науки и техники. Т. 21. Алгебра. Топология. Геометрия. — М.: ВИНИТИ, 1983. С. 80—134.
4. Мультипликативная структура тел над числовыми полями и нормежный принцип Хассе//Тр. Матем. ин-та АН СССР. 1984. Т. 165. С. 171—187.

Платонов В. П., Тавгень О. И.
1. К проблеме Гротендика о проконечных пополнениях групп//ДАН СССР. 1986. Т. 288, № 5. С. 1054—1058.
2. Grothendiek's Problem on Profinite completions and Representations of Groups//K-theory. 1990. V. 4, N 1.

Платонов В. П., Черноусов В. И.
1. О рациональности канонических спинорных многообразий//ДАН СССР. 1980. Т. 252, № 4. С. 796—800.

Платонов В. П., Шаромет А. А.
1. О конгруэнц-проблеме для линейных групп над арифметическими кольцами//ДАН БССР. 1972. Т. 16, № 5. С. 393—396.

Платонов В. П., Янчевский В. И.
1. Структура унитарных групп и коммутант простой алгебры над глобальными полями//ДАН СССР. 1973. Т. 208, № 3. С. 541—544.
2. О гипотезе Хардера//ДАН СССР. 1975. Т. 221, № 4. С. 784—787.
3. О гипотезе Кнезера — Титса для унитарных групп//ДАН СССР. 1975. Т. 225, № 1. С. 48—51.
4. К теории гензелевых тел//ДАН СССР. 1987. Т. 297, № 2. С. 294—298.
5. Конечномерные гензелевы тела//ДАН СССР. 1987. Т. 297, № 3. С. 542—546.

Плескен (Plesken W.)
1. Finite unimodular groups of prime degree and circulants//J. Algebra. 1985. V. 97, N 1. P. 286—312.

Прасад (Prasad G.)
1. Strong approximation for semi-simple groups over function fields//Ann. of Math. 1977. V. 105, N 3. P. 553—572.
2. Non-vanishing of the first cohomology//Bull. Sci. Math. France. 1977. T. 105, N 4. P. 415—418.
3. A variant of a theorem of Calvin Moore//C. r. Acad. Sci. Paris. 1986. T. 302, ser. 1, N 11. P. 405—408.
4. Volumes of S-arithmetic quotients of semi-simple groups//Publ. Math. I. H. E. S. 1989. V. 69. P. 91—117.

Прасад, Рагунатан (Prasad G., Ragunathan M. S.)
1. Tame subgroup of a semi-simple group over a local field//Amer. J. Math. 1983. V. 105, N 4. P. 1023—1048.
2. On the congruence subgroup problem: Determination of the metaplectic kernel//Invent. Math. 1983. V. 71, N 1. P. 21—42.
3. Topological central extensions of semi-simple groups over local fields// Ann. Math. 1984. V. 119, N 1—2. P. 143—268.
4. On the Kneser-Tits problem//Comment. math. helv. 1985. V. 60, N 1. P. 107—121.
5. Topological central extensions of $SL_1(D)$//Invent. Math. 1988. V. 92, N 4. P. 645—689.

Пятецкий-Шапиро И. И.
1. Арифметические группы в комплексных областях//Успехи мат. наук, 1964. Т. 19, № 6. С. 93—121.
2. Автоморфные функции и арифметические группы//Труды Междунар. конгр. матем. 1966. — М.: Мир, 1968. С. 232—247.

Рагунатан (Raghunathan M. S.)
1. Cohomology of arithmetic subgroups of algebraic groups I.//Ann. of Math. 1967. V. 86, N 3. P. 409—424.
2. Cohomology of arithmetic subgroups of algebraic groups II.//Ann. of Math. 1968. V. 87, N 2. P. 279—304.

3. A note on quotients of real algebraic groups by arithmetic subgroups// Invent. math. 1968. V. 4. P. 318—335.
4. On the congruence subgroup problem//Publ. Math. I. H. E. S. 1976. V. 46. P. 107—161.
5. Дискретные подгруппы групп Ли. — М.: Мир, 1977.
6. On congruence subgroup problem II//Invent. Math. 1986. V. 85, N 1. P. 73—117.
7. On the group of norm 1 elements in a division algebra//Math. Ann. 1988. V. 279. P. 457—484.

Радтке (Radtke W.)
1. Diskontinuierliche arithmetische Gruppen im Funktionenkörperfall//J. reine und angew. Math 1985. B. 363. S. 191—200.

Рапинчук А. С.
1. К гипотезе Платонова о роде в арифметических группах//ДАН БССР. 1981. Т. 25, № 2. С. 101—104.
2. Числа классов в роде квадратичных форм и алгебраические группы// Изв. АН СССР. Сер. мат. 1981. Т. 43, № 4. С. 775—792.
3. О метаплектическом ядре для анизотропных групп//ДАН БССР. 1985. Т. 29, № 12. С. 1068—1071.
4. Метаплектическое ядро для группы SL(1, D)//ДАН БССР. 1986. Т. 30, № 3. С. 197—200.
5. Принцип Хассе для симметрических пространств//ДАН БССР. 1987. Т. 31, № 9. С. 773—776.
6. Мультипликативная арифметика алгебр с делением над числовыми полями и метаплектическая проблема//Изв. АН СССР. Сер. мат. 1987. Т. 51, № 5. С. 1033—1064.
7. О конечной определяемости приведенных норм в простых алгебрах// ДАН БССР. 1988. Т. 32, № 1. С. 5—8.
8. Конгруэнц-проблема для алгебраических групп и сильная аппроксимация в аффинных многообразиях//ДАН БССР. 1988. Т. 32, № 7. С. 581—584.
9. О конгруэнц-проблеме для алгебраических групп//ДАН СССР. 1989. Т. 306, № 6. С. 1304—1307.

Ремесленников В. Н.
1. Финитная аппроксимируемость групп относительно сопряженности//Сиб. мат. ж. 1971. Т. 12, № 5. С. 1085—1099.

Рим (Riehm C.)
1. The norm 1 group of p-adic division algebra//Amer. J. Math. 1970. V. 92, N 2. P. 499—523.
2. The congruence subgroup problem over local fields//Amer. Math. J. 1970. V. 92, N 3. P. 771—778.

Ричардсон (Richardson R.)
1. Conjugacy classes in Lie algebras and algebraic groups//Ann. Math. 1967. V. 86, N 1. P. 1—15.

Ройтер А. В.
1. О целочисленных представлениях, принадлежащих одному роду//Изв. АН СССР. Сер. матем. 1966. Т. 30, № 6. С. 1315—1324.

Рольфс (Rohlfs J.)
1. Arithmetische definierte Gruppen mit Galois-operation//Invent. Math. 1978. V. 4, N 2. P. 185—205.
2. Über maximale arithmetische definierte Gruppen//Math. Ann. 1978. Bd 234, N 3. S. 239—252.
3. Die maximalen arithmetische definierten Untergruppen zerfallender einfacher Gruppen//Math. Ann. 1979. Bd 244. S. 219—231.
4. On the cuspidal cohomology of the Bianchi modular groups. Math. Z. 1985. Bd 188, N 2. S. 253—269.

Рубин (Rubin K.)
1. Tate — Shafarevich groups and L-functions of elliptic curves with complex multiplication//Invent. Math. 1987. V. 89, N 3, P. 527—560.

Сансюк (Sansuc J.-J.)
1. Groupe de Brauer et arithmetique des groupes algebriques lineaires sur un corps de nombres.//J. reine und angew. Math. 1981. Bd 327. S. 12—80.
2. Principle de Hasse, surfaces cubiques et intersections de deux quadriques//Asterisque. 1987. N. 147--148. P. 183—207.

Саркисян Р. А.
1. Об одной проблеме равенства для когомологий Галуа//Алгебра и логика. 1980. Т. 19, № 6. С. 707—725.
2. Алгоритмические вопросы для линейных алгебраических групп. I// Мат. сб. 1980. Т. 113, № 2. С. 179—216.
3. Алгоритмические вопросы для линейных алгебраических групп. II//Мат. сб. 1980. Т. 113, № 3. С. 400—436.

Сатаке И.
1. О компактификации фактор-пространств по арифметическим дискретным группам//Математика. 1961. Т. 5, № 4. С. 123—149.
2. Theory of spherical functions on reductive algebraic groups over p-adic fields//Publ. Math. I. H. E. S. 1963. V. 18, P. 1—69.

Свифт, Райнер (Swift J., Reiner D.)
1. Congruence subgroups of matrix groups//Pacif. J. Math. 1956. V. 6, N 3. P. 529—540.

Сейп-Хорникс (Seip-Hornix E. A. M.)
1. Clifford algebras of quadratic quaternion forms. I, II//Indag. Math. 1965. V. 27, N 2. P. 326—363.

Семинар по алгебраическим группам. — М.: Мир, 1973.

Серр (Serre J.-P.)
1. Когомологии Галуа. — М.: Мир, 1968.
2. Groupes de congruence//Semin. Bourbaki (1966—1967) exp. 330 New-York: Benjamin, 1968.
3. Алгебраические группы и поля классов. — М.: Мир, 1968.
4. Алгебры Ли и группы Ли. — М.: Мир, 1969.
5. Cohomologie des groupes discretes//Lect. Notes Math. 1971. V. 244. P. 337—350.
6. Cohomologie des groupes discretes//Ann. Math. Stud. 1971. V. 70. P. 77—169.
7. Проблема конгруэнц-подгрупп для SL_2.//Математика. 1971. Т. 15, № 6. С. 12—45.
8. Курс арифметики. — М.: Мир, 1972.
9. Абелевы l-адические представления и эллиптические кривые. — М.: Мир, 1973.
10. Деревья, амальгамы и SL_2//Математика. 1974. Т. 18, № 1. С. 3—51; 1974. Т. 18, № 2. С. 3—27.
11. Когомологии дискретных групп//Математика. 1974. Т. 18, № 3. С. 123—144; 1974. Т. 18, № 4. С. 3—33.
12. Arithmetic groups//London Math. Soc. Lect. Notes Ser. 1979. V. 36. P. 105—135.

Слаймэн (Sliman M.)
1. Theorie de Mackey pour les groupes adeliques//Asterisque. 1984. N 115. P. 151.
2. Theorie de Mackey pour les groupes adeliques. Decomposition de $L^2(G_A/G_Q)$ et $L^2(G_R/G_Z)$//C. r. Acad. sci. 1984. Ser. I. V. 298, N 12. P. 261—264.

Смайт (Smythe N.)
1. A presentation for group of integer matrices.//Canad. Math. Bull. 1982. V. 25, N 2. P. 215—221.

Спрингер (Springer T. A.)
1. On the equivalence of quadratic forms.//Indag. math. 1959. V. 21. P. 241—253.
2. Linear algebraic groups. — Boston: Birkhäuser, 1981.

3. Conjugacy classes in algebraic groups//Lect. Notes. Math. 1986. N 1185. P. 175—209.

Стейнберг (Steinberg R.)
1. Regular elements of semisimple algebraic groups.//Publ. Math. I. H. E. S. 1965. V. 25. P. 281—312.
2. Endomorphisms of linear algebraic groups//Mem. Amer. Math. Soc. 1968. N 80. P. 1—108.
3. Лекции о группах Шевалле. — М.: Мир, 1975.

Сузуки (Suzuki K.)
1. On normal subgroups of twisted Chevalley groups over local rings.// Sci Repts. Tokyo Kyoiku Daigaku. 1977. A13: 366—382. P. 238—249.

Суле (Soule C.)
1. The cohomology of $SL_3(Z)$//Topology. 1978. V. 17. P. 1—22.

Суле, Тезука, Ягита (Soule C., Tezuka M., Yagita N.)
1. Cohomological behaviour of the reduction modulo a prime of $GL_3(Z)$.// J. Pure and Appl. Algebra. 1984. V. 32, N 2. P. 219—229.

Тавгень О. И.
1. Проблема Гротендика в классе разрешимых групп//ДАН БССР. 1987. Т. 31, № 10. С. 873—876.
2. О гипотезах Гротендика и Платонова//ДАН БССР. 1988. Т. 32, № 6. С. 489—492.
3. Конечная ширина арифметических подгрупп Шевалле ранга $\geqslant 2$//ДАН СССР. 1990. Т. 310, № 4. С. 802—806.

Тамагава (Tamagawa T.)
1. On indefinite quadratic forms.//J. Math. Soc. Japan. 1977. V. 29. N 2. P. 355—361.

Тезука, Ягита (Tezuka M., Yagita N.)
1. The cohomology of subgroups of $GL_n(F_q)$//Contem. Math. 1983. V. 19. P. 379—396.

Тейт (Tate J.)
1. The cohomology groups of tori in finite Galois extensions of number fields//Nagoya Math. J. 1966. V. 27. P. 709—719.

Теория алгебр Ли. Топология групп Ли. (Семинар Софус Ли). — М.: ИЛ, 1962.

Титс (Tits J.)
1. Algebraic and abstract simple groups.//Ann. of Math. 1964. V. 80, N 2. P. 313—329.
2. Классификация полупростых алгебраических групп//Математика. 1968. Т. 12, № 2. С. 110—143.
3. Systems generateurs de groupes de congruence//C. r. Acad. Sci. 1976. T. 283, N 9. P. A693—A695.
4. Groupes de Whitehead de groupes algebriques simples sur un corps (d'apres V. P. Platonov et al.)//Sem. Bourbaki. 1977. exp. 505. Lecture Notes in Math. 1978. V. 677. P. 218—236.
5. Reductive groups over local fields//Proc. Symp. Pure Math. Amer. Math. Soc. Providence. 1979. V. 33. P. 29—69.
6. Liescher Gruppen und Algebren. — Berlin: Springer, 1983.

Томанов (Tomanov G. M.)
1. About the multiplicative structure of division algebras over number fields//Докл. Болг. АН 1985. V. 38, N 1. P. 11—14.
2. Sur la structure des groupes algebriques simples de type D_n definis sur des corps de nombres//C. r. Acad. sci. 1988. Ser. I. V. 306, N 15. P. 647—650.
3. On Grunwald-Wang's theorem//J. reine und angew. Math. 1988. Bd 389. 209—220.

Томас (Thomas S.)
1. An identification theorem for the locally finite nontwisted Chevalley groups//Arch. Math. 1983. Bd 40, N 1. S. 21—31.

Уитни (Whitney H.)
1. Elementary structure of real algebraic varieties//Ann. Math. 1957. V. 66, N 3. P. 545—556.
Уолас (Wallace D. I.)
1. Conjugacy class of hyperbolic matrices in SL(n,Z) and ideal classes in an order//Trans. Amer. Math. Soc. 1984. V. 283, N 1. P. 177—184.
Флёге (Flöge D.)
1. Zur Struktur der PSL_2 über einigen imaginär-quadratischen Zahlringen// Math. Z. 1983. Bd 183, N 2. S. 255—279.
Фогтман (Vogtmann K.)
1. Rational homology of Bianchi groups//Math. Ann. 1985. Bd 272, N 3. S. 399—419.
Фуливара (Fuliwara M.)
1. On the strong approximation theorem for the group F_4 and E_6//Sci. Pap. Coll. Gen. Educ. Univ. Tokyo. 1971. V. 21, N 2. P. 123—126.
Хамфрис (Humphreys J. E.)
1. Линейные алгебраические группы. — М.: Наука, 1980.
2. Арифметические группы. — М.: Мир, 1983.
Хардер (Harder G.)
1. Über die Galoiskohomologie halbeinfacher Matrizengruppen. I//Math. Z. 1965. Bd 90, N 5. S. 404—428.
2. Über die Galoiskohomologie halbeinfacher Matrizengruppen. II//Math. Z. 1966. Bd 92, N 5. S. 396—415.
3. Halbeinfacher Gruppenschemata über Dedekindringen//Invent. Math. 1967. V. 4. P. 165—191.
4. Bericht über neure Resultate der Galoiskohomologie halbeinfacher Gruppen//Jahresber. Dtsch. Math. Verein. 1968. Bd 70, N 4. S. 182—216.
5. Minkowskische Reduktiontheorie über Funktionkörpern//Invent. Math. 1969. V. 7, N 1. P. 33—54.
6. Semi-simple group schemes over curves and automorphis functions// Actes Congr. intern. Math. Paris. 1970. V. 2. P. 307—312.
7. A Gauss — Bonnet formula for discrete arithmetically defined groups// Ann. Sci. Ecole Norm. Sup. 1971. V. 4. P. 409—455.
8. Chevalley groups over function fields and automorphic forms//Ann. of Math. 1974. V. 100, N 2. P. 249—306.
9. Формула Гаусса — Бонне для дискретных арифметических групп//Математика. 1974. Т. 18, № 6. С. 20—55.
10. On the cohomology of discrete arithmetically defined groups//Discrete subgroups Lie Groups and Appl. Moduli Pap. Bombay Coll. 1973. Oxford. 1975. P. 129—160.
11. Über die Galoiskohomologie halbeinfacher algebraischer Gruppen//J. reine and angew. Math. 1975. Bd 274—275. S. 125—138.
12. Die Kohomologie S-arithmetischer Gruppen über Funktionenkörpern//Invent. Math. 1977. V. 42. P. 135—175.
Хариш-Чандра, Дик (Harish-Chandra, Dijk D.)
1. Harmonic analysis on reductive p-adic groups//Lect. Notes Math. 1970. N 162. P. 125.
Харрельбрюк (Hurrelbriuk J.)
1. On presentations of $SL_n(Z_s)$. $Z_s = Z\left[\frac{1}{p_1}, \ldots, \frac{1}{p_s}\right]$// Commun. Algebra. 1983. V. 11, N 9. P. 937—947.
Хартсхорн Р.
1. Алгебраическая геометрия. — М.: Мир. 1981.
Хассе (Hasse H.)
1. Über p-adische Schiefkörper und ihre Bedeutung für die Arithmetik Hypercomplexer Zahlsystem//Math. Ann. 1931. Bd 104. S. 495—534.
2. Neue Begründung und Verallgemeinerung der Theorie des Normrestsymbols//J. reine und angew. Math. 1930. Bd 162. S. 134—144.

Хашимото (Hashimoto K.)
1. A formula for the number of semi-simple conjugacy classes in the arithmetic subgroups//Proc. Jap. Acad. 1985. A61, N 2. P. 48—50.
2. On certain elliptic conjugacy classes of the Siegel modular group//Proc. Jap. Acad. 1985. A61, N 3. P. 74—77.
3. Elliptic conjugacy classes of the Siegel modular group and unimodular hermitian forms over the ring of cyclotomic integers//J. Fac. Sci. Univ. Tokyo. 1986. Sec. IA. V. 33, N 1. P. 57—82.

Хелгасон С.
1. Дифференциальная геометрия и симметрические пространства. — М.: Мир, 1964.

Хелм (Helm P.)
1. Linear groups: On non-congruence subgroups and presentations//Bull. Austral. Math. Soc. 1982. V. 26, N 3. P. 477—778.

Херстейн Н.
1. Некоммутативные кольца. — М.: Мир, 1972.

Хидзиката (Hijikata H.)
1. Hasse's principle on quaternionic anti-hermitian forms//J. Math. Soc. Japan. 1963. V. 75, N 2. P. 165—175.
2. On the structure of semisimple algebraic groups over valuation fields. I// Jap. J. Math. New ser. 1975. V. 1, N 2. P. 225—300.

Хохшильд (Hochschild G.)
1. Basic theory of algebraic group and Lie algebras. — New York: Springer, 1981.

Хупперт (Huppert B.)
1. Endliche Gruppen. I. — Berlin, 1967.

Хюрлиман (Hürlimann W.)
1. On algebraic tori of norm type//Comment. Math. Helv. 1984. V. 59, N 4. P. 539—549.

Циммерт (Zimmert R.)
1. Zur SL_2 der ganzen Zahlen eines imaginarquadratischen Zahlkörpers// Invent. Math. 1973. V. 19, P. 73—82.

Цукер (Zucker St.)
1. Hodge theory and arithmetic groups//Asterisque. 1983. N. 101—102. P. 365—381.

Чейхал (Chahal J. S.)
1. Solution of the congruence subgroup problem for solvable algebraic group//Nagoya Math. J. 1980. V. 79. P. 141—144.
2. Arithmetic subgroups of algebraic groups//Indiana Univ. Math. J. 1984. V. 33, N 6. P. 799—804.

Черноусов В. И.
1. О рациональности спинорных многообразий над полем рациональных чисел//ДАН БССР. 1981. Т. 25, № 4. С. 293—296.
2. О рациональности групповых компактных многообразий классического типа//ДАН БССР. 1983, Т. 27, № 12. С. 1061—1064.
3. О проективной простоте алгебраических групп, разложимых над квадратичным расширением основного поля//ДАН СССР. 1987. Т. 296, № 6. С. 1301—1305.
4. О структуре групп рациональных точек алгебраических групп типа D_l// ДАН БССР. 1987. Т. 31, № 7. С. 593—596.
5. О проективной простоте некоторых групп рациональных точек над полями алгебраических чисел//Изв. АН СССР. Сер. мат. 1989. Т. 53, № 2, С. 398—410.
6. О принципе Хассе для групп типа E_8//ДАН СССР. 1989. Т. 306, № 25. С. 1059—1063.

Шарлау (Scharlau W.)
1. Quadratic and hermitian forms. — Berlin — Heidelberg — New-York: Springer, 1985

Шаромет А. А.
1. Конгруэнц-проблема для разрешимых алгебраических групп над глобальными полями положительной характеристики//ДАН БССР. 1987. Т. 31, № 3. С. 201—204.
Шафаревич И. Р.
1. Основы алгебраической геометрии: В 2-х т. — М.: Наука, 1988.
Шахер (Schaher M.)
1. Subfields of division rings. I//J. Algebra. 1968. V. 9, N 4. P. 451—477.
Швермер (Schwermer J.)
1. Kohomologie arithmetische definierter Gruppen und Eisensteinreihen//Lect. Notes Math. 1983. V. 988. 170 p.
2. On arithmetic quotients on the Siegel upper half space of degree two// Compos. math. 1986. V. 58, N 2. P. 233—258.
Швермер, Фогтман (Schwermer J., Vogtmann K.)
1. The integral homology of SL_2 and PSL_2 of euclidean imaginary quadratic integers//Comment. math. helv. 1983. V. 58, N 4. P. 573—598.
Шевалле (Chevalley C.)
1. Теория групп Ли: В 3 т. Т. 1. — М.: ИЛ, 1948. Т. 2, 3 — М.: ИЛ, 1958.
2. Deux theoremes d'arithmetiques//J. Math. Soc. Japan. 1951. V. 3, N 1. P. 36—44.
3. On algebraic group varieties//J. Math. Soc. Japan. 1954. V. 6. N 3—4. P. 303—324.
4. О некоторых простых группах//Математика. 1958. Т. 2, № 1. С. 3—58.
Шимизу (Shimizu A.)
1. On complex tori with many endomorphisms//Tsukuba J. Math. 1984. V. 8, N 2. P. 297—318.
Шимура (Shimura G.)
1. Arithmetic of unitary groups//Ann. of Math. 1964. V. 79. P. 369—409.
2. Введение в арифметическую теорию автоморфных функций. — М.: Мир, 1973.
Шинцель (Schinzel A.)
1. Hasse's principle for systems of ternary quadratic forms and for one biquadratic form//Stud. math. 1983. V. 77, N 2. P. 103—109.
Шир (Shyr J.-M.)
1. On some class number relations of algebraic tori//Mich Math. J. 1977. V. 24, N 3. P. 365—377.
2. A generalization of Dirichlet's unit theorem//J. Number Theory. 1977. V. 9, N 2. P. 213—217.
Шпех (Spech B.)
1. Unitary representations of $SL(n, R)$ and the cohomology of congruence subgroups//Lect. Notes Math. 1981. V. 880. P. 4—505.
Штотер (Stothers W. W.)
1. Level and index in the modular group//Proc. Roy. Soc. Edinbourgh. 1984. V. A99, N 1—2, P. 115—126.
Штулер (Stuhler U.)
1. Zur Frage der endlichen Präsentierbarkeit gewisser arithmetischer Gruppen in Funktionenkörperfall//Math. Ann. 1976. Bd 224. S. 217—232.
2. Homological properties of certain arithmetic groups in the function field case//Invent. Math. 1980. V. 57, N 3. P. 263—281.
3. On the cohomology of SL_n over rings of algebraic functions//Lect. Notes Math. 1982. V. 967. P. 316—359.
4. Über die Faktorkommutatorgruppe der Gruppen $SL_2(Q)$ im Funktionenkörperfall//Arch. Math. 1984. Bd 42, N 4. S. 314—324.
5. Über die Kohomologie einiger arithmetischer Varietäten//Math. Ann. 1986. Bd 273, N 4. S. 685—699.

Шур (Schur I.)
1. Über die Darstellung der symmetrischen und der alternierenden Gruppen durch gebrochene lineare Substitutionen//J. reine und angew. Math. 1911. Bd 139. S. 155—250.
Эйхлер (Eichler M.)
1. Allgemeine Kongruenzklassenteilungen der Ideal einfacher Algebren über algebraischen Zahlkörpern und ihre L-Reihen//J. reine und angew. Math. 1938. Bd 179. S. 227—251.
2. Quadratische Formen und Orthogonale Gruppen. — Berlin: Springer, 1952.
3. Zur Zahlentheorie der quaternionen Algebren//J. reine und angew. Math. 1955. Bd 195, N 3—4. S. 127—151.
Эйчи (Eiichi A.)
1. Generation of some discrete subgroups of simple algebraic groups//Tohoku Math. J. 1965. V. 17, N 2. P. 178—184.
Эльстродт, Грюневальд, Меннике (Elstrodt J., Grunewald F., Mennicke J.)
1. PSL(2) over imaginary quadratic integers//Asterisque. 1982. N 94. P. 43—60.
2. On the group PSL (2, Z [i])//London Math. Soc. Lect. Note Ser. 1982. N 56. P. 255- 283.
Эрмит (Hermite C.)
1. Oeuvres completes. T. 1. — Paris: Gauthier-Villars, 1905.
Эрнест (Earnest A. G.)
1. Partitionings of a genus of quadratic forms//J. Number Theory. 1982. V. 14, N 1. P. 1—8.
Эрнест, Сия (Earnest A. G., Hsia J. G.)
1. Springer-type theorems for spinor genera of quadratic forms//Bull. Amer. Math. Soc. 1975. V. 81, N 5. P. 942—943.
2. Spinor genera under field extensions//Acta arithm. 1977. V. 32, N 2. P. 115—128.
Янчевский В. И.
1. Коммутанты простых алгебр с сюръективной приведенной нормой// ДАН СССР. 1975. Т. 221, № 5. С. 1056—1058.
2. Приведенная унитарная K-теория тела над генселевыми дискретно нормированными полями//Изв. АН СССР. Сер. Мат. 1978. Т. 42, № 4. С. 879—918.
3. Приведенная унитарная K-теория. Приложения к алгебраическим группам//Матем. сб., 1979. Т. 110, № 4. С. 579—596.

ОСНОВНЫЕ ОБОЗНАЧЕНИЯ

K^* (соответственно K^+) — мультипликативная (соответственно аддитивная) группа поля K.

V^K — множество всех попарно неэквивалентных нормирований числового поля K

V_f^K (соотв. V_∞^K) — подмножество неархимедовых (соответственно архимедовых) нормирований в V^K

K_v — пополнение числового поля K относительно нормирования $v \in V^K$

$\mathcal{O}_v$ — кольцо целых v-адических чисел (для $v \in V_f^K$)

$\mathfrak{p}_v$ — идеал нормирования в $\mathcal{O}_v$

U_v — группа v-адических единиц

$\mathcal{O}$ — кольцо целых числового поля K

$\mathcal{O}(S)$ — кольцо S-целых числового поля K (для конечного подмножества $S \subset V^K$, содержащего V_∞^K)

$w|v$ — продолжение нормирования

A — кольцо аделей

$A(S)$ — кольцо S-целых аделей

$A(\infty)$ — кольцо целых аделей

A_S — кольцо S-аделей

A_f — кольцо конечных аделей

$A_S(T)$ — кольцо T-целых S-аделей (для $T \supset S$)

J_K — группа иделей

J_K^∞ — группа целых иделей

J_K^S — группа S-целых иделей

h_K — число классов идеалов поля K

$\mathrm{Br}(K)$ — группа Брауэра поля K

$\mathrm{N}_{L/K}$ (соответственно $\mathrm{Tr}_{L/K}$) — норма (соответственно след) в конечном расширении L/K

$\mathrm{Nrd}_{D/K}$ (соответственно $\mathrm{Trd}_{D/K}$) — приведенная норма (соответственно приведенный след)

F_p — поле из p элементов

$\mathbf{Z}$ — (соответственно $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Q}_p$) кольцо целых (соответственно поле рациональных действительных, комплексных и p-адических) чисел

$\mathbf{A}^n$ (соответственно $\mathbf{P}^n$) — n-мерное аффинное (соответственно проективное) пространство

$\boldsymbol{G}_m$ — одномерный K-разложимый тор

$\boldsymbol{G}_a$ — одномерная связная унипотентная группа

$SL_n(D)$, $SU_m(D, f)$ — классические группы над телами

$\boldsymbol{SL}_n(D)$, $\boldsymbol{SU}_m(D, f)$ — соответствующие алгебраические группы

$\boldsymbol{R}_{L/K}$ — функтор ограничения основного поля

$\mathbf{X}(G)$ — группа характеров алгебраической группы G

$\mathbf{X}_*(G)$ — группа кохарактеров (однопараметрических подгрупп)

$R(T, G)$ — система корней алгебраической группы G относительно тора T

$W(T, G)$ — группа Вейля алгебраической группы G относительно тора T

$\mathfrak{g} = L(G)$ — алгебра Ли алгебраической группы G

U_α — одномерная унипотентная подгруппа, отвечающая корню $\alpha \in R(T, G)$

G_α — соответствующая корневая подгруппа

$\mathscr{T}$ — многообразие максимальных торов

$\mathscr{B}$ — многообразие борелевских подгрупп

$R(\Gamma, G)$ — многообразие представлений конечнопорожденной группы Γ в алгебраическую группу G

$R_n(\Gamma)$ — многообразие n-мерных представлений

$X_n(\Gamma)$ — многообразие n-мерных характеров

$T_x(X)$ — касательное пространство к многообразию X в точке x

$d_x f$ — дифференциал морфизма f в точке x

$\operatorname{rang} G$ — (абсолютный) ранг группы G

$\operatorname{rang}_K G$ — ранг группы G над K (K-ранг)

$\operatorname{rang}_S G = \sum_{v \in S} \operatorname{rang}_{K_v} G$ — S-ранг группы G (для конечного подмножества $S \subset V^K$)

G_K — группа K-точек алгебраической K-группы G

$G_{\mathcal{O}}$ — группа целых точек

$G_{\mathcal{O}(S)}$ — группа S-целых точек

$G_{\mathcal{O}}^L$ — группа целых точек относительно решетки $L \subset K^n$

$G_{\mathcal{O}_v}^{L_v}$ — группа целых v-адических точек относительно локальной решетки $L_v \subset K_v^n$

G_A — группа аделей

$G_{A(\infty)}$ — группа целых аделей

$G_{A(\infty)}^L$ — группа целый аделей относительно решетки $L \subset K^n$

$G_{A(S)}$ — группа S-целых аделей

G_{A_S} — группа S-аделей

$G_{A_S(T)}$ — группа T-целых S-аделей

$G_S = \prod_{v \in S} G_{K_v}$, $G_\infty = G_{V_\infty^K}$

$\operatorname{cl}(G)$ — число классов алгебраической группы G

$\operatorname{cl}(G^L)$ — число классов в реализации, задаваемой решеткой $L \subset K^n$

$\mathscr{G}\operatorname{cl}(G)$ — группа классов полупростой алгебраической группы G некомпактного типа

$\mathrm{cl}(a)$ — класс элемента a

$\mathrm{gen}(a)$ — род элемента a

$f_0(a)$ — число классов в роде элемента a

$H^i(G, A)$ — i-я группа (в некоммутативном случае — i-е множество) когомологий

$H^i(L/K, G) = H^i(\mathrm{Gal}(L/K), G_L)$ — i-я группа (множество) когомологий Галуа алгебраической K-группы G, связанная с расширением L/K

$H^i(K, G) = H^i\left(\mathrm{Gal}(\overline{K}/K), G_{\overline{K}}\right)$ ($\overline{K}$ — алгебраическое замыкание поля K)

$\widehat{H}^i(G, A)$ — i-я группа когомологий Тейта

Res — гомоморфизм ограничения

Cor — гомоморфизм коограничения

$\varprojlim$ — проективный предел

$\varinjlim$ — индуктивный предел

A^G — множество G-инвариантных элементов G-модуля A

$G(a)$ — стабилизатор элемента a относительно действия группы G

Ga — орбита элемента a

$[X]$ — мощность множества X

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Автоморфизм Фробениуса 15
Адели 20, 271
Аделизация морфизма 272
Алгебра Ли алгебраической группы 64
— — аналитической группы 135
Алгебраическая группа 60—61
— — анизотропная 80
— — диагонализируемая 66
— — изотропная 80
— — квазиразложимая 72
— — компактного типа 231, 256
— — K-определенная 62
— — K-разложимая 72
— — односвязная 77
— — полупростая 72
— — — некомпактного типа 231, 256
— — — смешанного типа 231, 256
— — присоединенная 77
— — простая 77
— — разрешимая K-разложимая 71
— — редуктивная 72
— — унипотентная 70
Аналитическая структура 129—130
Анизотропное ядро 82
Аппроксимация сильная для алгебраической группы 279, 466
— — для многообразия 436
— — — — абсолютная 436
— — — поля 24
— слабая для алгебраической группы 452—465
— — для многообразия 436
— — — поля 24

Базис Шевалле 78
Бирациональный изоморфизм 114
BN-пара 172

Выделенная вершина 81

Гильбертово поле классов 482
Гипотеза Кнезера—Титса 39, 443
Гипотеза Маргулиса 554
— Платонова о проективной простоте 552
— — об арифметичности 477
Гомоморфизм инфляции 29
— кограничный 33
— коограничения 30
— ограничения 29
— трансгрессии 30
Группа аделей 278
— — главных 278
— — конечных 279
— — S-целых 278
— — целых 279
— арифметическая 195, 255
— Брауэра 39
— Вейля 74, 80, 173
— ветвления 19
— единиц 195
— иделей поля 21
— — главных 22
— — специальных 22
— — S-целых 22
— — целых 22
— инерции 19
— классов алгебраической группы 492
— — идеалов поля 10
— когомологий 26
— — Тейта 333
— компактно определенная 176
— конечных аделей 279
— кохарактеров 67
— ограниченной ширины 229
— ортогональная 96
— проконечная 159
— — типа (F) 349
— разложения 15
— S-аделей 279
— — главных 279
— — T-целых 279
— самосопряженная 144
— S-арифметическая 200, 298

Группа S-единиц 298
— симплектическая 96
— специальная линейная 94
— — ортогональная 96
— — унитарная 100
— спинорная 98
— унимодулярная 184
— унитарная 98, 100
— финитно аппроксимируемая относительно сопряженности 543
— характеров 66
— Шафаревича—Тейта 315, 357
— Шевалле 80

Действие группы на многообразии 115
Дифференциальная форма 190
— — инвариантная 190
Доминантный морфизм 112

Идеал дробный 10
— нормирования 14
Идели поля 21
Изогения 69, 76
Инвариант тела 41
— простой алгебры 41
— Хассе—Витта 384
Инволюция 98
— второго рода 99
— первого рода 99
— — — второго типа 101
— — — первого типа 101
Индекс ветвления 14
— Витта 98
— простой алгебры 38
— тела 38
— Титса 81—82
Индуцированное множество 36
Интегрирование дифференциальной формы 192—193

Касательное пространство 113, 131
Класс решетки 488
— элемента 484
Классификация K-форм алгебраических групп 91—94
— полупростых алгебраических групп 77—78
Когомологии 26—37
— алгебраических групп 87
— — — вещественные 353
— Галуа 31
— групп аделей 329—332
— — целых v-адических точек 324—329
— неабелевы 31—37
— непрерывные 30
— неразветвленные 327
Когомологии Тейта 333
Когомологическая размерность 375
Кограничное отображение 88
Кольцо аделей 20
— — главных 21
— — конечных 23
— — S-целых 20
— — целых 20
— дедекиндово 10
— нормирования 14
— S-аделей 23
— — T-целых 23
— S-целых элементов 21
Конгруэнц-гипотеза Серра 601
Конгруэнц-подгруппа 43, 155, 197, 598
Конгруэнц-проблема 598
Конгруэнц-теорема 569
Конгруэнц-топология 600
Конгруэнц-ядро 600
Корневая подгруппа 388, 592
Критерий Малера 238
— компактности факторпространства $G_{\mathbf{R}}/G_{\mathbf{Z}}$ 237
— — — G_A/G_K 291
— — — $G_S/G_{\mathcal{O}(S)}$ 299
— конечности объема факторпространства $G_{\mathbf{R}}/G_{\mathbf{Z}}$ 240
— — — — G_A/G_K 295
— — — — $G_S/G_{\mathcal{O}(S)}$ 299
— свободы решетки 482

Лемма Гензеля 165
— Краснера 350
— —, унитарный вариант 400
— Минковского 261, 534
— о замкнутых орбитах 116
— Шапиро 30, 36
Локально-глобальный принцип (принцип Хассе) 24—25
— — для алгебраических групп 317
— — — когомологий арифметических групп 532
— — — односвязных алгебраических групп 317
— — — полуторалинейных форм 381—382
— — — — — сильный 382
— — — — — слабый 382
— — — торов 315, 340
— — мультинорменный 346
— — норменный 25, 340—346
L/K-форма 82

Мера 182—194
— борелевская 183
— инвариантная 183
— на произведении 184

Мера на факторпространстве 186—187
— Тамагавы 291
— Хаара 183
Метаплектическое ядро 602
Многомерный класс сопряженности 117
Многообразие борелевских подгрупп 123
— гладкое 114
— K-определенное 112
— представлений 120
— рациональное 114
— торов 121
— унирациональное 115
— характеров 474
Многочлен Эйзенштейна 19
Множители сходимости 291
Модуль автоморфизма 184
— группы 184
Морфизм алгебраических групп 62
— — — K-определенный 62
Мультипликативная арифметика 580
Мультипликатор Шура 28, 344

Накрытие универсальное 77, 92
— специальное 92
Норма приведенная 38
Нормирование поля 10
— — архимедово 11
— — вещественное 13
— — комплексное 13
— — логарифмическое 11
— — неархимедово 11
— — нормализованное 22
— — p-адическое 11
— тела 40
Нормирования эквивалентные 11

Область Зигеля 201
— — обобщенная 252
— — относительная 242
Ограничение основного поля 62
Ограниченное топологическое произведение 185
Определитель Дьедонне 51
Основа 172
Отображение логарифмическое 136
— — усеченное 70
— редукции 165
— экспоненциальное 136
— — усеченное 70

Параметризация Кэли—Диксона 440
Подгруппа арифметическая 195, 255
— Бореля 71
— Ивахори 172
— параболическая 72
Подгруппа параболическая стандартная 76
— парахорическая 172
— S-арифметическая 200, 298
— соизмеримости 233
Поле вычетов 14
— локальное 13—14
— определения 112
— разложения 38, 66
— типа (F) 349
— числовое 9
Пополнение 12
Порядок 54
— локальный 54
— максимальный 54
Последовательность Хохшильда—Серра 30
— — для неабелевых когомологий 36
Препятствие к принципу Хассе 342—344
— — — — первое 342
Приведенная группа Уайтхеда 39
— — — унитарная 446
Принцип Хассе — см. локально-глобальный принцип
Присоединенное представление 65
Проблема Бартельса 341
— Гротендика 474
— рода 535—549
— — в арифметических группах 535
— — для целочисленных представлений 545
— Таннака—Артина 39, 446
Продолжение нормирования 11
Проективная система 159
Проективный предел 159
Про-p-группа 160
— силовская 160
Простая точка редукции 164
Пространство аделей 271
— — главных 272
— — S-целых 272
— — целых 272
Процедура выбрасывания вершин 448
Псевдобазис 54

Радикал 72
— унипотентный 72
Ранг 72
— над K 80
Расширение полей адекватное 341
— — вполне вещественное 258
— — — разветвленное 14
— — неразветвленное 14
Разложение Брюа 74
— Жордана 65

Разложение Жордана аддитивное 65
— Ивасавы в $GL_n(\mathbb{R})$ 150
— — — произвольной группе 152
— Картана 174
— Леви 72
— полярное в $GL_n(\mathbb{R})$ 142
— — — произвольной группе 146
Реализация алгебраической группы 479
Регулярный полупростой элемент 76
Редукция 163, 169
— гладкая 164
Решетка (на векторном пространстве) 53
— локальная 54
— (в локально компактной группе 248
Род решетки 488
— элемента 484

Связная компонента 65
Система корней 73
— — относительная 80
— простых корней 73
— Титса — см. BN-пара
Скручивание 34, 83
Слабая метаплектическая гипотеза 576, 605
Список классических групп 108
Стабилизатор решетки 56, 57
Стандартное описание нормальных делителей 581
Степень алгебраической группы 61
— поля вычетов 14

Тело вычетов 40
Теорема Бартельса—Китаоки 262
— Бера 176
— Бореля о плотности 231
— Бореля—Хариш-Чандры 217
— Ванга 50
— Витта 109
— — для алгебры октав 589
— 90 Гильберта 85
— Дирихле о единицах 236
— — — — обобщенная 311
— инвариантности для арифметических подгрупп 199, 230
— — для S-арифметических подгрупп 301
— Э. Картана 137, 444
— Кнезера 502
— конечности для орбит арифметических групп 218
— — — — групп аделей 287
— — — — S-арифметических групп 300
Теорема конечности для числа классов 280
— — несопряженных конечных подгрупп 199, 302
— Ландера 395
— Ленга 313
— — об изогениях 322
— Маргулиса 560
— Мацумото 161
— Мейера 377
— Минковского—Хассе 25
— Мостова 144, 148
— Накаямы—Тейта локальная 314
— — глобальная 315
— Нётер 165
— о конечной определенности арифметических групп 199, 220
— — — — S-арифметических групп 304
— — неограниченности чисел классов 525
— — реализации 492
— — сильной аппроксимации 24, 466
— — слабой аппроксимации 24, 452—453
— — стабилизаторе 484
— — централизаторе 488
— об обратной функции 129
— — одноклассных решетках 492
— Островского 11
— Платонова 451, 464
— — о слабой аппроксимации над произвольным полем 465
— — — об изогениях 444
— Платонова—Бондаренко—Рапинчука 527
— Платонова—Янчевского 42
— плотности Чеботарева 18
— Прасада—Маргулиса 559
— Прасада—Рагунатана 449, 606
— Рапинчука 613
— Рима 134
— Рольфса 531
— Сколема—Нётер 38
— Стейнберга 372, 376
— Тейта 334, 339, 341
— Титса 443
— Уитни 138
— Фробениуса 320
— Хариш-Чандры 208
— Хассе о нормах 341
— Хассе—Брауэра—Нётер 49
— Черноусова 424
— Шевалле 116
— — усиленная 116
— Эйхлера 50
— —, унитарный вариант 396

Теорема Эрмита 19
Теоремы конечности для когомологий Галуа 326, 348
Теория приведения 200—220
— — для арифметических групп 214
— — — $GL_n(\mathbf{R})$ 200
— — — групп аделей 282—290
— — — S-арифметических групп 298—299
Топология адельная 20, 272
— арифметическая 600
— v-адическая 126
— идельная 21
Тор (алгебраический) 66
— анизотропный 67
— квазиразложимый 68
— мультинорменный 68
— норменный 68
— разложимый 66
Точка простая 114
— особая 114

Униформизующий элемент 14
— — в теле 40

Фактормногообразие 65
Форма внешняя 81
Форма внутренняя 81
— Киллинга 65
Формула произведения 22
Фундаментальная группа алгебраической группы 77
— область 187, 204
Фундаментальное множество 188, 218, 256, 283, 298

Характер 66

Центры простых односвязных групп 79, 366

Число классов алгебраической группы 280, 479
— — в роде 484
— — — — квадратичной формы 486, 502, 515
— — — — решетки 488
— — — — — на $M_n(K)$ относительно сопряженности 505
— — — — целочисленного представления 487
— — — — целочисленной матрицы относительно сопряженности 488
— — идеалов поля 10
— Тамагавы 292, 297

ОГЛАВЛЕНИЕ

Предисловие 5

Глава I. **Алгебраическая теория чисел** 9

§ 1.1. Поля алгебраических чисел, их нормирования и пополнения . . 9
§ 1.2. Адели и идели. Сильная и слабая аппроксимации. Локально-глобальный принцип 20
§ 1.3. Когомологии 26
§ 1.4. Простые алгебры над локальными полями 38
§ 1.5. Простые алгебры над полями алгебраических чисел 49

Глава II. **Алгебраические группы** 60

§ 2.1. Структурные свойства алгебраических групп 60
§ 2.2. Классификация K-форм при помощи когомологий Галуа . . . 82
§ 2.3. Классические группы 94
§ 2.4. Некоторые результаты из алгебраической геометрии 112

Глава III. **Алгебраические группы над локально компактными полями** 125

§ 3.1. Топология и аналитическая структура 125
§ 3.2. Архимедов случай 138
§ 3.3. Неархимедов случай 154
§ 3.4. Элементы теории Брюа — Титса 171
§ 3.5. Необходимые сведения из теории меры 182

Глава IV. **Арифметические группы и теория приведения** 195

§ 4.1. Арифметические группы 195
§ 4.2. Теория приведения (общая схема). Приведение в группе $GL_n(\mathbf{R})$ 200
§ 4.3. Приведение в произвольных группах 214
§ 4.4. Теоретико-групповые свойства арифметических групп . . . 220
§ 4.5. Критерий компактности факторпространства $G_{\mathbf{R}}/G_{\mathbf{Z}}$ 234
§ 4.6. Конечность объема факторпространства $G_{\mathbf{R}}/G_{\mathbf{Z}}$ 240
§ 4.7. Заключительные замечания по теории приведения 251
§ 4.8. Конечные арифметические группы 257

Глава V. **Адели** 271

§ 5.1. Основные определения 271
§ 5.2. Теория приведения для G_A относительно G_K 282
§ 5.3. Критерии компактности и конечности объема факторпространства G_A/G_K 291
§ 5.4. Теория приведения и структурные теоремы для S-арифметических подгрупп 298

Глава VI. **Когомологии Галуа** 312

§ 6.1. Основные результаты 312
§ 6.2. Когомологии алгебраических групп над конечными полями . . 318
§ 6.3. Когомологии Галуа алгебраических торов 332

§ 6.4. Теоремы конечности для когомологий Галуа 348
§ 6.5. Когомологии полупростых алгебраических групп над локальными и числовыми полями 359
§ 6.6. Когомологии Галуа и квадратичные, эрмитовы и другие формы 377
§ 6.7. Доказательство теорем 4 и 6: группы классических типов . . 391
§ 6.8. Доказательство теорем 4 и 6: группы исключительных типов 404

Глава VII. Аппроксимация в алгебраических группах 435
§ 7.1. Сильная и слабая аппроксимация в алгебраических многообразиях 435
§ 7.2. Гипотеза Кнезера — Титса 442
§ 7.3. Слабая аппроксимация в алгебраических группах 452
§ 7.4. Теорема о сильной аппроксимации 466
§ 7.5. Обобщения сильной аппроксимационной теоремы 472

Глава VIII. Числа и группы классов алгебраических групп 478
§ 8.1. Числа классов алгебраических групп и числа классов в роде 479
§ 8.2. Числа и группы классов полупростых групп некомпактного типа. Теорема реализации 489
§ 8.3. Числа классов алгебраических групп компактного типа 511
§ 8.4. Оценки чисел классов редуктивных групп 524
§ 8.5. Проблема рода 535

Глава IX. Нормальное строение групп рациональных точек алгебраических групп 551
§ 9.1. Основные гипотезы и результаты 552
§ 9.2. Группы типа A_n 561
§ 9.3. Группы классических типов 581
§ 9.4. Группы, разложимые над квадратичным расширением 591
§ 9.5. Конгруэнц-проблема (обзор) 597
Дополнение 615

Список литературы 623
Основные обозначения 647
Предметный указатель 650