К.Айерлэнд, М.Роузен

КЛАССИЧЕСКОЕ ВВЕДЕНИЕ В СОВРЕМЕННУЮ ТЕОРИЮ ЧИСЕЛ

М.: Мир, 1987, 416 с.

Учебное пособие по теории чисел, написанное известными математиками из Канады и США. От читателя не требуется предварительных знаний. Авторы начинают с простейших понятий и примеров и доводят изложение до современных проблем и результатов теории чисел. В книге приведено много задач различной трудности вместе с указаниями для их решения.

Для математиков разной квалификации в качестве введения в предмет, для преподавателей и студентов вузов.

ОГЛАВЛЕНИЕ

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ПРЕДИСЛОВИЕ РЕДАКТОРА ПЕРЕВОДА

Теория алгебраических чисел возникла во второй половине XIX в. из целого ряда не связанных друг с другом задач теории чисел. Первое место среди них занимали задачи о диофантовых уравнениях, таких, как уравнение Ферма или вопросы о представимости чисел квадратичными формами. Другой не менее важный круг идей, стимулировавший развитие алгебраической теории чисел — теория делимости и законы разложения простых чисел в кольцах целых алгебраических чисел. Впрочем, отделить друг от друга конкретные факты, идеи и конструкции, приведшие к созданию теории алгебраических чисел, вряд ли возможно. Классический период теории завершается созданием теории полей классов, описывающей абелевы расширения полей алгебраических чисел и законы разложения в них.

Существует много учебных изложений теории алгебраических чисел. Предлагаемая вниманию читателя книга отличается элементарностью и насыщенностью конкретными фактами и примерами. Ряд вопросов, например, кубический и биквадратичный законы взаимности излагаются в учебной литературе с такой степенью подробности, пожалуй, впервые. Помимо основ теории авторы включили в книгу ряд глав, излагающих более современные достижения, связанные с применением методов алгебраической геометрии к диофантовым уравнениям. Сюда относятся определение дзета-функций алгебраических многообразий, гипотеза Римана — Вейля для многообразий над конечными полями, связь группы рациональных точек на эллиптической кривой с ее дзета-функцией. Подробно разобранные частные случаи являются хорошим введением в общую теорию, с которой читатель может познакомиться по сочинениям более общего характера (см. библиографические указания в конце глав).

Последние годы принесли теории чисел заметное оживление: доказана гипотеза Морделла о рациональных точках на кривых рода больше 1, первый случай теоремы Ферма решен для бесконечного числа простых показателей, найдены первые примеры эллиптических кривых с конечной группой Шафаревича. Можно не сомневаться, что книга Айерлэнда и Роузена будет ценным подспорьем для начинающих математиков, желающих принять участие в дальнейшем развитии теории чисел.

А. Н. Паршин

ПРЕДИСЛОВИЕ

Эта книга является пересмотренным и сильно расширенным вариантом нашей книги «Элементы теории чисел», опубликованной в 1972 г. Как и в первой книге, основная аудитория, к которой мы обращаемся, состоит из студентов-математиков старших курсов и аспирантов. Мы предполагаем некоторое знакомство с материалом стандартного курса по абстрактной алгебре. Большую часть гл. 1—11 можно читать даже без такой предварительной подготовки, используя небольшое количество дополнительного материала. Последующие главы предполагают некоторое знание теории Галуа, а для гл. 16 и 18 необходимо знакомство с теорией функций комплексной переменной.

Теория чисел — древний предмет, и содержание его обширно. Для всякой вводной книги следует в силу необходимости произвести очень строгий отбор возможных тем из их громадного многообразия. Мы сосредотачиваемся на темах, связанных с теорией алгебраических чисел и арифметической алгебраической геометрией. Тщательный отбор материала дает нам возможность изложить некоторые довольно сложные вопросы без больших технических приготовлений. Значительная часть этого материала является классической в том смысле, что она была открыта в XIX в. и ранее, но этот материал и современен, так как тесно связан с важными исследованиями, продолжающимися вплоть до настоящего времени.

В гл. 1—5 мы обсуждаем простые числа, однозначное разложение на простые множители, арифметические функции, сравнения и квадратичный закон взаимности. Предварительных знаний здесь требуется очень мало. Удивительно, однако, как малая толика теории групп и колец привносят в излагаемый материал неожиданный порядок. Например, многие разрозненные результаты оказываются частями ответа на естественный вопрос: какова структура группы единиц в кольце $\mathbf{Z}/n\mathbf{Z}$.

Законы взаимности составляют основную тему последующих глав. Квадратичный закон взаимности, красивый сам по себе, является первым в серии, завершающейся законом взаимности Артина — одним из основных достижений теории алгебраических чисел. Выбранный нами путь изложения после биквадратичного

закона взаимности проходит через формулировки и доказательства кубического и биквадратичного законов взаимности. В качестве подготовки к этим вопросам развивается техника теории алгебраических чисел: алгебраические числа и алгебраические целые числа, конечные поля, разложение простых чисел и т. д. Другим важным инструментом в этом исследовании (и в других тоже!) является теория сумм Гаусса и Якоби. Этот материал изложен в гл. 6—9. Далее в этой книге мы формулируем и доказываем более глубокое частичное обобщение этих результатов — закон взаимности Эйзенштейна.

Вторая главная тема — диофантовы уравнения, сначала над конечными полями, а затем над полем рациональных чисел. Обсуждение полиномиальных уравнений начинается в гл. 8 и 10 и достигает кульминации в гл. 11 при изложении части статьи «Число решений уравнений над конечными полями» А. Вейля. Опубликованная в 1948 г., эта статья оказала очень сильное влияние на современное развитие как алгебраической геометрии, так и теории чисел. В гл. 17 и 18 мы рассматриваем диофантовы уравнения над полем рациональных чисел. В гл. 17 излагаются многие стандартные темы, начиная с сумм квадратов и кончая последней теоремой Ферма. Однако, используя предыдущий материал, мы можем трактовать некоторые из этих вопросов с новой точки зрения. Глава 18 посвящена арифметике эллиптических кривых. Она отличается от остальных глав тем, что это в основном обзор, содержащий много определений и утверждений, но мало доказательств. Тем не менее, концентрируя внимание на некоторых важных частных случаях, мы надеемся приобщить читателей к красоте достигнутого в этой области, где проделана большая работа, но осталось много тайн.

Третья (и последняя) из главных тем — дзета-функции. В гл. 11 мы обсуждаем конгруэнц-дзета-функции, связанные с многообразиями над конечными полями. В гл. 16 рассматриваются дзета-функции Римана и L-функции Дирихле. В гл. 18 излагаются результаты о дзета-функциях алгебраических кривых над полем рациональных чисел и L-функциях Гекке. Дзета-функции сводят обширную арифметическую информацию к одной функции и дают возможность применить мощные методы анализа к теории чисел.

На протяжении всей книги мы уделяем большое внимание истории излагаемых вопросов. В замечаниях в конце каждой главы мы приводим краткие исторические справки и ссылки на литературу. Обширная библиография затрагивает многие области, как классические, так и современные. Мы хотим снабдить читателя обильным материалом для дальнейшего изучения.

В книге много упражнений, как стандартных, так и требующих больших усилий. Некоторые из упражнений дополняют

основной текст доказательствами важных результатов. В последних главах ряд упражнений основан на результатах последнего времени. Мы надеемся, что работа над упражнениями будет одновременно как приятной, так и поучительной.

При написании этой книги нам существенно помогли заинтересованность и поддержка многих наших друзей и знакомых — математиков. Мы благодарим всех их. В частности, мы хотели бы выразить признательность Г. Полмэну, настоявшему на том, чтобы мы довели некоторые темы до логического завершения, Д. Госсу, позволившему включить часть его работы в гл. 16, а также О. Макгинессу за полезное содействие при подготовке гл. 18. Мы благодарим также Д. Кавано, Д. Филлипс и особенно К. Ферейру за терпеливую и квалифицированную перепечатку больших кусков рукописи. Наконец, второй из авторов хочет выразить свою признательность «Vaughn Foundation Fund» за финансовую поддержку в течение его годичного отпуска, проведенного в Беркли, Калифорния (1979/1980).

25 *июля* 1981 *г.*

К. Айерлэнд
М. Роузен

Глава 1

ОДНОЗНАЧНОЕ РАЗЛОЖЕНИЕ НА МНОЖИТЕЛИ

Понятие простого числа является основным в теории чисел. Первая часть этой главы посвящена доказательству того, что каждое целое число может быть по существу однозначно представлено в виде произведения простых чисел.

Затем мы докажем аналогичную теорему для кольца многочленов над некоторым полем.

В более абстрактном плане идея однозначного разложения на множители рассматривается для областей главных идеалов.

Наконец, возвращаясь от абстрактного к конкретному, мы прилагаем общую теорию к двум конкретным кольцам, которые будут иметь большое значение в этой книге.

§ 1. Однозначное разложение на множители в Z

В первом приближении теория чисел может быть определена как изучение натуральных чисел 1, 2, 3, 4, ... Кронекер однажды заметил (говоря о математике вообще), что Бог создал натуральные числа, а все остальное — дело рук человеческих. Хотя натуральные числа представляют собой, в некотором смысле, наиболее элементарную математическую систему, изучение их свойств поставило перед поколениями математиков множество завораживающих проблем.

Мы говорим, что натуральное число a *делит* натуральное число b, если существует такое натуральное число c, что $b = ac$. Если b делится на a, то мы пишем $a \mid b$. Например, $2 \mid 8$, $3 \mid 15$, но $6 \nmid 21$. Если задано некоторое натуральное число, то мы пытаемся последовательно разлагать его на множители до тех пор, пока дальнейшее разложение уже будет невозможным. Например, $180 = 18 \times 10 = 2 \times 9 \times 2 \times 5 = 2 \times 3 \times 3 \times 2 \times 5$. Числа, которые не могут быть далее разложены на множители, называются *простыми*. Более точно, мы говорим, что некоторое натуральное число p *простое*, если его делителями являются лишь 1 и p. Простые числа важны потому, что каждое натуральное число может быть представлено в виде произведения простых. Кроме того, простые числа представляют большой интерес еще и потому, что с ними связано большое количество про-

блем, которые легко поставить, но очень трудно разрешить. В самом деле, многие старые проблемы относительно простых чисел не решены до сих пор.

Первыми простыми числами являются 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, ... Можно спросить, бесконечно ли их много? Ответ утвердительный. Изящное доказательство этого факта дал Евклид более 2000 лет назад. Мы изложим его доказательство и некоторые другие в гл. 2. Можно поставить и другие вопросы в том же направлении. Пусть $\pi(x)$ обозначает число простых чисел между 1 и x. Что можно сказать о функции $\pi(x)$? Несколько математиков экспериментально обнаружили, что при больших x функция $\pi(x)$ приближенно равна $x/\ln(x)$. Это утверждение, известное как теорема о простых числах, было доказано к концу XIX в. Адамаром и независимо от него де ла Валле-Пуссеном. Более точно, они доказали, что

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

Даже на небольшом списке простых чисел можно заметить, что они имеют тенденцию появляться парами, как, например, 3 и 5, 5 и 7, 11 и 13, 17 и 19. Бесконечно ли много пар простых чисел? Ответ неизвестен.

Другая знаменитая нерешенная проблема известна как гипотеза Гольдбаха. Можно ли каждое четное число представить в виде суммы двух простых чисел? Гольдбах пришел к этой гипотезе экспериментально. В настоящее время ЭВМ дают возможность экспериментировать с очень большими числами. До сих пор не найдено ни одного противоречащего примера к гипотезе Гольдбаха. Большой прогресс в ее доказательстве был достигнут И. М. Виноградовым и Л. Г. Шнирельманом. В 1937 г. Виноградову удалось показать, что любое достаточно большое нечетное число является суммой трех простых нечетных чисел.

В этой книге мы не будем углубляться в изучение распределения простых чисел или «аддитивных» проблем относительно них (типа гипотезы Гольдбаха). Мы преимущественно будем исследовать, каким образом простые числа входят в мультипликативную структуру чисел. Основная теорема в этом направлении по существу восходит к Евклиду. Это теорема об однозначном разложении на простые множители. Ее иногда называют основной теоремой арифметики, и она достойна такого титула. Почти все результаты, которые будут излагаться, тем или иным способом зависят от нее. В ней утверждается, что каждое целое число может быть разложено в произведение простых чисел единственным образом. О какой единственности идет речь, будет объяснено ниже.

В качестве иллюстрации рассмотрим число 180. Как мы видели, $180 = 2 \times 2 \times 3 \times 3 \times 5 = 2^2 \times 3^2 \times 5$. Единственность

в данном случае означает, что единственными простыми числами, делящими 180, являются 2, 3 и 5 и что показатели степени 2, 2 и 1 однозначно определяются числом 180.

Будем обозначать через **Z** кольцо целых чисел, т. е. множество 0, ± 1, ± 2, ± 3, ... с обычными определениями сложения и умножения. С кольцом **Z** работать будет более удобно, чем с одними лишь положительными целыми числами. Понятие делимости без труда переносится на **Z**. Если p — некоторое положительное простое число, то $-p$ также будет простым числом. Мы не будем считать 1 или -1 простыми числами, хотя они и удовлетворяют определению. Это просто полезное соглашение. Заметим, что 1 и -1 делят каждое число и это единственные целые числа с таким свойством. Они называются *единицами* кольца **Z**. Заметим также, что нуль делится на любое отличное от нуля целое число. Как обычно, мы исключаем деление на нуль.

Имеется несколько простых свойств деления, которые мы только перечислим. При желании читатель может воспроизвести их доказательства.

(1) $a \mid a$, $a \neq 0$.
(2) Если $a \mid b$ и $b \mid a$, то $a = \pm b$.
(3) Если $a \mid b$ и $b \mid c$, то $a \mid c$.
(4) Если $a \mid b$ и $a \mid c$, то $a \mid b + c$.

Пусть $n \in \mathbf{Z}$ и p — некоторое простое число. Если $n \neq 0$, то существует такое неотрицательное целое число a, что $p^a \mid n$ и $p^{a+1} \nmid n$. В этом легко убедиться в случае, когда p и n оба положительны, ибо тогда степени p становятся все больше и больше и в конечном счете превосходят n. Другие случаи без труда сводятся к этому. Число a называется *порядком* числа n в p и обозначается через $\mathrm{ord}_p(n)$. Грубо говоря, $\mathrm{ord}_p(n)$ показывает, какая степень p делит n. Если $n = 0$, то мы полагаем $\mathrm{ord}_p(0) = \infty$. Заметим, что $\mathrm{ord}_p(n) = 0$ тогда и только тогда, когда $p \nmid n$.

Лемма 1. *Каждое ненулевое целое число может быть представлено в виде произведения простых чисел.*

Доказательство. Предположим, что существует число, которое не может быть представлено в таком виде. Пусть N — наименьшее положительное целое число с таким свойством. Так как N само не может быть простым, то $N = mn$, где $1 < m$, $n < N$. Но так как m и n положительны и меньше N, они должны быть произведениями простых чисел. А тогда произведением простых чисел будет и $N = mn$ (противоречие).

Если воспользоваться методом математической индукции, то можно привести более строгое доказательство. Достаточно доказать результат для всех положительных целых чисел. 2 — простое число. Предположим, что $2 < N$ и что результат доказан

для всех целых чисел m, таких, что $2 \leqslant m < N$. Мы хотим доказать, что N является произведением простых чисел. Если N само простое, то доказывать нечего. Если N не простое, то $N = mn$, где $2 \leqslant m, n < N$. По индукции m и n оба будут произведениями простых чисел, а потому таким произведением будет и N. □

Собирая вместе одинаковые простые числа, можно записать $n = p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$, где p_i — простые числа и a_i — неотрицательные целые числа. Мы будем использовать следующую запись:

$$n = (-1)^{\varepsilon(n)} \prod_p p^{a(p)},$$

где $\varepsilon(n) = 0$ или 1 в зависимости от того, будет n положительным или отрицательным, а произведение берется по всем положительным простым числам. Показатели степени $a(p)$ — неотрицательные целые числа и, конечно, $a(p) = 0$ для всех простых чисел, кроме конечного их числа. Например, если $n = 180$, то $\varepsilon(n) = 0$, $a(2) = 2$, $a(3) = 2$ и $a(5) = 1$, а все остальные $a(p)$ равны 0.

Мы можем сформулировать теперь основную теорему.

Теорема 1. *Для любого ненулевого целого числа n имеется разложение на простые множители*

$$n = (-1)^{\varepsilon(n)} \prod_p p^{a(p)}$$

с показателями степени, которые однозначно определяются числом n. На самом деле $a(p) = \operatorname{ord}_p(n)$.

Доказательство этой теоремы не такое простое, как может показаться с первого взгляда. Приведем сначала некоторые вспомогательные результаты.

Лемма 2. *Если a, $b \in \mathbf{Z}$ и $b > 0$, то существуют такие q, $r \in \mathbf{Z}$, что $a = qb + r$, где $0 \leqslant r < b$.*

Доказательство. Рассмотрим множество всех целых чисел вида $a - bx$ с $x \in \mathbf{Z}$. Это множество содержит положительные элементы. Пусть $r = a - qb$ — наименьший неотрицательный элемент этого множества. Мы утверждаем, что $0 \leqslant r < b$. В противном случае $r = a - qb \geqslant b$, а потому $0 \leqslant a - (q+1)b < r$, что противоречит минимальности r. □

Определение. Для $a_1, a_2, \ldots, a_n \in \mathbf{Z}$ определим $(a_1, a_2, \ldots, a_n)$ как множество всех целых чисел вида $a_1x_1 + a_2x_2 + \ldots + a_nx_n$ с $x_1, x_2, \ldots, x_n \in \mathbf{Z}$.

Пусть $A = (a_1, a_2, \ldots, a_n)$. Заметим, что сумма и разность двух элементов из A снова принадлежат A. Кроме того, если $a \in A$ и $r \in \mathbf{Z}$, то $ra \in A$. На языке теории колец A является *идеалом* в кольце $\mathbf{Z}$.

Лемма 3. *Если $a, b \in \mathbf{Z}$, то существует такой элемент $d \in \mathbf{Z}$, что $(a, b) = (d)$.*

Доказательство. Можно считать, что хотя бы один из элементов a, b ненулевой, так что в (a, b) имеются положительные элементы. Пусть d — наименьший положительный элемент в (a, b). Очевидно, что $(d) \subseteq (a, b)$. Мы покажем, что выполняется и обратное включение.

Пусть $c \in (a, b)$. По лемме 2 существуют такие целые числа q и r, что $c = qd + r$ с $0 \leqslant r < d$. Так как c и d входят в (a, b), то $r = c - qd$ также входит в (a, b). Поскольку $0 \leqslant r < d$, то $r = 0$. Таким образом, $c = qd \in (d)$. □

Определение. Пусть $a, b \in \mathbf{Z}$. Целое число d называется *наибольшим общим делителем* целых чисел a и b, если d делит одновременно a и b и каждый другой общий делитель a и b делит d.

Заметим, что если c — некоторый другой наибольший общий делитель a и b, то $c \mid d$ и $d \mid c$, так что $c = \pm d$. Таким образом, наибольший общий делитель двух целых чисел, если он существует, определен с точностью до знака.

В качестве примера можно проверить, что 14 — наибольший общий делитель чисел 42 и 196. Следующая лемма обеспечивает существование наибольшего общего делителя, но в ней не дается метода его вычисления. В упражнениях будет намечен один эффективный метод вычисления, известный как алгоритм Евклида.

Лемма 4. *Пусть $a, b \in \mathbf{Z}$. Если $(a, b) = (d)$, то d является наибольшим общим делителем чисел a и b.*

Доказательство. Так как $a \in (d)$ и $b \in (d)$, мы видим, что d — общий делитель a и b. Предположим, что c — их общий делитель. Тогда c делит каждое число вида $ax + by$. В частности, $c \mid d$. □

Определение. Мы говорим, что два целых числа a и b *взаимно просты*, если их единственными общими делителями являются единицы ± 1.

Стандартным стало использование обозначения (a, b) для наибольшего общего делителя целых чисел a и b. По нашему определению (a, b) — это некоторое множество. Однако ввиду равенства $(a, b) = (d)$ и того, что d — некоторый наибольший общий делитель (если потребовать, чтобы d было положительным, то можно обойтись без слова «некоторый»), использование символа (a, b) в обоих смыслах не должно вносить путаницы. При этом соглашении мы можем сказать, что числа a и b взаимно просты, если $(a, b) = 1$.

Предложение 1.1.1. *Предположим, что* $a \mid bc$ *и что* $(a, b) = 1$. *Тогда* $a \mid c$.

Доказательство. Так как $(a, b) = 1$, то существуют целые числа r и s, для которых $ra + sb = 1$. Поэтому $rac + sbc = c$. Так как a делит левую часть этого равенства, то $a \mid c$. □

Это предложение неверно, если $(a, b) \neq 1$. Например, $6 \mid 24$, но $6 \nmid 3$ и $6 \nmid 8$.

Следствие 1. *Если* p — *простое число и* $p \mid bc$, *то либо* $p \mid b$, *либо* $p \mid c$.

Доказательство. Единственными делителями числа p являются ± 1, $\pm p$. Таким образом, $(p, b) = 1$ или p, т. е. либо $p \mid b$, либо p и b взаимно просты. Если $p \mid b$, то доказательство закончено. Если $p \nmid b$, то $(p, b) = 1$ и, согласно предложению 1.1.1, $p \mid c$. □

Следствие 1 можно сформулировать в слегка измененном виде, который часто бывает полезным: если p — простое число и $p \nmid b$, $p \nmid c$, то $p \nmid bc$.

Следствие 2. *Предположим, что* p — *простое число и* $a, b \in \mathbf{Z}$. *Тогда* $\operatorname{ord}_p ab = \operatorname{ord}_p a + \operatorname{ord}_p b$.

Доказательство. Пусть $\alpha = \operatorname{ord}_p a$, $\beta = \operatorname{ord}_p b$. Тогда $a = p^\alpha c$ и $b = p^\beta d$, где $p \nmid c$ и $p \nmid d$. Далее, $ab = p^{\alpha+\beta} cd$ и, согласно следствию 1, $p \nmid cd$. Таким образом, $\operatorname{ord}_p ab = \alpha + \beta = \operatorname{ord}_p a + \operatorname{ord}_p b$. □

Теперь мы готовы приступить к доказательству основной теоремы.

Применим функцию ord_q к обеим частям равенства

$$n = (-1)^{\varepsilon(n)} \prod_p p^{a(p)}$$

и воспользуемся ее свойством из следствия 2. В результате получим равенство $\operatorname{ord}_q n = \varepsilon(n) \operatorname{ord}_q(-1) + \sum_p a(p) \operatorname{ord}_q(p)$.

Из определения функции ord_q имеем $\operatorname{ord}_q(-1) = 0$ и $\operatorname{ord}_q(p) = 0$ при $p \neq q$ и $\operatorname{ord}_q(p) = 1$ при $p = q$. Таким образом, правая часть сводится к единственному члену $a(q)$, т. е. $\operatorname{ord}_q n = a(q)$, что мы и хотели доказать.

Надо подчеркнуть, что ключевым шагом в доказательстве является следствие 1, а именно, если $p \mid ab$, то $p \mid a$ или $p \mid b$. Вся трудность доказательства концентрируется в этом факте.

§ 2. Однозначное разложение на множители в $k[x]$

Теорема об однозначном разложении на множители может быть сформулирована и доказана в более общем контексте, чем в § 1. В этом параграфе мы рассмотрим кольцо $k[x]$ многочленов с коэффициентами в некотором поле k. В § 3 мы рассмотрим области главных идеалов. Оказывается, что анализ этих случаев будет полезен при изучении целых чисел.

Если $f, g \in k[x]$, то мы говорим, что f делит g, если существует такой многочлен $h \in k[x]$, что $g = fh$.

Если $\deg f$ обозначает степень многочлена f, то $\deg fg = \deg f + \deg g$. Кроме того, напомним, что $\deg f = 0$ тогда и только тогда, когда f — ненулевая константа. Отсюда следует, что $f \mid g$ и $g \mid f$ тогда и только тогда, когда $f = cg$, где c — ненулевая константа. Отсюда получаем также, что единственными многочленами, делящими все другие, будут ненулевые константы. Последние являются единицами[1]) в $k[x]$. Многочлен p, отличный от константы, называется *неприводимым*, если из $q \mid p$ следует, что либо q — константа, либо q отличается от p на мультипликативную константу. Неприводимые многочлены являются аналогами простых чисел.

Лемма 1. *Каждый многочлен, отличный от константы, представляется в виде произведения неприводимых многочленов.*

Доказательство. Применим индукцию по степени многочленов. Очевидно, что многочлены степени 1 неприводимы. Предположим, что наш результат доказан для всех многочленов степени $< n$ и что $\deg f = n$. Если f неприводим, то все доказано. В противном случае $f = gh$, где $1 \leqslant \deg g$, $\deg h < n$. По предположению индукции оба многочлена g и h будут произведениями неприводимых многочленов. Поэтому произведением неприводимых многочленов будет и $f = gh$. □

[1]) См. примечание на стр. 19. — *Прим. перев.*

Удобно ввести в рассмотрение *приведенные* (monic) *многочлены*. Многочлен f называется *приведенным*, если его старший коэффициент равен 1. Например, $x^2 + x - 3$ и $x^3 - x^2 + 3x + 17$ — приведенные многочлены, а $2x^3 - 5$ и $3x^4 + 2x^2 - 1$ — нет. Каждый многочлен (за исключением нуля) отличается от приведенного на мультипликативную константу.

Пусть p — некоторый приведенный неприводимый многочлен. Мы вводим функцию $\operatorname{ord}_p f$ как целое число a, определяемое следующим свойством: $p^a \mid f$, но $p^{a+1} \nmid f$. Такое целое число должно существовать, ибо $\deg p^m$ становится все больше и больше при возрастании m. Заметим, что $\operatorname{ord}_p f = 0$ тогда и только тогда, когда $p \nmid f$.

Теорема 2. *Пусть $f \in k[x]$. Тогда можно записать*

$$f = c \prod_p p^{a(p)},$$

где произведение берется по всем приведенным неприводимым многочленам и c — константа. Константа c и показатели степени $a(p)$ определены многочленом f однозначно; на самом деле $a(p) = \operatorname{ord}_p f$.

Существование такого произведения сразу же следует из леммы 1. Как и раньше, доказательство однозначности труднее и будет отложено до получения вспомогательных фактов.

Лемма 2. *Пусть $f, g \in k[x]$. Если $g \neq 0$, то существуют такие многочлены $h, r \in k[x]$, что $f = hg + r$, где либо $r = 0$, либо $r \neq 0$ и $\deg r < \deg g$.*

Доказательство. При $g \mid f$ положим просто $h = f/g$ и $r = 0$. При $g \nmid f$ пусть $r = f - hg$ будет многочленом наименьшей степени среди всех многочленов вида $f - lg$ с $l \in k[x]$. Мы утверждаем, что $\deg r < \deg g$. Если это не так, то пусть ax^d — старший член в r, а bx^m — старший член в g. Тогда $r - ab^{-1}x^{d-m}g = f - (h + ab^{-1}x^{d-m})g$ имеет меньшую степень, чем r, и заданный вид — противоречие. □

Определение. Если $f_1, f_2, \ldots, f_n \in k[x]$, то $(f_1, f_2, \ldots, f_n)$ — множество всех многочленов вида $f_1h_1 + f_2h_2 + \ldots + f_nh_n$, где $h_1, h_2, \ldots, h_n \in k[x]$.

На языке теории колец $(f_1, f_2, \ldots, f_n)$ — идеал, порожденный многочленами $f_1, f_2, \ldots, f_n$.

Лемма 3. *Для заданных $f, g \in k[x]$ существует такой многочлен $d \in k[x]$, что $(f, g) = (d)$.*

Доказательство. Пусть d — некоторый элемент наименьшей степени в множестве (f, g). Ясно, что $(d) \subseteq (f, g)$, и мы хотим доказать обратное включение. Пусть $c \in (f, g)$. Если $d \nmid c$, то существуют такие многочлены h и r, что $c = hd + r$, где $\deg r < \deg d$. Так как c и d лежат в (f, g), то $r = c - hd \subseteq (f, g)$. Поскольку r имеет меньшую степень, чем d, мы пришли к противоречию. Поэтому $d \mid c$ и $c \in (d)$. □

Определение. Пусть $f, g \in k[x]$. Тогда $d \in k[x]$ называется *наибольшим общим делителем многочленов* f и g, если d делит f и g и каждый общий делитель f и g делит d.

Заметим, что наибольший общий делитель двух многочленов определен с точностью до умножения на константу. Если потребовать, чтобы он был приведенным, то он будет определен однозначно, и мы можем тогда, говоря о наибольшем общем делителе, иметь в виду именно *этот* наибольший общий делитель.

Лемма 4. *Пусть $f, g \in k[x]$. Согласно лемме 3, существует такой многочлен $d \in k[x]$, что $(f, g) = (d)$. Он является одним из наибольших общих делителей многочленов f и g.*

Доказательство. Так как $f \in (d)$ и $g \in (d)$, то $d \mid f$ и $d \mid g$. Предположим, что $h \mid f$ и $h \mid g$. Тогда h делит все многочлены вида $fl + gm$, где $l, m \in k[x]$. В частности, $h \mid d$, и все доказано. □

Определение. Два многочлена f и g называются *взаимно простыми*, если общими делителями для f и g являются лишь константы. Другими словами, $(f, g) = (1)$.

Предложение 1.2.1. *Если f и g взаимно просты и $f \mid gh$, то $f \mid h$.*

Доказательство. Если f и g взаимно просты, то $(f, g) = (1)$, а потому существуют такие многочлены l и m, что $lf + mg = 1$. В таком случае $lfh + mgh = h$. Так как f делит левую часть этого равенства, то он должен делить h. □

Следствие 1. *Если p — неприводимый многочлен и $p \mid fg$, то $p \mid f$ или $p \mid g$.*

Доказательство. Так как p неприводим, то $(p, f) = (p)$ или $(p, f) = (1)$. В первом случае $p \mid f$ и следствие доказано. Во втором случае p и f взаимно просты и результат следует из предложения 1.2.1. □

Следствие 2. *Если p — приведенный неприводимый многочлен и $f, g \in k[x]$, то* $\operatorname{ord}_p fg = \operatorname{ord}_p f + \operatorname{ord}_p g$.

Доказательство. Оно почти дословно совпадает с доказательством следствия 2 предложения 1.1.1. □

Доказательство теоремы 2 теперь не представляет труда. Применив функцию ord_q к обеим частям равенства

$$f = c \prod_p p^{a(p)},$$

получаем

$$\mathrm{ord}_q f = \mathrm{ord}_q c + \sum_p a(p) \mathrm{ord}_q p.$$

Далее, ввиду того, что c — константа, $q \nmid c$ и $\mathrm{ord}_q c = 0$. Кроме того, $\mathrm{ord}_q p = 0$ при $q \neq p$ и $\mathrm{ord}_q p = 1$ при $q = p$. Таким образом, найденное соотношение сводится к $\mathrm{ord}_q f = a(q)$. Это значит, что показатели степени определены однозначно. Очевидно, что если показатели степени однозначно определяются многочленом f, то однозначно определяется и c. Это завершает доказательство. □

§ 3. Однозначное разложение на множители в областях главных идеалов

Читатель, конечно, обратил внимание на большое сходство методов доказательства в § 1 и 2. В этом параграфе мы докажем одну общую теорему, которая содержит предыдущие результаты в качестве частных случаев.

В этом параграфе R будет всюду обозначать некоторую область целостности.

Определение 1. Кольцо R называется *евклидовой областью*, если существует какая-либо функция λ из множества его ненулевых элементов в множество $\{0, 1, 2, 3, \ldots\}$, обладающая следующим свойством: для любых $a, b \in R$, $b \neq 0$, найдутся такие $c, d \in R$, что $a = cb + d$ и либо $d = 0$, либо $\lambda(d) < \lambda(b)$.

Кольца $\mathbf{Z}$ и $k[x]$ оба являются евклидовыми областями. В $\mathbf{Z}$ в качестве функции λ можно взять обычное абсолютное значение; в кольце $k[x]$ нужному условию будет удовлетворять функция, ставящая в соответствие каждому многочлену его степень.

Предложение 1.3.1. *Если R — некоторая евклидова область и $I \subseteq R$ — идеал, то существует такой элемент $a \in R$, что $I = Ra = \{ra \mid r \in R\}$.*

Доказательство. Рассмотрим множество неотрицательных целых чисел $\{\lambda(b) \mid b \in I, b \neq 0\}$. Ввиду того что каждое множе-

ство неотрицательных целых чисел содержит наименьший элемент, существует такой элемент $a \in I$, $a \neq 0$, что $\lambda(a) \leqslant \lambda(b)$ для всех $b \in I$, $b \neq 0$. Мы утверждаем, что $I = Ra$. Очевидно, что $Ra \subseteq I$. Предположим, что $b \in I$; тогда, как мы знаем, существуют такие элементы $c, d \in R$, что $b = ca + d$, где либо $d = 0$, либо $\lambda(d) < \lambda(a)$. Так как $d = b - ca \in I$, не может выполняться неравенство $\lambda(d) < \lambda(a)$. Таким образом, $d = 0$ и $b = ca \in Ra$. Поэтому $I \subseteq Ra$ и предложение доказано. □

Для элементов $a_1, \ldots, a_n \in R$ положим

$$(a_1, a_2, \ldots, a_n) = Ra_1 + Ra_2 + \cdots + Ra_n =$$

$$= \left\{ \sum_{i=1}^{n} r_i a_i \mid r_i \in R \right\}.$$

Множество $(a_1, a_2, \ldots, a_n)$ является идеалом. Если идеал I совпадает с $(a_1, \ldots, a_n)$ для некоторых элементов $a_i \in I$, то говорят, что I *конечно порожден*. Если $I = (a)$ для некоторого $a \in I$, то мы говорим, что I — *главный* идеал.

Определение 2. Кольцо R называется *областью главных идеалов* (ОГИ), если каждый идеал в нем главный.

Предложение 1.3.1 утверждает, что каждая евклидова область будет ОГИ. Обращение этого утверждения неверно, хотя не так просто привести соответствующие примеры.

Оставшаяся часть этого параграфа посвящена ОГИ. Понятие евклидовой области полезно, поскольку на практике можно показать, что многие кольца являются ОГИ, установив сначала, что они — евклидовы области. В § 4 мы приведем еще два примера.

Введем несколько терминов. Если $a, b \in R$, $b \neq 0$, то мы будем говорить, что b *делит* a, если $a = bc$ для некоторого $c \in R$; обозначение: $b \mid a$. Элемент $u \in R$ называется *единицей*[1]), если он делит 1. Два элемента $a, b \in R$ *ассоциированы*, если $a = bu$ для некоторой единицы u. Элемент $p \in R$, не являющийся единицей, называется *неприводимым*, если $a \mid p$ означает, что элемент a — либо единица, либо ассоциирован с p. Неединица $p \in R$ называется *простым* элементом, если $p \neq 0$ и из $p \mid ab$ следует, что $p \mid a$ или $p \mid b$.

---

[1]) Следует помнить, что в этой книге термин «единица» может означать как единичный элемент кольца, группы или поля, так и обратимый элемент кольца. Из контекста всегда бывает ясно, какое его значение имеется в виду. — *Прим. перев.*

Различие между неприводимым и простым элементами является новым. В общем случае эти понятия не совпадают. Как мы видели, они совпадают в $\mathbf{Z}$ и $k[x]$, и мы докажем вскоре, что они совпадают в ОГИ.

Некоторые из обсуждаемых понятий можно перевести на язык идеалов. Так, $a \mid b$ тогда и только тогда, когда $(b) \subseteq (a)$. Элемент $u \in R$ является единицей тогда и только тогда, когда $(u) = R$. Элементы a и b ассоциированы в том и только том случае, если $(a) = (b)$. Простота элемента p эквивалентна тому, что из $ab \in (p)$ вытекает, что либо $a \in (p)$, либо $b \in (p)$. Все эти утверждения суть легкие упражнения. Понятие неприводимого элемента тоже можно сформулировать в терминах идеалов, но это нам не понадобится.

Определение. Элемент $d \in R$ называется *наибольшим общим делителем* (НОД) двух элементов $a, b \in R$, если

(a) $d \mid a$ и $d \mid b$;

b) $d' \mid a$ и $d' \mid b \Rightarrow d' \mid d$.

Как нетрудно убедиться, если оба элемента d и d' суть НОД для элементов a и b, то d и d' ассоциированы.

В произвольном кольце НОД двух элементов не обязательно существует. Однако справедливо следующее утверждение.

Предложение 1.3.2. *Пусть R является* ОГИ *и $a, b \in R$. Тогда элементы a и b имеют наибольший общий делитель d и $(a, b) = (d)$.*

Доказательство. Образуем идеал (a, b). Ввиду того что R есть ОГИ, существует такой элемент d, что $(a, b) = (d)$. Так как $(a) \subseteq (d)$ и $(b) \subseteq (d)$, то $d \mid a$ и $d \mid b$. Если $d' \mid a$ и $d' \mid b$, то $(a) \subseteq (d')$ и $(b) \subseteq (d')$. Поэтому $(d) = (a, b) \subseteq (d')$ и $d' \mid d$. Мы доказали, что d есть НОД элементов a и b и что $(a, b) = (d)$. □

Два элемента a и b называются *взаимно простыми*, если их единственными общими делителями являются единицы.

Следствие 1. *Если R является* ОГИ *и $a, b \in R$ взаимно просты, то $(a, b) = R$.*

Следствие 2. *Если R является* ОГИ *и элемент $p \in R$ неприводим, то p — простой элемент.*

Доказательство. Предположим, что $p \mid ab$ и $p \nmid a$. Так как $p \nmid a$, то их общими делителями будут только единицы. Согласно

следствию 1, $(a, p) = R$. Таким образом, $(ab, pb) = (b)$. Ввиду того что $ab \in (p)$ и $pb \in (p)$, имеем $(b) \subseteq (p)$. Итак, $p \mid b$. □

Нетрудно убедиться в том, что простой элемент неприводим. Начиная с этого места, кольцо R будет ОГИ, и мы используем термины *простой* и *неприводимый* как синонимы.

Наша цель — показать, что каждый ненулевой элемент из R представляется в виде произведения неприводимых элементов. Доказательство проводится в два этапа. Сначала мы покажем, что для заданного элемента $a \in R$, $a \neq 0$, существует неприводимый элемент, делящий a. Затем мы убедимся в том, что элемент a представляется в виде произведения неприводимых элементов.

Лемма 1. *Пусть* $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \ldots$ *— возрастающая цепь идеалов. Тогда существует такое целое число* k, *что* $(a_k) = (a_{k+l})$ *для* $l = 0, 1, 2, \ldots$. *Другими словами, цепь обрывается после конечного числа шагов.*

Доказательство. Пусть $I = \bigcup_{i=1}^{\infty} (a_i)$. Нетрудно убедиться в том, что I — идеал. Таким образом, $I = (a)$ для некоторого $a \in R$. Но поскольку $a \in \bigcup_{i=1}^{\infty} (a_i)$, то $a \in (a_k)$ при некотором k, откуда следует, что $I = (a) \subseteq (a_k)$. Значит, $I = (a_k) = (a_{k+1}) = \ldots$. □

Предложение 1.3.3. *Каждый ненулевой элемент из* R, *не являющийся единицей, представляется в виде произведения неприводимых элементов.*

Доказательство. Пусть $a \in R$, $a \neq 0$, a — не единица. Прежде всего мы хотим показать, что a делится на некоторый неприводимый элемент. Если сам a неприводим, то мы получили то, что хотели. В противном случае $a = a_1 b_1$, где a_1 и b_1 — не единицы. Если a_1 неприводим, то опять получено то, что было нужно. В противном случае $a_1 = a_2 b_2$, где a_2 и b_2 — не единицы. Если a_2 неприводим, то мы опять получили то, что хотели. В противном случае продолжаем рассуждение, как прежде. Заметим, что $(a) \subset (a_1) \subset (a_2) \subset \ldots$. Согласно лемме 1, эта цепь не может быть бесконечной. Таким образом, при некотором k элемент a_k неприводим.

Теперь мы покажем, что элемент a представляется в виде произведения неприводимых элементов. Если a сам неприводим, то мы получили, что хотели. В противном случае пусть p_1 — такой неприводимый элемент, что $p_1 \mid a$. Тогда $a = p_1 c_1$. Если c_1 — единица, то нужное разложение получено. В противном

случае пусть p_2 — такой неприводимый элемент, что $p_2 \mid c_1$. Тогда $a = p_1 p_2 c_2$. Если c_2 — единица, то опять искомое разложение найдено. В противном случае продолжаем рассуждение, как прежде. Заметим, что $(a) \subset (c_1) \subset (c_2) \subset \ldots$. Эта цепь не может продолжаться бесконечно ввиду леммы 1. Таким образом, при некотором k имеем $a = p_1 p_2 \ldots p_k c_k$, где c_k — единица. Так как $p_k c_k$ неприводим, доказательство предложения закончено. □

Мы хотим теперь определить функцию ord, как это уже было сделано в § 1 и 2.

Лемма 2. *Пусть p — некоторый простой элемент и $a \neq 0$. Тогда существует такое целое число n, что $p^n \mid a$, но $p^{n+1} \nmid a$.*

Доказательство. Если бы утверждение леммы не выполнялось, то для каждого целого числа $m > 0$ существовал бы такой элемент b_m, что $a = p^m b_m$. Тогда $p b_{m+1} = b_m$ и последовательность $(b_1) \subset (b_2) \subset (b_3) \subset \ldots$ была бы бесконечной возрастающей цепью идеалов, которая не обрывалась бы. Это противоречит лемме 1. □

Целое число n, определенное в лемме 2, однозначно определяется элементами p и a. Мы полагаем $n = \operatorname{ord}_p a$.

Лемма 3. *Если $a, b \in R$ и $a, b \neq 0$, то* $\operatorname{ord}_p ab = \operatorname{ord}_p a + \operatorname{ord}_p b$.

Доказательство. Положим $\alpha = \operatorname{ord}_p a$ и $\beta = \operatorname{ord}_p b$. Тогда $a = p^\alpha c$ и $b = p^\beta d$ с $p \nmid c$ и $p \nmid d$. Таким образом, $ab = p^{\alpha+\beta} cd$. Так как p — простой элемент, то $p \nmid cd$. Следовательно, $\operatorname{ord}_p ab = \alpha + \beta = \operatorname{ord}_p a + \operatorname{ord}_p b$. □

Мы теперь можем сформулировать и доказать основную теорему этого параграфа.

Пусть S — некоторое множество простых элементов в R со следующими двумя свойствами:

(a) Каждый простой элемент в R ассоциирован с некоторым простым элементом из S.

(b) Никакие два простых элемента из S не ассоциированы.

Для получения такого множества S выберем по одному представителю из каждого класса ассоциированных простых элементов. В таком выборе имеется, конечно, большая доля произвольности. В кольцах $\mathbf{Z}$ и $k[x]$ имелся единственный способ произвести этот выбор. В $\mathbf{Z}$ в качестве S выбирается множество положительных простых чисел. В $k[x]$ в качестве S берется множество при-

веденных неприводимых многочленов. В общем случае естественного способа произвести указанный выбор нет, что приводит иногда к осложнениям (см. гл. 9).

Теорема 3. *Пусть R является* ОГИ *и S — некоторое множество простых элементов с заданными выше свойствами. Тогда для $a \in R$, $a \neq 0$, можно записать*

$$a = u \prod_p p^{e(p)}, \tag{1}$$

где u — единица и произведение берется по всем элементам из S. Единица u, а также показатели степени $e(p)$ определены элементом a однозначно. На самом деле $e(p) = \operatorname{ord}_p a$.

Доказательство. Существование выписанного представления сразу же следует из предложения 1.3.3.

Для доказательства однозначности считаем q простым элементом из S и применяем функцию ord_q к обеим частям равенства (1). Используя лемму 3, получаем

$$\operatorname{ord}_q a = \operatorname{ord}_q u + \sum_p e(p) \operatorname{ord}_q p.$$

Далее, согласно определению функции ord_q, $\operatorname{ord}_q u = 0$ и $\operatorname{ord}_q p = 0$ при $q \neq p$ и $\operatorname{ord}_q p = 1$ при $q = p$. Таким образом, $\operatorname{ord}_q a = e(q)$. Так как показатели степени $e(q)$ определены однозначно, то однозначно определена и единица u. Это завершает доказательство. □

§ 4. Кольца $\mathbf{Z}[i]$ и $\mathbf{Z}[\omega]$

В качестве приложения результатов § 3 мы рассмотрим два примера, которые будут полезны в дальнейшем.

Пусть $i = \sqrt{-1}$, и рассмотрим множество комплексных чисел $\mathbf{Z}[i]$, определенное как $\{a + bi \mid a, b \in \mathbf{Z}\}$. Нетрудно убедиться, что это множество замкнуто относительно сложения и вычитания. Кроме того, если $a + bi$, $c + di \in \mathbf{Z}[i]$, то $(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i \in \mathbf{Z}[i]$. Таким образом, $\mathbf{Z}[i]$ замкнуто относительно умножения и является кольцом. Так как $\mathbf{Z}[i]$ содержится в поле комплексных чисел, оно является областью целостности.

Предложение 1.4.1. $\mathbf{Z}[i]$ *— евклидова область.*

Доказательство. Для $a + bi \in \mathbf{Z}[i]$ положим $\lambda(a + bi) = a^2 + b^2$.

Пусть $\alpha = a + bi$ и $\gamma = c + di$, и предположим, что $\gamma \neq 0$. Тогда $\alpha/\gamma = r + si$, где r и s — вещественные числа (они на самом деле рациональны). Выберем целые числа m, $n \in \mathbf{Z}$ так, что $|r - m| \leqslant 1/2$ и $|s - n| \leqslant 1/2$. Положим $\delta = m + ni$. Тогда $\delta \in \mathbf{Z}[i]$ и $\lambda((\alpha/\gamma) - \delta) = (r - m)^2 + (s - n)^2 \leqslant 1/4 + 1/4 = 1/2$. Пусть $\rho = \alpha - \gamma\delta$. Тогда $\rho \in \mathbf{Z}[i]$ и либо $\rho = 0$, либо $\lambda(\rho) = \lambda(\gamma((\alpha/\gamma) - \delta)) = \lambda(\gamma)\lambda((\alpha/\gamma) - \delta) \leqslant (1/2)\lambda(\gamma) < \lambda(\gamma)$.

Отсюда следует, что функция λ превращает $\mathbf{Z}[i]$ в евклидову область. □

Кольцо $\mathbf{Z}[i]$ называется *кольцом гауссовых целых чисел* в честь К. Ф. Гаусса, который первый детально изучил его арифметические свойства.

Числа ± 1, $\pm i$ суть корни уравнения $x^4 = 1$ над полем комплексных чисел. Рассмотрим уравнение $x^3 = 1$. Так как $x^3 - 1 = (x - 1)(x^2 + x + 1)$, то корнями этого уравнения будут 1, $(-1 \pm \sqrt{-3})/2$. Пусть $\omega = (-1 + \sqrt{-3})/2$. Тогда нетрудно проверить, что $\omega^2 = (-1 - \sqrt{-3})/2$ и что $1 + \omega + \omega^2 = 0$.

Рассмотрим множество $\mathbf{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbf{Z}\}$. Оно замкнуто относительно сложения и вычитания. Кроме того, $(a + b\omega)(c + d\omega) = ac + (ad + bc)\omega + bd\omega^2 = (ac - bd) + (ad + bc - bd)\omega$. Таким образом, $\mathbf{Z}[\omega]$ является кольцом. Опять ввиду того, что $\mathbf{Z}[\omega]$ — подмножество поля комплексных чисел, оно будет областью целостности.

Заметим, что $\mathbf{Z}[\omega]$ замкнуто относительно комплексного сопряжения. Действительно, так как $\overline{\sqrt{-3}} = \sqrt{3i} = -\sqrt{3}i = -\sqrt{-3}$, мы видим, что $\bar{\omega} = \omega^2$. Таким образом, если $\alpha = a + b\omega \in \mathbf{Z}[\omega]$, то $\bar{\alpha} = a + b\bar{\omega} = a + b\omega^2 = (a - b) - b\omega \in \mathbf{Z}[\omega]$.

Предложение 1.4.2. $\mathbf{Z}[\omega]$ — *евклидова область.*

Доказательство. Для $\alpha = a + b\omega \in \mathbf{Z}[\omega]$ определим $\lambda(a) = a^2 - ab + b^2$. Простое вычисление показывает, что $\lambda(\alpha) = \alpha\bar{\alpha}$.

Пусть теперь $\alpha, \beta \in \mathbf{Z}[\omega]$, и предположим, что $\beta \neq 0$. Тогда $\alpha/\beta = \alpha\bar{\beta}/\beta\bar{\beta} = r + s\omega$, где r и s — рациональные числа. Мы использовали тот факт, что $\beta\bar{\beta} = \lambda(\beta)$ — положительное целое число и что $\alpha\bar{\beta} \in \mathbf{Z}[\omega]$, так как α и $\bar{\beta} \in \mathbf{Z}[\omega]$.

Выберем целые числа m и n так, чтобы $|r - m| \leqslant 1/2$ и $|s - n| \leqslant 1/2$, и пусть $\gamma = m + n\omega$. Тогда $\lambda((\alpha/\beta) - \gamma) = (r - m)^2 - (r - m)(s - n) + (s - n)^2 \leqslant 1/4 + 1/4 + 1/4 < 1$.

Пусть $\rho = \alpha - \gamma\beta$. Тогда либо $\rho = 0$, либо $\lambda(\rho) = \lambda(\beta((\alpha/\beta) - \gamma)) = \lambda(\beta)\lambda((\alpha/\beta) - \gamma) < \lambda(\beta)$. □

Из анализа, проведенного в § 3, вытекает, что теорема об однозначном разложении на простые множители справедлива в обоих кольцах $\mathbf{Z}[i]$ и $\mathbf{Z}[\omega]$. Для более глубокого проникновения в мультипликативную структуру этих колец нам следовало бы изучить единицы и простые элементы в них. Некоторые результаты этого типа приведены в упражнениях.

Замечания

Кольца, для которых справедлива теорема об однозначном разложении на неприводимые элементы, называются областями с однозначным разложением на множители (ООР). Результат о том, что кольцо $\mathbf{Z}$ является ООР, в неявном виде имеется уже у Евклида, но первое явное и ясное утверждение об этом, по-видимому, содержится в выдающемся произведении К. Ф. Гаусса «Арифметические исследования» [34]. Цермело дал искусное доказательство с помощью приведения к противоречию, которое воспроизведено в замечательной книге [40]. Укажем также [120].

Как мы показали, каждая ОГИ является ООР. Обращение этого утверждения неверно. Для примера можно рассмотреть кольцо многочленов над некоторым полем от более чем одной переменной, которое будет ООР, но не ОГИ. Имеется превосходная вводная статья по ООР [67]. Более элементарное введение можно найти в книге [65].

Читатель может счесть полезным познакомиться с вводным материалом по нескольким книгам по теории чисел. Особенно удачны гл. 3 из [32] и предисловие к [73]. Имеется также более давняя лекция Харди [39], которую мы настоятельно рекомендуем.

Кольцо $\mathbf{Z}[i]$ было введено Гауссом в его втором мемуаре о биквадратичном законе взаимности [34]. Кольцо $\mathbf{Z}[\omega]$ рассматривалось Эйзенштейном в связи с его работой о кубическом законе взаимности. Он замечает, что для исследования свойств этого кольца следует лишь использовать работу Гаусса о $\mathbf{Z}[i]$ и модифицировать доказательства [28]. Тщательное рассмотрение этих двух колец проведено в гл. 12 книги [40]. В гл. 14 той же книги рассматривается обобщение, а именно кольца целых чисел в квадратичных числовых полях. Тому же материалу посвящена гл. 8 из [73]. В 1966 г. Старк получил решение одной из знаменитых проблем теории чисел, показав, что кольцо целых чисел (см. гл. 6 этой книги) в поле $\mathbf{Q}(\sqrt{d})$ с отрицательным d является ООР лишь при значениях $d = -1, -2, -3, -7, -11, -19, -43, -67$ и -163 [1]).

[1]) Независимо этот результат получил А. Бейкер (см. гл. 13, § 1). — *Прим. ред.*

Тот, кто хоть немного знаком с началами алгебры, заметит, что не-ООР «общего вида» будет кольцо $k[x, y, z, w]$ с соотношением $xy = zw$, где k — некоторое поле. Другим примером не-ООР является $\mathbf{C}[x, y, z]$ с соотношением $x^2 + y^2 + z^2 = 1$, где $\mathbf{C}$ — поле комплексных чисел. Чтобы убедиться в этом, заметим, что $(x + iy)(x - iy) = (1 - z)(1 + z)$.

Упражнения

1. Пусть a и b — некоторые отличные от нуля целые числа. Мы можем найти такие целые числа q и r, что $a = qb + r$, где $0 \leqslant r < b$. Доказать, что $(a, b) = (b, r)$.

2 (продолжение). Если $r \neq 0$, где мы можем найти такие q_1 и r_1, что $b = q_1 r + r_1$, где $0 \leqslant r_1 < r$. Показать, что $(a, b) = (r, r_1)$. Этот процесс можно продолжить. Показать, что он заканчивается за конечное число шагов и что последний ненулевой остаток должен быть равен (a, b). Этот прием выглядит следующим образом:

$$a = qb + r, \quad 0 \leqslant r < b,$$

$$b = q_1 r + r_1, \quad 0 \leqslant r_1 < r,$$

$$r = q_2 r_1 + r_2, \quad 0 \leqslant r_2 < r_1,$$

$$\vdots$$

$$r_{k-1} = q_{k+1} r_k + r_{k+1}, \quad 0 \leqslant r_{k+1} < r_k,$$

$$r_k = q_{k+2} r_{k+1}.$$

Тогда $r_{k+1} = (a, b)$. Этот способ нахождения (a, b) известен как *алгоритм Евклида*.

3. Вычислить (187, 221), (6188, 4709) и (314, 159).

4. Пусть $d = (a, b)$. Показать, как можно использовать алгоритм Евклида для нахождения таких чисел m и n, что $am + bn = d$. [*Указание.* В упр. 2 $d = r_{k+1}$. Выразить r_{k+1} через r_k и r_{k-1}, затем через r_{k-1} и r_{k-2} и т. д.]

5. Найти m и n для пар (a, b) в упр. 3.

6. Пусть $a, b, c \in \mathbf{Z}$. Показать, что уравнение $ax + by = c$ имеет решение в целых числах тогда и только тогда, когда $(a, b) \mid c$.

7. Пусть $d = (a, b)$ и $a = da'$ и $b = db'$. Показать, что $(a', b') = 1$.

8. Пусть x_0 и y_0 являются решением уравнения $ax + by = c$. Показать, что все решения имеют вид $x = x_0 + t(b/d)$, $y = y_0 - t(a/d)$, где $d = (a, b)$ и $t \in \mathbf{Z}$.

9. Предположим, что $u, v \in \mathbf{Z}$ и что $(u, v) = 1$. Если $u \mid n$ и $v \mid n$, то $uv \mid n$. Показать, что это неверно, если $(u, v) \neq 1$.

10. Предположим, что $(u, v) = 1$. Показать, что $(u + v, u - v)$ равен либо 1, либо 2.

11. Показать, что $(a, a + k) \mid k$.

12. Предположим, что у нас имеется несколько экземпляров некоторого правильного многоугольника, которые мы пытаемся плотно уложить друг около друга вокруг одной вершины. Доказать, что единственными реализуемыми возможностями будут шесть равносторонних треугольников, четыре квадрата и три шестиугольника.

13. Пусть $n_1, n_2, \ldots, n_s \in \mathbf{Z}$. Определить наибольший общий делитель d для $n_1, n_2, \ldots, n_s$ и доказать, что существуют такие целые числа $m_1, m_2, \ldots, m_s$, что $n_1 m_1 + n_2 m_2 + \ldots + n_s m_s = d$.

14. Рассмотреть вопрос о разрешимости в целых числах уравнения $a_1x_1 + a_2x_2 + \ldots + a_rx_r = c$. [*Указание.* Используя упр. 13, обобщить рассуждение, применяемое в упр. 6.]

15. Доказать, что $a \in \mathbf{Z}$ является квадратом некоторого целого числа тогда и только тогда, когда $\operatorname{ord}_p a$ четно для всех простых чисел p. Обобщить этот результат.

16. Если $(u, v) = 1$ и $uv = a^2$, то показать, что u и v оба будут квадратами.

17. Доказать, что квадратный корень из 2 иррационален, т. е. что не существует рационального числа $r = a/b$, такого, что $r^2 = 2$.

18. Доказать, что $\sqrt[n]{m}$ иррационально, если m не является n-й степенью некоторого целого числа.

19. Определим *наименьшее общее кратное* двух чисел a и b как такое целое число m, что $a \mid m$, $b \mid m$ и m делит каждое общее кратное чисел a и b. Показать, что такое m существует. Оно определено однозначно с точностью до знака. Мы будем обозначать его через $[a, b]$.

20. Доказать такие свойства:

(a) $\operatorname{ord}_p [a, b] = \max (\operatorname{ord}_p a, \operatorname{ord}_p b)$;

(b) $(a, b)\,[a, b] = ab$;

(c) $(a + b, [a, b]) = (a, b)$.

21. Доказать, что $\operatorname{ord}_p (a + b) \geqslant \min (\operatorname{ord}_p a, \operatorname{ord}_p b)$, причем равенство имеет место при $\operatorname{ord}_p a \neq \operatorname{ord}_p b$.

22. Почти все предыдущие упражнения остаются верными, если вместо кольца $\mathbf{Z}$ рассматривать кольцо $k[x]$. В самом деле, в большинстве из них можно рассматривать произвольную евклидову область. Убедиться в этом. Для простоты мы будем продолжать работать в $\mathbf{Z}$.

23. Предположим, что $a^2 + b^2 = c^2$, где $a, b, c \in \mathbf{Z}$. Например, $3^2 + 4^2 = 5^2$ и $5^2 + 12^2 = 13^2$. Предположим, что $(a, b) = (b, c) = (c, a) = 1$. Доказать, что существуют такие целые числа u и v, что $c - b = 2u^2$ и $c + b = 2v^2$ и $(u, v) = 1$ (без ограничения общности можно считать, что b и c нечетны, а a четно). Следовательно, $a = 2uv$, $b = v^2 - u^2$ и $c = v^2 + u^2$. И обратно, показать, что если u и v заданы, то три числа a, b и c, задаваемые этими формулами, удовлетворяют уравнению $a^2 + b^2 = c^2$.

24. Доказать тождества

(a) $x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \cdots + y^{n-1})$;

(b) $x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + x^{n-3}y^2 - \cdots + y^{n-1})$

для нечетного n.

25. Если $a^n - 1$ — простое число, то показать, что $a = 2$ и что n — простое число. Простые числа вида $2^p - 1$ называются *числами Мерсенна*. Например, $2^3 - 1 = 7$ и $2^5 - 1 = 31$. Неизвестно, бесконечно ли много чисел Мерсенна.

26. Если $a^n + 1$ — простое число, то показать, что a четно и что n является степенью 2. Простые числа вида $2^{2^t} + 1$ называются *числами Ферма*. Например, $2^{2^1} + 1 = 5$ и $2^{2^2} + 1 = 17$. Неизвестно, бесконечно ли много простых чисел Ферма.

27. Для всех нечетных n показать, что $8 \mid n^2 - 1$. Если $3 \nmid n$, то показать, что $6 \mid n^2 - 1$.

28. Для всех n показать, что $30 \mid n^5 - n$ и что $42 \mid n^7 - n$.

29. Предположим, что $a, b, c, d \in \mathbf{Z}$ и что $(a, b) = (c, d) = 1$. Если $(a/b) + (c/d)$ — целое число, то показать, что $b = \pm d$.

30. Доказать, что $1/2 + 1/3 + \ldots + 1/n$ не является целым числом.

31. Показать, что 2 делится на $(1+i)^2$ в $\mathbf{Z}[i]$.

32. Для $\alpha = a + bi \in \mathbf{Z}[i]$ мы определили $\lambda(\alpha) = a^2 + b^2$. Из свойств функции λ вывести тождество $(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$.

33. Показать, что $\alpha \in \mathbf{Z}[i]$ является единицей тогда и только тогда, когда $\lambda(\alpha) = 1$. Получить отсюда, что $1, -1, i, -i$ — единственные единицы в $\mathbf{Z}[i]$.

34. Показать, что 3 делится на $(1-\omega)^2$ в $\mathbf{Z}[\omega]$.

35. Для $\alpha = a + b\omega \in \mathbf{Z}[\omega]$ мы определили $\lambda(\alpha) = a^2 - ab + b^2$. Показать, что α является единицей тогда и только тогда, когда $\lambda(\alpha) = 1$. Вывести отсюда, что $1, -1, \omega, -\omega, \omega^2$ и $-\omega^2$ являются единственными единицами в $\mathbf{Z}[\omega]$.

36. Определим $\mathbf{Z}[\sqrt{-2}]$ как множество комплексных чисел вида $a + b\sqrt{-2}$, где $a, b \in \mathbf{Z}$. Показать, что $\mathbf{Z}[\sqrt{-2}]$ — кольцо. Определим функцию $\lambda(\alpha) = a^2 + 2b^2$ для $\alpha = a + b\sqrt{-2}$. Воспользоваться функцией λ для доказательства того, что $\mathbf{Z}[\sqrt{-2}]$ — евклидова область.

37. Показать, что единственными единицами в $\mathbf{Z}[\sqrt{-2}]$ будут 1 и -1.

38. Предположим, что $\lambda(\pi) = p$ — простое число в $\mathbf{Z}$ для некоторого $\pi \in \mathbf{Z}[i]$. Показать, что π — простой элемент в $\mathbf{Z}[i]$. Показать, что соответствующий результат верен в $\mathbf{Z}[\omega]$ и в $\mathbf{Z}[\sqrt{-2}]$.

39. Показать, что в любой области целостности простой элемент неприводим.

Глава 2

ПРИМЕНЕНИЯ ОДНОЗНАЧНОГО РАЗЛОЖЕНИЯ НА МНОЖИТЕЛИ

Из результатов гл. 1 становится очевидной важность понятия простого числа.

В этой главе мы приведем несколько доказательств того факта, что простых чисел в **Z** *бесконечно много. Аналогичный вопрос мы рассмотрим также для кольца* $k[x]$.

На теорему об однозначном разложении на множители ссылаются иногда как на основную теорему арифметики. Ее пользу мы продемонстрируем на примере исследования свойств некоторых естественных теоретико-числовых функций.

§ 1. В Z бесконечно много простых чисел

Теорема 1 (Евклид). *В кольце* **Z** *имеется бесконечно много простых чисел.*

Доказательство. Будем рассматривать положительные простые числа. Расположим их в возрастающей последовательности $p_1, p_2, p_3, \ldots$. Таким образом, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ и т. д. Пусть $N = (p_1 p_2 \ldots p_n) + 1$. Число N больше 1 и не делится ни на какое p_i, $i = 1, 2, \ldots, n$. С другой стороны, N делится на некоторое простое число p и p должно быть больше, чем p_n.

Мы показали, что для любого заданного положительного простого числа существует другое простое число, которое больше первого. Отсюда следует, что множество простых чисел бесконечно. □

Аналогичная теорема для кольца $k[x]$ состоит в том, что существует бесконечно много приведенных неприводимых многочленов. Если поле k бесконечно, то это очевидно, поскольку $x - a$ приведен и неприводим при всех $a \in k$. Это доказательство не проходит в случае, когда k конечно, но к этому случаю легко приспосабливается доказательство Евклида. Мы оставляем проверку этого читателю в качестве упражнения.

Напомним, что в некоторой области целостности два элемента называются ассоциированными, если они отличаются лишь умножением на какую-либо единицу. Сейчас нам известно, что в коль-

цах $\mathbf{Z}$ и $k[x]$ существует бесконечно много неассоциированных простых элементов. Интересно рассмотреть какое-либо кольцо, в котором все простые элементы ассоциированы, так что по существу имеется лишь один простой элемент.

Пусть $p \in \mathbf{Z}$ — некоторое простое число и $\mathbf{Z}_p$ — множество всех рациональных чисел a/b с $p \nmid b$. Используя замечание после следствия 1 предложения 1.1.1, нетрудно проверить, что $\mathbf{Z}_p$ — кольцо. Элемент $a/b \in \mathbf{Z}_p$ будет единицей, если существует такое число $c/d \in \mathbf{Z}_p$, что $a/b \cdot c/d = 1$. В таком случае $ac = bd$, откуда получаем, что $p \nmid a$, ибо $p \nmid b$ и $p \nmid d$. Обратно, любое рациональное число a/b будет единицей в $\mathbf{Z}_p$, если $p \nmid b$ и $p \nmid a$. Если $a/b \in \mathbf{Z}_p$, запишем $a = p^l a'$, где $p \nmid a'$. Тогда $a/b = p^l a'/b$. Таким образом, каждый элемент в $\mathbf{Z}_p$ будет некоторой степенью числа p, умноженной на единицу. На основании этого нетрудно убедиться в том, что все простые элементы в $\mathbf{Z}_p$ имеют вид pc/d, где c/d — некоторая единица. Поэтому все простые элементы в $\mathbf{Z}_p$ ассоциированы.

Упражнение

Если $a/b \in \mathbf{Z}_p$ — не единица, то доказать, что $a/b + 1$ — единица. Этот факт показывает, почему доказательство Евклида не проходит в общем виде для областей целостности.

§ 2. Некоторые арифметические функции

В оставшейся части этой главы мы рассмотрим ряд приложений теоремы об однозначном разложении на множители.

Целое число $a \in \mathbf{Z}$ называется *свободным от квадратов*, если оно не делится на квадрат никакого другого целого числа, большего 1.

Предложение 2.2.1. *Любое $n \in \mathbf{Z}$ может быть записано в виде $n = ab^2$, где $a, b \in \mathbf{Z}$ и a свободно от квадратов.*

Доказательство. Пусть $n = p_1^{a_1} p_2^{a_2} \dots p_l^{a_l}$. Можно записать $a_i = 2b_i + r_i$, где $r_i = 0$ или 1 в зависимости от того, будет ли a_i четным или нет. Положим $a = p_1^{r_1} p_2^{r_2} \dots p_l^{r_l}$ и $b = p_1^{b_1} p_2^{b_2} \dots p_l^{b_l}$. Тогда $n = ab^2$ и очевидно, что a свободно от квадратов. □

Это предложение можно использовать для другого доказательства того, что простых чисел в $\mathbf{Z}$ бесконечно много. Предположим, что это утверждение неверно; пусть $p_1, p_2, \dots, p_l$ — полный список положительных простых чисел. Рассмотрим множество положительных целых чисел, меньших или равных некоторому числу N. Если $n \leqslant N$, то $n = ab^2$, где a свободно от

квадратов и поэтому равно одному из 2^l чисел $p_1^{\varepsilon_1} p_2^{\varepsilon_2} \dots p_l^{\varepsilon_l}$, где $\varepsilon_i = 0$ или 1, $i = 1, 2, \dots, l$. Заметим, что $b \leqslant \sqrt{N}$. Имеется, самое большее, $2^l \sqrt{N}$ чисел, удовлетворяющих этим условиям, так что $N \leqslant 2^l \sqrt{N}$, т. е. $\sqrt{N} \leqslant 2^l$, что, безусловно, неверно при достаточно большом N. Полученное противоречие доказывает наш результат.

Можно дать аналогичное этому доказательство и того, что в $k[x]$, где k — конечное поле, существует бесконечно много приведенных неприводимых многочленов.

На целых числах имеется ряд естественно определенных функций. Например, для заданного положительного целого числа n пусть $\nu(n)$ — число его положительных делителей, а $\sigma(n)$ — сумма его положительных делителей. Скажем, $\nu(3) = 2$, $\nu(6) = 4$ и $\nu(12) = 6$ и $\sigma(3) = 4$, $\sigma(6) = 12$ и $\sigma(12) = 28$. Используя однозначность разложения на множители, можно получить довольно простые формулы для этих функций.

Предложение 2.2.2. *Пусть n — положительное целое число и $n = p_1^{a_1} p_2^{a_2} \dots p_l^{a_l}$ — его разложение на простые множители. Тогда*

(a) $\nu(n) = (a_1 + 1)(a_2 + 1) \dots (a_l + 1)$;

(b) $\sigma(n) = ((p_1^{a_1+1} - 1)/(p_1 - 1))((p_2^{a_2+1} - 1)/(p_2 - 1)) \dots$

$\dots((p_l^{a_l+1} - 1)/(p_l - 1))$.

Доказательство. Для доказательства п. (a) заметим, что $m \mid n$ тогда и только тогда, когда $m = p_1^{b_1} p_2^{b_2} \dots p_l^{b_l}$ и $0 \leqslant b_i \leqslant a_i$ для $i = 1, 2, \dots, l$. Таким образом, положительные делители находятся во взаимно однозначном соответствии с l-наборами $(b_1, b_2, \dots, b_l)$, где $0 \leqslant b_i \leqslant a_i$ для $i = 1, 2, \dots, l$, а таких наборов имеется в точности $(a_1 + 1)(a_2 + 1) \dots (a_l + 1)$.

Для доказательства п. (b) заметим, что

$$\sigma(n) = \sum p_1^{b_1} p_2^{b_2} \dots p_l^{b_l},$$

где сумма берется по упомянутым выше l-наборам. Таким образом,

$$\sigma(n) = \left(\sum_{b_1=0}^{a_1} p_1^{b_1}\right)\left(\sum_{b_2=0}^{a_2} p_2^{b_2}\right) \dots \left(\sum_{b_l=0}^{a_l} p_l^{b_l}\right),$$

откуда и следует доказываемый результат, если воспользоваться формулой суммирования для геометрической прогрессии. □

С функцией $\sigma(n)$ связана одна интересная нерешенная проблема. Натуральное число n называется *совершенным*, если $\sigma(n) = 2n$. Например, 6 и 28 — совершенные числа. Вообще, если $2^{m+1} - 1$ — простое число, то $n = 2^m(2^{m+1} - 1)$ — совершенное число, в чем можно убедиться, применив п. (b) предложения 2.2.2. Этот факт был известен уже Евклиду. Эйлер показал, что любое четное совершенное число имеет такой вид. Таким образом, проблема нахождения четных совершенных чисел сводится к нахождению простых чисел вида $2^{m+1} - 1$. Эти простые числа называются *числами Мерсенна*. С совершенными числами связаны следующие две знаменитые проблемы: бесконечно ли много совершенных чисел? Существуют ли нечетные совершенные числа?

Мультипликативный аналог этой проблемы тривиален. Целое число n называется *мультипликативно совершенным*, если произведение его положительных делителей равно n^2. Такое число не может быть простым или квадратом простого числа. Таким образом, существует некоторый его собственный делитель d, для которого $d \neq n/d$. Произведение делителей 1, d, n/d и n уже равно n^2. Поэтому n мультипликативно совершенно тогда и только тогда, когда у него есть в точности два собственных делителя. Единственные такие числа суть кубы простых чисел и произведения двух различных простых чисел. Например, 27 и 10 мультипликативно совершенны.

Мы введем теперь очень важную арифметическую функцию, функцию Мёбиуса μ. Для $n \in \mathbf{Z}^+$ полагаем $\mu(1) = 1$, $\mu(n) = 0$, если n не свободно от квадратов, и $\mu(p_1 p_2 \ldots p_l) = (-1)^l$, где p_i — различные простые числа.

Предложение 2.2.3. *При $n > 1$ имеем* $\sum_{d \mid n} \mu(d) = 0$.

Доказательство. Если $n = p_1^{a_1} p_2^{a_2} \ldots p_l^{a_l}$, то

$$\sum_{d \mid n} \mu(d) = \sum_{(\varepsilon_1, \ldots, \varepsilon_l)} \mu\left(p_1^{\varepsilon_1} \ldots p_l^{\varepsilon_l}\right),$$

где ε_i есть 0 или 1. Таким образом,

$$\sum_{d \mid n} \mu(d) = 1 - l + \binom{l}{2} - \binom{l}{3} + \ldots + (-1)^l = (1-1)^l = 0. \quad \square$$

Во всей полноте значение функции Мёбиуса μ может стать понятным лишь тогда, когда будет установлена ее связь с умножением Дирихле. Пусть f и g — некоторые комплекснозначные функции на $\mathbf{Z}^+$. *Произведение Дирихле* двух функций f и g определяется формулой $f \circ g(n) = \sum f(d_1) g(d_2)$, где сумма берется по всем таким парам (d_1, d_2) положительных целых чисел, что

$d_1d_2 = n$. Это произведение ассоциативно, в чем можно убедиться, проверив, что

$$f \circ (g \circ h)(n) = (f \circ g) \circ h(n) = \sum f(d_1)\, g(d_2)\, h(d_3),$$

где сумма берется по всем 3-наборам (d_1, d_2, d_3) положительных целых чисел, таким, что $d_1d_2d_3 = n$.

Определим функцию $\mathbb{I}$ равенствами $\mathbb{I}(1) = 1$ и $\mathbb{I}(n) = 0$ для $n > 1$. Тогда $f \circ \mathbb{I} = \mathbb{I} \circ f$. Определим также функцию I равенствами $I(n) = 1$ для всех $n \in \mathbf{Z}^+$. Тогда $f \circ I(n) = I \circ f(n) = \sum\limits_{d|n} f(d)$.

Лемма. $I \circ \mu = \mu \circ I = \mathbb{I}$.

Доказательство. $\mu \circ I(1) = \mu(1)\, I(1) = 1$. Если $n > 1$, то $\mu \circ I(n) = \sum\limits_{d|n} \mu(d) = 0$. То же доказательство применимо к $I \circ \mu$. □

Теорема 2 (теорема обращения Мёбиуса). *Положим* $F(n) = \sum\limits_{d|n} f(d)$. *Тогда* $f(n) = \sum\limits_{d|n} \mu(d)\, F(n/d)$.

Доказательство. Имеем $F = f \circ I$. Поэтому $F \circ \mu = (f \circ I) \circ \mu = f \circ (I \circ \mu) = f \circ \mathbb{I} = f$. Это показывает, что $f(n) = F \circ \mu(n) = \sum\limits_{d|n} \mu(d)\, F(n/d)$. □

Замечание. Мы рассматривали комплекснозначные функции на положительных целых числах. Полезно отметить, что теорема 2 справедлива и в том случае, когда функции принимают значения в какой-либо абелевой группе. Доказательство дословно совпадает с приведенным.

Когда групповая операция в абелевой группе записана мультипликативно, теорема 2 принимает такой вид:

$$\text{если } F(n) = \prod_{d|n} f(d), \text{ то } f(n) = \prod_{d|n} F(n/d)^{\mu(d)}.$$

Теорема обращения Мёбиуса имеет много приложений. Мы воспользуемся ею при получении формулы для еще одной арифметической функции, функции Эйлера φ. Для $n \in \mathbf{Z}^+$ функция $\varphi(n)$ определяется как количество целых чисел между 1 и n, взаимно простых с n. Например, $\varphi(1) = 1$, $\varphi(5) = 4$, $\varphi(6) = 2$ и $\varphi(9) = 6$. Если p — простое число, то очевидно, что $\varphi(p) = p - 1$.

Предложение 2.2.4. $\sum\limits_{d|n} \varphi(d) = n$.

Доказательство. Рассмотрим n рациональных чисел $1/n$, $2/n$, $3/n$, ..., $(n-1)/n$, n/n. Произведем максимальное сокращение этих дробей, т. е. представим каждое из них в виде отношения взаимно простых целых чисел. Полученные знаменатели — это все делители числа n. Если $d \mid n$, то точно $\varphi(d)$ наших чисел будут иметь d в качестве знаменателя после проведенного сокращения. Поэтому $\sum_{d|n} \varphi(d) = n$. □

Предложение 2.2.5. *Если* $n = p_1^{a_1} p_2^{a_2} \dots p_l^{a_l}$, *то*

$$\varphi(n) = n(1 - (1/p_1))(1 - (1/p_2)) \dots (1 - (1/p_l)).$$

Доказательство. Так как $n = \sum_{d|n} \varphi(d)$, из теоремы обращения Мёбиуса следует, что

$$\varphi(n) = \sum_{d|n} \mu(d)\, n/d = n - \sum_i n/p_i + \sum_{i<j} n/p_i p_j - \dots =$$
$$= n(1 - (1/p_1))(1 - (1/p_2)) \dots (1 - (1/p_l)). \quad \square$$

Позже мы приведем доказательство этой формулы, полнее вскрывающее суть дела. Мы используем функцию Мёбиуса также для того, чтобы определить число приведенных неприводимых многочленов данной фиксированной степени в $k[x]$, где k — конечное поле.

§ 3. Ряд $\sum 1/p$ расходится

Мы начали эту главу с доказательства того, что в $\mathbf{Z}$ существует бесконечно много простых чисел. Закончим мы ее доказательством несколько более сильного утверждения. При этом нам будут нужны некоторые элементарные факты из теории бесконечных рядов.

Теорема 3. *Ряд* $\sum 1/p$, *где сумма берется по всем положительным простым числам из* $\mathbf{Z}$, *расходится.*

Доказательство. Пусть $p_1, p_2, \dots, p_{l(n)}$ — все простые числа, меньшие n, и положим

$$\lambda(n) = \prod_{i=1}^{l(n)} (1 - 1/p_i)^{-1}.$$

Так как $(1 - 1/p_i)^{-1} = \sum_{a_i=0}^{\infty} 1/p_i^{a_i}$, то

$$\lambda(n) = \sum (p_1^{a_1} p_2^{a_2} \dots p_l^{a_l})^{-1},$$

где сумма берется по всем l-наборам неотрицательных целых чисел $(a_1, a_2, \ldots, a_l)$. В частности, мы видим, что $1 + 1/2 + 1/3 + \ldots + 1/n < \lambda(n)$. Таким образом, $\lambda(n) \to \infty$ при $n \to \infty$. Это уже дает новое доказательство того, что простых чисел бесконечно много.

Далее, рассмотрим $\ln \lambda(n)$. Имеем

$$\ln \lambda(n) = -\sum_{i=1}^{l} \ln\left(1 - p_i^{-1}\right) = \sum_{i=1}^{l} \sum_{m=1}^{\infty} \left(m p_i^m\right)^{-1} =$$

$$= p_1^{-1} + p_2^{-1} + \ldots + p_l^{-1} + \sum_{i=1}^{l} \sum_{m=2}^{\infty} \left(m p_i^m\right)^{-1}.$$

Но

$$\sum_{m=2}^{\infty} \left(m p_i^m\right)^{-1} < \sum_{m=2}^{\infty} p_i^{-m} = p_i^{-2}\left(1 - p_i^{-1}\right)^{-1} \leqslant 2p_i^{-2}.$$

Таким образом, $\ln \lambda(n) \leqslant p_1^{-1} + p_2^{-1} + \ldots + p_l^{-1} + 2\left(p_1^{-2} + p_2^{-2} + \ldots + p_l^{-2}\right)$. Хорошо известно, что ряд $\sum_{n=1}^{\infty} n^{-2}$ сходится. Отсюда следует, что ряд $\sum_{i=1}^{\infty} p_i^{-2}$ сходится. Итак, если бы ряд $\sum p^{-1}$ сходился, то существовала бы константа M, для которой $\ln \lambda(n) < M$, т. е. $\lambda(n) < e^M$. Это, однако, невозможно, ибо $\lambda(n) \to \infty$ при $n \to \infty$. Таким образом, ряд $\sum p^{-1}$ расходится. □

Полезно получить аналог теоремы 3 для кольца $k[x]$, где k — некоторое конечное поле из q элементов. Роль положительных простых чисел p берут на себя приведенные неприводимые многочлены $p(x)$. «Размер» приведенного многочлена $f(x)$ задается величиной $q^{\deg f(x)}$.

Это разумно, поскольку положительное целое число n есть в то же время число неотрицательных целых чисел, меньших n, т. е. число элементов в множестве $\{0, 1, 2, \ldots, n-1\}$. Аналогично $q^{\deg f(x)}$ есть число многочленов, имеющих степень, меньшую, чем степень $f(x)$, в чем нетрудно убедиться. Любой такой многочлен имеет вид $a_0 x^m + a_1 x^{m-1} + \ldots + a_m$, где $m = \deg f(x) - 1$ и $a_i \in k$. Для a_i имеется q возможностей и выбор для каждого индекса не зависит от других Таким образом, имеется $q^{m+1} = q^{\deg f(x)}$ таких многочленов.

Теорема 4. *Ряд $\sum q^{-\deg p(x)}$, где сумма берется по всем приведенным неприводимым многочленам $p(x)$ из $k[x]$, расходится.*

Доказательство. Мы покажем сначала, что ряд $\sum q^{-\deg f(x)}$ расходится, а ряд $\sum q^{-2\deg f(x)}$ сходится, когда сумма в обоих

случаях берется по всем приведенным многочленам $f(x)$ из $k[x]$. Оба результата следуют из того факта, что в $k[x]$ имеется точно q^n приведенных многочленов степени n. Рассмотрим $\sum_{\deg f(x) \leqslant n} q^{-\deg f(x)}$. Эта сумма равна $\sum_{m=0}^{n} q^m q^{-m} = n+1$. Таким образом, ряд $\sum q^{-\deg f(x)}$ расходится. Подобно предыдущему,

$$\sum_{\deg f(x) \leqslant n} q^{-2\deg f(x)} = \sum_{m=0}^{n} q^m q^{-2m} < (1-1/q)^{-1}.$$

Таким образом, $\sum q^{-2\deg f(x)}$ сходится.

Остальная часть доказательства в точности повторяет доказательство теоремы 3. Дополнить детали предоставляется читателю. □

§ 4. Рост функции $\pi(x)$

Во введении к гл. 1 мы определили $\pi(x)$ как число простых чисел p, таких, что $1 < p \leqslant x$. Для изучения поведения функции $\pi(x)$ при больших x надо привлечь технику математического анализа. В этом параграфе мы докажем несколько результатов, которые требуют минимум сведений из анализа. В действительности используются лишь простейшие свойства логарифмической функции.

Мы начнем с простого следствия из рассуждения Евклида (теорема 1), которое задает слабую нижнюю границу для $\pi(x)$. Далее $\ln x$ обозначает натуральный логарифм от x.

Предложение 2.4.1. $\pi(x) \geqslant \ln(\ln x)$, $x \geqslant 2$.

Доказательство. Пусть p_n обозначает n-е простое число. Тогда ввиду того, что любое простое число, делящее $p_1 p_2 \ldots p_n + 1$, отлично от $p_1, p_2, \ldots, p_n$, получаем $p_{n+1} \leqslant p_1 p_2 \ldots p_n + 1$. Далее, $p_1 < 2^{(2^1)}$, $p_2 < 2^{(2^2)}$ и, если $p_n < 2^{(2^n)}$, то $p_{n+1} \leqslant 2^{(2^1)} \cdot 2^{(2^2)} \ldots 2^{(2^n)} + 1 = 2^{(2^{n+1}-2)} + 1 < 2^{(2^{n+1})}$. Отсюда следует, что $\pi\left(2^{(2^n)}\right) \geqslant n$. Для $x > 2$ выберем такое целое число n, что $e^{(e^{n-1})} < x \leqslant e^{(e^n)}$. Если $n > 2$, то $e^{n-1} > 2^n$, так что

$$\pi(x) \geqslant \pi\left(e^{(e^{n-1})}\right) \geqslant \pi\left(e^{(2^n)}\right) \geqslant \pi\left(2^{(2^n)}\right) \geqslant n \geqslant \ln(\ln x).$$

Это доказывает наш результат для $x > e^e$. Если $x \leqslant e^e$, то неравенство очевидно. □

Метод, примененный в абзаце, горый идет за предложением 2.2.1, для доказательства того, что $\pi(x) \to \infty$, можно также ис-

пользовать для получения следующего улучшения только что доказанного предложения. Для положительного целого числа n пусть $\gamma(n)$ обозначает множество его простых делителей.

Предложение 2.4.2. $\pi(x) \geqslant \ln x/2 \ln 2$.

Доказательство. Для любого множества простых чисел S определим $f_S(x)$ как число целых чисел n, $1 \leqslant n \leqslant x$, с $\gamma(n) \subset S$. Предположим, что S — конечное множество из t элементов. Записывая такое n в виде $n = m^2 s$ со свободным от квадратов s, мы видим, что $m \leqslant \sqrt{x}$, в то время как для s имеется, самое большее, 2^t возможностей, соответствующих различным подмножествам в S. Таким образом, $f_S(x) \leqslant 2^t \sqrt{x}$. Положим $\pi(x) = m$, так что $p_{m+1} > x$. Если $S = \{p_1, \ldots, p_m\}$, то очевидно, что $f_S(x) = x$, откуда следует, что $x \leqslant 2^m \sqrt{x} = 2^{\pi(x)} \sqrt{x}$. Нужный результат сразу же следует отсюда. □

Интересно отметить, что примененный выше метод может быть использован для другого доказательства теоремы 3. Действительно, если $\sum 1/p_j$ сходится, то существует такое n, что $\sum_{j>n} 1/p_j < \frac{1}{2}$. Если $S = \{p_1, \ldots, p_n\}$, то $x - f_S(x)$ есть число положительных целых чисел $m \leqslant x$, таких, что $\gamma(m) \not\subset S$, т. е. существует простое число p_j, $j > n$, такое, что $p_j \mid m$. Для такого простого числа существует $[x/p_j]$ кратных ему, не превосходящих x. Таким образом,

$$x - f_S(x) \leqslant \sum_{j>n} \left[\frac{x}{p_j}\right] \leqslant \sum_{j>n} \frac{x}{p_j} < \frac{x}{2},$$

так что $f_S(x) \geqslant x/2$. С другой стороны, $f_S(x) \leqslant 2^n \sqrt{x}$. Эти неравенства означают, что $2^n \geqslant \sqrt{x}/2$. Последнее неравенство не выполняется при фиксированном n и достаточно большом x.

Тесно связанная с $\pi(x)$ функция определяется формулой $\theta(x) = \sum_{p \leqslant x} \ln p$, где сумма берется по всем простым числам, не превосходящим x. Мы воспользуемся функцией $\theta(x)$, чтобы ограничить $\pi(x)$ сверху. Положим $\theta(1) = 0$.

Предложение 2.4.3. $\theta(x) < (4 \ln 2)\, x$.

Доказательство. Рассмотрим биномиальный коэффициент

$$\binom{2n}{n} = \frac{(n+1)\ldots(2n)}{1 \cdot 2 \ldots n}.$$

Очевидно, что это целое число делится на все простые числа p, $n < p < 2n$. Далее, ввиду того, что

$$(1+1)^{2n} = \sum_{j=0}^{2n} \binom{2n}{j},$$

$2^{2n} > \binom{2n}{n}$. Следовательно,

$$2^{2n} > \binom{2n}{n} > \prod_{p>n}^{p<2n} p,$$

а потому

$$2n \ln 2 > \sum_{p>n}^{p<2n} \ln p = \theta(2n) - \theta(n).$$

Суммирование этих неравенств для $n = 1, 2, 4, 8, \ldots, 2^{m-1}$ приводит к неравенству

$$\theta(2^m) < (\ln 2)(2^{m+1} - 2) < (\ln 2)\, 2^{m+1}.$$

Если $2^{m-1} < x \leqslant 2^m$, то

$$\theta(x) \leqslant \theta(2^m) < (\ln 2)\, 2^{m+1} = (4 \ln 2)\, 2^{m-1} < (4 \ln 2)\, x. \quad \square$$

Следствие 1. *Существует такая положительная константа* c_1, *что* $\pi(x) < c_1 x/\ln x$ *для* $x \geqslant 2$.

Доказательство.

$$\theta(x) \geqslant \sum_{p>\sqrt{x}}^{p\leqslant x} \ln p \geqslant (\ln \sqrt{x})\,(\pi(x) - \pi(\sqrt{x})) \geqslant$$
$$\geqslant (\ln \sqrt{x})\,\pi(x) - \sqrt{x} \ln \sqrt{x}.$$

Таким образом,

$$\pi(x) \leqslant \frac{2\theta(x)}{\ln x} + \sqrt{x} \leqslant (8 \ln 2)\frac{x}{\ln x} + \sqrt{x}.$$

Наш результат следует теперь из неравенства $\sqrt{x} \leqslant 2x/\ln x$ для $x \geqslant 2$. $\square$

Следствие 2. $\pi(x)/x \to 0$ *при* $x \to \infty$.

Для ограничения $\pi(x)$ снизу мы начнем с более детального рассмотрения биномиального коэффициента $\binom{2n}{n}$. Прежде всего,

$$\binom{2n}{n} = \left(\frac{n+1}{1}\right)\left(\frac{n+2}{2}\right)\cdots\left(\frac{n+n}{n}\right) \geqslant 2^n.$$

С другой стороны, используя упр. 6 в конце этой главы, получаем

$$\operatorname{ord}_p \binom{2n}{n} = \operatorname{ord}_p \frac{(2n)!}{(n!)^2} = \sum_{j=1}^{t_p} \left(\left[\frac{2n}{p^j} \right] - 2 \left[\frac{n}{p^j} \right] \right),$$

где t_p — максимальное целое число с $p^{t_p} \leqslant 2n$, т. е. $t_p = \lfloor \ln 2n / \ln p \rfloor$. Далее, как нетрудно убедиться, $\lfloor 2x \rfloor - 2\lfloor x \rfloor$ всегда равно либо 1, либо 0. Поэтому

$$\operatorname{ord}_p \binom{2n}{n} \leqslant \frac{\ln 2n}{\ln p}.$$

Предложение 2.4.4. *Существует такая положительная константа c_2, что $\pi(x) > c_2 (x/\ln x)$.*

Доказательство. По предыдущему

$$2^n \leqslant \binom{2n}{n} \leqslant \prod_{p<2n} p^{t_p}.$$

Таким образом,

$$n \ln 2 \leqslant \sum_{p<2n} t_p \ln p = \sum_{p<2n} \left[\frac{\ln 2n}{\ln p} \right] \ln p.$$

Если $\ln p > (1/2) \ln 2n$, т. е. $p > \sqrt{2n}$, то $\lfloor \ln 2n / \ln p \rfloor = 1$. Поэтому

$$n \ln 2 \leqslant \sum_{p \leqslant \sqrt{2n}} \left[\frac{\ln 2n}{\ln p} \right] \ln p + \sum_{p > \sqrt{2n}}^{p<2n} \ln p \leqslant \sqrt{2n} \ln 2n + \theta(2n).$$

Отсюда следует, что $\theta(2n) \geqslant n \ln 2 - \sqrt{2n} \ln 2n$. Но $\sqrt{2n} \ln 2n / n$ стремится к 0 при $n \to \infty$, так что $\theta(2n) > Tn$ при некотором $T > 0$ и достаточно большом n. Записывая для большого x неравенства $2n \leqslant x < 2n + 1$, получаем $\theta(x) \geqslant \theta(2n) > Tn \geqslant T(x-1)/2 > Cx$ для подходящей константы C. Таким образом, существует такая константа $c_2 > 0$, что $\theta(x) \geqslant c_2 x$ для всех $x \geqslant 2$. Для завершения доказательства заметим, что

$$\theta(x) = \sum_{p \leqslant x} \ln p \leqslant \pi(x) \ln x.$$

Таким образом,

$$\pi(x) \geqslant \frac{\theta(x)}{\ln x} > c_2 \frac{x}{\ln x}. \qquad \square$$

Два предыдущих предложения были впервые доказаны Чебышёвым в 1852 г. Эти результаты примыкают к знаменитой теореме о распределении простых чисел, в которой утверждается,

что на самом деле $\pi(x)(\ln x/x) \to 1$ при $x \to \infty$. Как нетрудно убедиться, это эквивалентно тому, что $\theta(x)/x \to 1$ при $x \to \infty$. Теорема о распределении простых чисел была в несколько ином виде сформулирована в качестве гипотезы Гауссом, когда ему было 15 или 16 лет. Доказательство этой гипотезы было получено лишь в 1896 г. независимо Адамаром и де ла Валле-Пуссеном. В их доказательствах использованы комплексно-аналитические свойства дзета-функции Римана. Без использования комплексного анализа этот результат удалось доказать в 1948 г. Сельбергу.

Замечания

В теории простых чисел имеется масса нерешенных проблем. Например, неизвестно, бесконечно ли много простых чисел вида $n^2 + 1$. С другой стороны, как мы докажем в гл. 16, линейный многочлен $an + b$ всегда представляет бесконечно много простых чисел при условии, что $(a, b) = 1$. Это утверждение — знаменитая теорема Дирихле о простых числах в арифметической прогрессии.

Неизвестно, существует ли бесконечно много простых чисел вида $2^N + 1$, так называемых простых чисел Ферма, а также простых чисел вида $2^N - 1$, простых чисел Мерсенна.

Еще одна знаменитая проблема: существует ли бесконечно много простых чисел p, для которых $p + 2$ тоже простое? Известно, что сумма обратных значений множества таких простых чисел сходится [52].

Подробное обсуждение нерешенных проблем о простых числах можно найти в [71] и [70]. Читателю, знакомому с математическим анализом, рекомендуется работа [31], а также [38] и [39].

Ключевая идея доказательства теоремы 2 принадлежит Эйлеру. Хорошее изложение этого материала для начинающих имеется в [65].

Теорема 3 дает доказательство (в духе Эйлера) того факта, что $k[x]$ содержит бесконечно много неприводимых многочленов. Уже это наводит на мысль, что многие теоремы из классической теории чисел имеют аналоги в кольце $k[x]$. В действительности дело так и обстоит. Интересные ссылки по этому кругу вопросов имеются в [10].

Упомянутая выше теорема Дирихле была доказана для $k[x]$, где k — конечное поле, в [50]. Многообещающая карьера автора этой статьи Корнблюма оборвалась вскоре после того, как он добровольцем ушел в 1914 г. в армию. Теорема о распределении простых чисел также имеет аналог в $k[x]$. Это было доказано Артином в его диссертации [2].

Хорошим введением в аналитическую теорию чисел является книга [112]. В последней главе этой прекрасно читающейся

монографии приводится доказательство теоремы о распределении простых чисел, использующее комплексный анализ. Не использующие комплексный анализ, но достаточно сложные доказательства были получены в [215] и [133]. Интересное изложение истории этой теоремы см. в [139]. Наконец, мы рекомендуем замечательную брошюру [229]; эта книга объемом менее ста страниц содержит, в дополнение ко многим элементарным результатам о распределении простых чисел, доказательство Сельберга теоремы о простых числах, а также «элементарное» доказательство упомянутой выше теоремы Дирихле. См. также [198] (и [14*], [18*]. — *Ред.*).

Упражнения

1. Показать, что $k[x]$, где k — некоторое конечное поле, имеет бесконечно много неприводимых многочленов.

2. Пусть $p_1, p_2, \ldots, p_t \in \mathbf{Z}$ — некоторые простые числа. Рассмотрим множество всех рациональных чисел $r = a/b$, $a, b \in \mathbf{Z}$, для которых $\operatorname{ord}_{p_i} a \geqslant \operatorname{ord}_{p_i} b$ при $i = 1, 2, \ldots, t$. Показать, что это множество является кольцом и что с точностью до взятия ассоциированных $p_1, p_2, \ldots, p_t$ — единственные простые элементы в нем.

3. Используя формулу для $\varphi(n)$, дать доказательство того, что простых чисел бесконечно много. [*Указание.* Если $p_1, p_2, \ldots, p_t$ — все простые числа, то $\varphi(n) = 1$, где $n = p_1 p_2 \ldots p_t$.]

4. Если a — отличное от нуля целое число, то для $n > m$ показать, что $(a^{2^n} + 1,\ a^{2^m} + 1) = 1$ или 2 в зависимости от того, будет a нечетным или четным. [*Указание.* Если p — нечетное простое число и $p \mid a^{2^m} + 1$, то $p \mid a^{2^n} - 1$ при $n > m$.]

5. Используя результат упр. 4, показать, что существует бесконечно много простых чисел. [Это доказательство принадлежит Пойа.]

6. Для рационального числа r пусть $[r]$ — наибольшее целое число, меньшее или равное r, т. е. $[1/2] = 0$; $[2] = 2$ и $[3\,1/3] = 3$. Доказать, что $\operatorname{ord}_p n! = [n/p] + [n/p^2] + \ldots$.

7. Получить из упр. 6, что $\operatorname{ord}_p n! \leqslant n/(p-1)$ и что $\sqrt[n]{n!} \leqslant \prod_{p \mid n} p^{1/(p-1)}$.

8. Используя упр. 7, показать, что существует бесконечно много простых чисел. [*Указание.* $(n!)^2 \geqslant n^n$.] (Это доказательство принадлежит Коэну.)

9. Функция f на целых числах называется *мультипликативной*, если $f(ab) = f(a) f(b)$ при $(a, b) = 1$. Показать, что мультипликативная функция полностью определяется своими значениями на степенях простых чисел.

10. Если $f(n)$ — мультипликативная функция, то функция $g(n) = \sum_{d \mid n} f(d)$ тоже мультипликативна.

11. Показать, что $\varphi(n) = n \sum_{d \mid n} \mu(d)/d$, доказав сначала, что $\mu(d)/d$ мультипликативна, а затем использовав упр. 9 и 10.

12. Найти формулы для $\sum_{d \mid n} \mu(d)\varphi(d)$, $\sum_{d \mid n} \mu(d)^2 \varphi(d)^2$ и $\sum_{d \mid n} \mu(d)/\varphi(d)$.

13. Пусть $\sigma_k(n) = \sum_{d \mid n} d^k$. Показать, что $\sigma_k(n)$ мультипликативна, и найти для нее формулу.

14. Если $f(n)$ мультипликативна, то показать, что $h(n) = \sum_{d|n} \mu(n/d) f(d)$ тоже мультипликативна.

15. Показать, что

(a) $\sum_{d|n} \mu(n/d) \nu(d) = 1$ для всех n;

(b) $\sum_{d|n} \mu(n/d) \sigma(d) = n$ для всех n.

16. Показать, что $\nu(n)$ нечетно тогда и только тогда, когда n — квадрат.

17. Показать, что $\sigma(n)$ нечетно тогда и только тогда, когда n — квадрат или удвоенный квадрат.

18. Доказать, что $\varphi(n)\varphi(m) = \varphi((n, m))\varphi([n, m])$.

19. Доказать, что $\varphi(mn)\varphi((m, n)) = (m, n)\varphi(m)\varphi(n)$.

20. Доказать, что $\prod_{d|n} d = n^{\nu(n)/2}$

21. Положим $\Lambda(n) = \ln p$, если n — степень p, и $\Lambda(n) = 0$ в противном случае. Доказать, что $\sum_{d|n} \mu(n/d) \ln d = \Lambda(n)$. [*Указание.* Вычислить сначала $\sum_{d|n} \Lambda(d)$, а затем применить формулу обращения Мёбиуса.]

22. Показать, что сумма всех целых чисел t с $1 \leqslant t \leqslant n$ и $(t, n) = 1$ равна $(1/2) n\varphi(n)$.

23. Пусть $f(x) \in \mathbf{Z}[x]$ и $\psi(n)$ — число значений $f(j)$, $j = 1, 2, \ldots, n$, таких, что $(f(j), n) = 1$. Показать, что $\psi(n)$ мультипликативна и что $\psi(p^t) = p^{t-1}\psi(p)$. Вывести отсюда, что $\psi(n) = n \sum_{p|n} \psi(p)/p$.

24. Восстановить детали доказательства теоремы 3.

25. Рассмотрим функцию $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$. Она называется *дзета-функцией Римана*. Эта функция сходится для $s > 1$. Доказать формальное тождество (тождество Эйлера)

$$\zeta(s) = \prod_p (1 - (1/p^s))^{-1}.$$

Если допустить для s комплексные значения, то можно доказать, что $\zeta(s)$ имеет аналитическое продолжение на всю комплексную плоскость. В знаменитой гипотезе Римана утверждается, что все нули $\zeta(s)$ в полосе $0 \leqslant \operatorname{Re} s \leqslant 1$ лежат на прямой $\operatorname{Re} s = 1/2$.

26. Проверить формальные тождества

(a) $\zeta(s)^{-1} = \sum_{n=1}^{\infty} \mu(n)/n^s$;

(b) $\zeta(s)^2 = \sum_{n=1}^{\infty} \nu(n)/n^s$;

(c) $\zeta(s)\zeta(s-1) = \sum_{n=1}^{\infty} \sigma(n)/n^s$.

27. Показать, что ряд $\sum' 1/n$, где сумма берется по свободным от квадратов целым числам, расходится. Вывести отсюда, что $\prod_{p<N} (1 + 1/p) \to \infty$ при $N \to \infty$. Так как $e^x > 1 + x$, получить отсюда, что $\sum_{p<N} 1/p \to \infty$ при $N \to \infty$. (Это доказательство предложено Нивеном.)

Глава 3

СРАВНЕНИЯ

Понятие сравнения было введено впервые Гауссом в «Disquisitiones Arithmeticae» (*см. замечания в гл. 1*). *Несмотря на то что понятие это очень просто, его важность и полезность нельзя преувеличить.*

Эта глава посвящена изложению простейших свойств сравнений. В гл. 4 этот вопрос будет рассмотрен более глубоко.

§ 1. Элементарные наблюдения

Простое наблюдение показывает, что произведение двух нечетных чисел нечетно, произведение двух четных чисел четно и произведение нечетного и четного чисел четно. Отметим также, что сумма нечетных чисел четна, сумма четных чисел четна и сумма четного числа и нечетного числа нечетна. Эта информация сведена в табл. 1 и 2. Таблица 1 соответствует умножению, таблица 2 — сложению.

Таблица 1

	ч	н
ч	ч	ч
н	ч	н

Таблица 2

	ч	н
ч	ч	н
н	н	ч

Эти наблюдения настолько элементарны, что возникает вопрос о том, можно ли из них извлечь что-нибудь интересное. Ответ, как это ни странно, утвердительный.

Многие проблемы в теории чисел имеют такой вид: если f — некоторый многочлен от одной или нескольких переменных с целыми коэффициентами, то спрашивается, имеет ли уравнение $f = 0$ решения в целых числах? Такие вопросы рассматривались греческим математиком Диофантом и называются диофантовыми в его честь [1]).

[1] Тем не менее сам Диофант рассматривал решения неопределенных уравнений в рациональных числах. См. [13*], [3*]. — *Прим. ред.*

Рассмотрим уравнение $x^2 - 117x + 31 = 0$. Мы утверждаем, что у него не существует решения, являющегося целым числом. Пусть n — какое-либо целое число. Оно либо четно, либо нечетно. Если n четно, то четными будут n^2 и $117n$. Таким образом, $n^2 - 117n + 31$ нечетно. Если n нечетно, то n^2 и $117n$ оба нечетны. Таким образом, $n^2 - 117n + 31$ в этом случае тоже нечетно. Так как каждое целое число либо четно, либо нечетно, это показывает, что $n^2 - 117n + 31$ никогда не равно нулю.

В гл. 2 мы показали, что простых чисел бесконечно много. Мы покажем сейчас, что существует бесконечно много простых чисел, которые дают остаток 3 при делении на 4. Примеры таких чисел: 3, 7, 19 и 59.

Любое целое число при делении на 4 имеет остаток 0, 1, 2 или 3. Таким образом, нечетные числа будут иметь либо вид $4k + 1$, либо вид $4l + 3$. Произведение двух чисел вида $4k + 1$ опять имеет тот же вид:

$$(4k + 1)(4k' + 1) = 4(4kk' + k + k') + 1.$$

Отсюда следует, что целое число вида $4l + 3$ должно делиться на некоторое простое число вида $4l + 3$.

Предположим теперь, что имеется лишь конечное число положительных простых чисел вида $4l + 3$. Список их начинается с 3, 7, 11, 19, 23, ... Положим $p_1 = 7$, $p_2 = 11$, $p_3 = 19$ и т. д. Предположим, что p_m — наибольшее простое число такого вида, и положим $N = 4p_1p_2 \ldots p_m + 3$. Число N не делится ни на какое число p_i. Однако N имеет вид $4l + 3$ и поэтому должно делиться на какое-то простое число p вида $4l + 3$. Имеем $p > p_m$ — противоречие.

Очевидно, что в основе обоих приведенных рассуждений лежит некоторый общий принцип. Он исследуется в § 2.

§ 2. Сравнения в Z

Определение. Если $a, b, m \in \mathbf{Z}$ и $m \neq 0$, то мы говорим, что *a сравнимо с b по модулю m*, если m делит $b - a$. Это отношение записывается так: $a \equiv b \pmod{m}$.

Предложение 3.2.1.
(a) $a \equiv a \pmod{m}$.
(b) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$.
(c) *Если* $a \equiv b \pmod{m}$ *и* $b \equiv c \pmod{m}$, *то* $a \equiv c \pmod{m}$.

Доказательство.
(a) $a - a = 0$ и $m \mid 0$.
(b) Если $m \mid b - a$, то $m \mid a - b$.
(c) Если $m \mid b - a$ и $m \mid c - b$, то $m \mid c - a = (c - b) + (b - a)$. □

Предложение 3.2.1 показывает, что сравнимость по модулю m является отношением эквивалентности на множестве целых чисел. Если $a \in \mathbf{Z}$, то $\bar{a}$ обозначает множество целых чисел, сравнимых с a по модулю m, $\bar{a} = \{n \in \mathbf{Z} \mid n \equiv a\ (m)\}$. Другими словами, $\bar{a}$ есть множество целых чисел вида $a + km$.

Если $m = 2$, то $\bar{0}$ есть множество четных целых чисел и $\bar{1}$ — множество нечетных целых чисел.

Определение. Множество вида $\bar{a}$ называется *классом вычетов по модулю* m.

Предложение 3.2.2.
(a) $\bar{a} = \bar{b} \Leftrightarrow a \equiv b\ (m)$.
(b) $\bar{a} \neq \bar{b} \Leftrightarrow \bar{a} \cap \bar{b}$ *пусто.*
(c) *Имеется в точности* m *классов вычетов по модулю* m.

Доказательство. (a) Если $\bar{b} = \bar{a}$, то $a \in \bar{a} = \bar{b}$. Таким образом, $a \equiv b\ (m)$. Обратно, если $a \equiv b\ (m)$, то $a \in \bar{b}$. Если $c \equiv a\ (m)$, то $c \equiv b\ (m)$, что доказывает включение $\bar{a} \subseteq \bar{b}$. Так как $a \equiv b\ (m)$ означает, что $b \equiv a\ (m)$, то также $\bar{b} \subseteq \bar{a}$. Поэтому $\bar{a} = \bar{b}$.

(b) Если $\bar{a} \cap \bar{b}$ пусто, то очевидно, что $\bar{a} \neq \bar{b}$. Мы покажем, что из непустоты $\bar{a} \cap \bar{b}$ следует, что $\bar{a} = \bar{b}$. Пусть $c \in \bar{a} \cap \bar{b}$. Тогда $c \equiv a\ (m)$ и $c \equiv b\ (m)$: Отсюда следует, что $a \equiv b\ (m)$ и поэтому по п. (a) имеем $\bar{a} = \bar{b}$.

(c) Мы покажем, что $\bar{0}$, $\bar{1}$, $\bar{2}$, ..., $\overline{m-1}$ все различны и составляют полное множество классов вычетов по модулю m. Предположим, что $0 \leqslant k < l < m$. Равенство $\bar{k} = \bar{l}$ означает, что $k \equiv l\ (m)$, т. е. что m делит $l - k$. Так как $0 < l - k < m$, это невозможно. Поэтому $\bar{k} \neq \bar{l}$. Пусть теперь $a \in \mathbf{Z}$. Мы можем найти такие целые числа q и r, что $a = qm + r$, где $0 \leqslant r < m$. Отсюда следует, что $a = r\ (m)$, так что $\bar{a} = \bar{r}$. □

Определение. Множество классов вычетов по модулю m обозначается через $\mathbf{Z}/m\mathbf{Z}$.

Если $\bar{a_1}, \bar{a_2}, \ldots, \bar{a_m}$ — полное множество классов вычетов по модулю m, то $\{a_1, a_2, \ldots, a_m\}$ называется *полной системой вычетов по модулю* m.

Например, $\{0, 1, 2, 3\}$, $\{4, 9, 14, -1\}$ и $\{0, 1, -2, -1\}$ — полные системы вычетов по модулю 4.

Множество $\mathbf{Z}/m\mathbf{Z}$ можно превратить в кольцо, определив сложение и умножение естественным образом. Это достигается при помощи следующего предложения.

Предложение 3.2.3. *Если* $a \equiv c\ (m)$ *и* $b \equiv d\ (m)$, *то* $a + b \equiv c + d\ (m)$ *и* $ab \equiv cd\ (m)$.

Доказательство. Если $m \mid c - a$ и $m \mid d - b$, то $m \mid (c - a) + (d - b) = (c + d) - (a + b)$. Таким образом, $a + b \equiv c + d\ (m)$.

Заметим, что $cd - ab = c(d - b) + b(c - a)$. Таким образом, $m \mid cd - ab$ и $ab \equiv cd\ (m)$. □

Если $\bar{a}, \bar{b} \in \mathbf{Z}/m\mathbf{Z}$, то мы определяем $\bar{a} + \bar{b}$ как $\overline{a + b}$ и $\bar{a}\bar{b}$ как $\overline{ab}$.

Это определение на первый взгляд зависит от a и b. Мы должны показать, что результаты зависят лишь от классов вычетов, определяемых a и b. В этом нетрудно убедиться. Предположим, что $\bar{c} = \bar{a}$ и $\bar{d} = \bar{b}$. Мы должны показать, что $\overline{a + b} = \overline{c + d}$ и $\overline{ab} = \overline{cd}$, но это непосредственно следует из предложений 3.2.2 и 3.2.3.

Введенные определения превращают $\mathbf{Z}/m\mathbf{Z}$ в кольцо. Проверка этого факта предоставляется читателю.

Таблицы 3 и 4 в явном виде задают сложение и умножение в кольце $\mathbf{Z}/3\mathbf{Z}$. (Черточки над числами опущены.) Читателю рекомендуется построить подобные таблицы для $m = 4$, 5 и 6.

Таблица 3

Сложение

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Таблица 4

Умножение

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

При обсуждении арифметических проблем иногда бывает удобнее работать с кольцом $\mathbf{Z}/m\mathbf{Z}$, чем с понятием сравнимости по модулю m, а иногда наоборот. Мы будем выбирать способ интерпретации, сообразуясь с обстоятельствами.

Ранее было доказано, что многочлен $x^2 - 117x + 31$ не имеет целочисленных корней. Используя предыдущие рассмотрения, этот результат можно обобщить.

Если $a \equiv b\ (m)$, то $a^2 \equiv b^2\ (m)$, $a^3 = b^3\ (m)$ и вообще $a^n \equiv b^n\ (m)$. Отсюда следует, что если $p(x) \in \mathbf{Z}[x]$, то $p(a) \equiv p(b)\ (m)$. Все это вытекает из предложения 3.2.3.

Возьмем $m = 2$. Тогда a сравнимо либо с 0, либо с 1 по модулю 2 и или $p(a) \equiv p(0)\ (2)$, или $p(a) \equiv p(1)\ (2)$.

Если $p(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$, то $p(0) = a_n$ и $p(1) = a_0 + a_1 + \ldots + a_n$. Наши вычисления приводят

к такому результату: если $p(x) \in \mathbf{Z}[x]$ и $p(0)$ и $p(1)$ оба нечетны, то $p(x)$ не имеет целочисленных корней.

Многочлен $x^2 - 117x + 31$ имеет свободный член 31, а сумма его коэффициентов равна -85; оба эти числа нечетны. Другие примеры: $2x^2 + 2x + 1$ и $3x^3 + 2x^2 + x + 3$.

§ 3. Сравнение $ax \equiv b\ (m)$

Простейшим сравнением является $ax \equiv b\ (m)$. В этом параграфе мы выясняем условие разрешимости этого сравнения и, если оно разрешимо, даем формулу для числа решений.

Сначала следует дать определение того, что мы подразумеваем под числом решений сравнения. В самом общем виде пусть $f(x_1, \ldots, x_n)$ — некоторый многочлен от n переменных с целыми коэффициентами. Рассмотрим сравнение $f(x_1, \ldots, x_n) \equiv 0\ (m)$. Решение — это n-набор целых чисел $(a_1, \ldots, a_n)$, такой, что $f(a_1, a_2, \ldots, a_n) \equiv 0\ (m)$. Если $(b_1, \ldots, b_n)$ — другой n-набор, такой, что $b_i \equiv a_i\ (m)$ для $i = 1, \ldots, n$, то нетрудно видеть, что $f(b_1, \ldots, b_n) \equiv 0\ (m)$. Мы не хотим рассматривать эти два решения как существенно различные. Итак, два решения $(a_1, \ldots, a_n)$ и $(b_1, \ldots, b_n)$ называются *эквивалентными*, если $a_i \equiv b_i\ (m)$ для $i = 1, \ldots, n$. *Число решений* сравнения $f(x_1, \ldots, x_n) \equiv 0\ (m)$ определяется как число неэквивалентных решений.

Например, 3, 8 и 13 суть решения для $6x \equiv 3\ (15)$. Число 18 — тоже решение, но решение $x = 18$ эквивалентно решению $x = 3$.

Полезно взглянуть на излагаемый материал с другой точки зрения. Отображение из $\mathbf{Z}$ в $\mathbf{Z}/m\mathbf{Z}$, задаваемое соответствием $a \to \bar{a}$, является гомоморфизмом. Если $f(a_1, \ldots, a_n) \equiv 0\ (m)$, то $\bar{f}(\bar{a}_1, \ldots, \bar{a}_n) = \bar{0}$. Здесь $\bar{f}(x_1, \ldots, x_n) \in \mathbf{Z}/m\mathbf{Z}[x_1, \ldots, x_n]$ — многочлен, получающийся из f, если поставить черту над каждым коэффициентом многочлена f. Далее, можно убедиться в том, что классы эквивалентности решений сравнения $f(x_1, \ldots, x_n) \equiv 0\ (m)$ находятся во взаимно однозначном соответствии с решениями уравнения $\bar{f}(x_1, \ldots, x_n) = \bar{0}$ в кольце $\mathbf{Z}/m\mathbf{Z}$. Эта интерпретация числа решений сравнений встречается довольно часто.

Мы возвращаемся теперь к вопросу о числе решений сравнения $ax \equiv b\ (m)$.

Пусть $d > 0$ — наибольший общий делитель целых чисел a и m. Положим $a' = a/d$ и $m' = m/d$. Тогда a' и m' взаимно просты.

Предложение 3.3.1. *Сравнение $ax \equiv b\ (m)$ имеет решения тогда и только тогда, когда $d \mid b$. Если $d \mid b$, то имеется ровно d решений. Если x_0 — одно из них, то все другие решения — это $x_0 + m'$, $x_0 + 2m'$, ..., $x_0 + (d-1)m'$.*

Доказательство. Если x_0 — некоторое решение, то $ax_0 - b = my_0$ при некотором целом y_0. Таким образом, $ax_0 - my_0 = b$. Так как d делит $ax_0 - my_0$, мы должны иметь $d \mid b$.

Обратно, пусть $d \mid b$. Согласно лемме 4 из § 1 гл. 1, существуют такие целые числа x_0' и y_0', что $ax_0' - my_0' = d$. Положим $c = b/d$ и умножим обе части выписанного равенства на c. Тогда $a(x_0'c) - m(y_0'c) = b$. Положим $x_0 = x_0'c$. Тогда $ax_0 \equiv b\ (m)$.

Мы показали, что сравнение $ax \equiv b\ (m)$ имеет хотя бы одно решение тогда и только тогда, когда $d \mid b$.

Предположим, что x_0 и x_1 суть решения. Тогда из $ax_0 \equiv b\ (m)$ и $ax_1 \equiv b\ (m)$ следует, что $a(x_1 - x_0) \equiv 0\ (m)$. Таким образом, $m \mid a(x_1 - x_0)$ и $m' \mid a'(x_1 - x_0)$, а это означает, что $m' \mid x_1 - x_0$, т. е. $x_1 = x_0 + km'$ для некоторого целого k. Нетрудно убедиться в том, что любое число вида $x_0 + km'$ будет решением и что решения x_0, $x_0 + m'$, ..., $x_0 + (d-1)m'$ не эквивалентны. Пусть $x_1 = x_0 + km'$ — какое-нибудь решение. Существуют такие целые числа r и s, что $k = rd + s$ и $0 \leqslant s < d$. Таким образом, $x_1 = x_0 + sm' + rm$ и x_1 эквивалентно $x_0 + sm'$. Это завершает доказательство. □

В качестве примера рассмотрим еще раз сравнение $6x \equiv 3\ (15)$. Мы решаем сначала уравнение $6x - 15y = 3$. Деля на 3, получаем $2x - 5y = 1$. Пара $x = 3$, $y = 1$ является решением нашего уравнения. Таким образом, $x_0 = 3$ — решение сравнения $6x \equiv 3\ (15)$. Далее, $m = 15$ и $d = 3$, так что $m' = 5$. Тремя неэквивалентными решениями будут 3, 8 и 13.

Имеется два важных следствия предложения 3.3.1.

Следствие 1. *Если a и m взаимно просты, то сравнение $ax \equiv b\ (m)$ имеет одно и только одно решение.*

Доказательство. В этом случае $d = 1$, так что $d \mid b$ и имеется $d = 1$ решений. □

Следствие 2. *Если p — простое число и $a \not\equiv 0\ (p)$, то сравнение $ax \equiv b\ (p)$ имеет одно и только одно решение.*

Доказательство непосредственно получается из следствия 1. □

Следствия 1 и 2 можно интерпретировать в терминах кольца $\mathbf{Z}/m\mathbf{Z}$. Сравнение $ax \equiv b\ (m)$ эквивалентно уравнению $\bar{a}x = \bar{b}$ в кольце $\mathbf{Z}/m\mathbf{Z}$.

Каковы единицы кольца $\mathbf{Z}/m\mathbf{Z}$? Элемент $\bar{a} \in \mathbf{Z}/m\mathbf{Z}$ является единицей тогда и только тогда, когда уравнение $\bar{a}x = \bar{1}$ разрешимо. Сравнение $ax \equiv 1\ (m)$ разрешимо в том и только том случае,

когда $d \mid 1$, т. е. тогда и только тогда, когда a и m взаимно просты. Таким образом, $\bar{a}$ — единица, если и только если $(a, m) = 1$, откуда нетрудно получить, что в $\mathbf{Z}/m\mathbf{Z}$ имеется в точности $\varphi(m)$ единиц. [Определение функции $\varphi(m)$ см. в § 2 гл. 2.]

Если p — простое число и $\bar{a} \neq \bar{0}$ — элемент из $\mathbf{Z}/p\mathbf{Z}$, то $(a, p) = 1$. Таким образом, каждый ненулевой элемент в $\mathbf{Z}/p\mathbf{Z}$ будет единицей; это показывает, что $\mathbf{Z}/p\mathbf{Z}$ — поле.

Если m — не простое число, то $m = m_1 m_2$, где $0 < m_1, m_2 < m$. Таким образом, $\overline{m_1} \neq \bar{0}$, $\overline{m_2} \neq \bar{0}$, но $\overline{m_1}\,\overline{m_2} = \overline{m_1 m_2} = \overline{m} = \bar{0}$. Поэтому $\mathbf{Z}/m\mathbf{Z}$ — не поле.

Объединяя изложенное, получаем

Предложение 3.3.2. *Элемент $\bar{a} \in \mathbf{Z}/m\mathbf{Z}$ является единицей тогда и только тогда, когда $(a, m) = 1$. В $\mathbf{Z}/m\mathbf{Z}$ имеется в точности $\varphi(m)$ единиц. Кольцо $\mathbf{Z}/m\mathbf{Z}$ является полем в том и только том случае, когда m — простое число.*

Следствие 1 (теорема Эйлера). *Если $(a, m) = 1$, то $a^{\varphi(m)} \equiv 1\ (m)$.*

Доказательство. Единицы кольца $\mathbf{Z}/m\mathbf{Z}$ образуют группу порядка $\varphi(m)$. Если $(a, m) = 1$, то $\bar{a}$ — единица. Поэтому $\bar{a}^{\varphi(m)} = \bar{1}$, т. е. $a^{\varphi(m)} \equiv 1\ (m)$. □

Следствие 2 (малая теорема Ферма). *Если p — простое число и $p \nmid a$, то $a^{p-1} \equiv 1\ (p)$.*

Доказательство. Если $p \nmid a$, то $(a, p) = 1$. Таким образом, $a^{\varphi(p)} \equiv 1\ (p)$. Поскольку $\varphi(p) = p - 1$ для простого числа p, наш результат установлен. □

Многие результаты этого параграфа можно обобщить на области главных идеалов.

Понятия сравнимости и классов вычетов можно распространить на произвольное коммутативное кольцо. Предложение 3.3.1 справедливо в ОГИ; а именно сравнение $ax \equiv b\ (m)$ имеет решение тогда и только тогда, когда $d \mid b$, и решение единственно тогда и только тогда, когда a и m взаимно просты. Единственное отличие состоит в том, что число решений не обязательно конечно. В любом случае, используя этот результат, доказываем аналог части предложения 3.3.2 о том, что если R — ОГИ и $m \in R$ не является ни нулем, ни одной из единиц, то $R/(m)$ — поле в том и только том случае когда m — простой элемент.

В частности, если k — некоторое поле, то $k[x]/(f(x))$ будет полем тогда и только тогда, когда $f(x)$ неприводим.

§ 4. Китайская теорема об остатках

Если модуль m некоторого сравнения — составное число, то иногда бывает возможно свести сравнение по модулю m к системе более простых сравнений. Основная теорема этого типа — китайская теорема об остатках (теорема 1), которая доказывается ниже. Эта теорема справедлива для любой ОГИ (на самом деле даже в более общем случае) [1]). Однако мы будем продолжать работать в $\mathbf{Z}$ и предоставим читателю относительно простое упражнение по переносу доказательств на ОГИ.

Лемма 1. *Если числа $a_1, \ldots, a_l$ взаимно просты с m, то взаимно простым с m будет и $a_1 a_2 \ldots a_l$.*

Доказательство. $\bar{a}_i \in \mathbf{Z}/m\mathbf{Z}$ — единица. Поэтому единицей будет и $\bar{a}_1 \bar{a}_2 \ldots \bar{a}_l = \overline{a_1 a_2 \ldots a_l}$. По предложению 3.3.2 $a_1 a_2 \ldots a_l$ взаимно просто с m. □

Приведем другое доказательство. Если бы $a_1 a_2 \ldots a_l$ не было взаимно простым с m, то существовало бы некоторое простое число p, делящее их оба. Из того что $p \mid a_1 a_2 \ldots a_l$, следует, что $p \mid a_i$ при некотором i. Тогда $(a_i, m) \neq 1$, что противоречит предположению.

Лемма 2. *Предположим, что все числа $a_1, \ldots, a_t$ делят n и что $(a_i, a_j) = 1$ для $i \neq j$. Тогда $a_1, a_2 \ldots a_t$ делит n.*

Доказательство. Применим индукцию по t. Если $t = 1$, доказывать нечего. Пусть $t > 1$, и предположим, что лемма верна при $t - 1$. Тогда $a_1 a_2 \ldots a_{t-1}$ делит n. По лемме 1 число a_t взаимно просто с $a_1 a_2 \ldots a_{t-1}$. Поэтому существуют целые числа r и s, для которых $ra_t + sa_1 a_2 \ldots a_{t-1} = 1$. Умножая обе части этого равенства на n, убеждаемся в том, что левая его часть делится на $a_1 a_2 \ldots a_l$, откуда и следует доказываемый результат. □

Теорема 1 (китайская теорема об остатках). *Предположим, что $m = m_1 m_2 \ldots m_t$ и что $(m_i, m_j) = 1$ при $i \neq j$. Пусть $b_1, b_2, \ldots, b_t$ — целые числа, и рассмотрим систему сравнений*

$$x \equiv b_1 \ (m_1), \quad x \equiv b_2 \ (m_2), \ldots, \quad x \equiv b_t \ (m_t).$$

Эта система всегда имеет решения, и любые два решения отличаются на кратное числа m.

Доказательство. Положим $n_i = m/m_i$. Согласно лемме 1, $(m_i, n_i) = 1$. Поэтому существуют целые числа r_i и s_i, такие, что

[1]) См. предложение 12.3.1 гл. 12. — *Прим. ред.*

$r_i m_i + s_i n_i = 1$. Пусть $e_i = s_i n_i$. Тогда $e_i \equiv 1\ (m_i)$ и $e_i \equiv 0\ (m_j)$ при $j \neq i$.

Положим $x_0 = \sum_{i=1}^{t} b_i e_i$. Тогда $x_0 \equiv b_i e_i\ (m_i)$ и, следовательно, $x_0 \equiv b_i\ (m_i)$, т. е. x_0 — решение.

Предположим, что x_1 — некоторое другое решение. Тогда $x_1 - x_0 \equiv 0\ (m_i)$ для $i = 1, 2, \ldots, t$. Другими словами, $m_1, m_2, \ldots, m_t$ делят $x_1 - x_0$. По лемме 2 $x_1 - x_0$ делится на m. □

Приведем интерпретацию теоремы 1 с точки зрения теории колец. Если $R_1, R_2, \ldots, R_n$ — некоторые кольца, то $R_1 \oplus R_2 \oplus \ldots \oplus R_n = S$, прямая сумма колец R_i, определяется как множество n-наборов $(r_1, r_2, \ldots, r_n)$ с $r_i \in R_i$. Сложение и умножение определяются формулами

$$(r_1, r_2, \ldots, r_n) + (r_1', r_2', \ldots, r_n') = (r_1 + r_1', \ldots, r_n + r_n'),$$

$$(r_1, r_2, \ldots, r_n)(r_1', r_2', \ldots, r_n') = (r_1 r_1', r_2 r_2', \ldots, r_n r_n').$$

Нулевым элементом будет элемент $(0, 0, \ldots, 0)$, а единичным — элемент $(1, 1, \ldots, 1)$. Элемент $u \in S$ будет единицей тогда и только тогда, когда существует $v \in S$, такой, что $uv = 1$. Если $u = (u_1, \ldots, u_n)$ и $v = (v_1, \ldots, v_n)$, то из $uv = 1$ следует, что $u_i v_i = 1$ при $i = 1, \ldots, n$. Таким образом, u_i — единица для каждого i. Обратно, если u_i — единица для каждого i, то $u = (u_1, \ldots, u_n)$ — единица. Группу единиц кольца R будем обозначать через $U(R)$. Далее, $U(R_1) \times U(R_2) \times \ldots \times U(R_n)$ есть множество n-наборов $(u_1, u_2, \ldots, u_n)$ с единицами $u_i \in R_i$. Это множество является группой при покомпонентном умножении.

Предложение 3.4.1. *Если* $S = R_1 \oplus R_2 \oplus \ldots \oplus R_n$, *то* $U(S) = U(R_1) \times U(R_2) \times \ldots \times U(R_n)$.

Пусть $m_1, m_2, \ldots, m_t$ — попарно взаимно простые целые числа и ψ_i обозначает естественный гомоморфизм из $\mathbf{Z}$ в $\mathbf{Z}/m_i\mathbf{Z}$. Мы строим отображение ψ из $\mathbf{Z}$ в $\mathbf{Z}/m_1\mathbf{Z} \oplus \mathbf{Z}/m_2\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}/m_t\mathbf{Z}$ следующим образом: $\psi(n) = (\psi_1(n), \psi_2(n), \ldots, \psi_t(n))$ при всех $n \in \mathbf{Z}$. Нетрудно проверить, что ψ — кольцевой гомоморфизм. Чему равны ядро и образ ψ?

Равенство $(b_1, b_2, \ldots, b_t) = \psi(n)$ выполняется тогда и только тогда, когда $\psi_i(n) = b_i$ для $i = 1, \ldots, t$, т. е. $n \equiv b_i\ (m_i)$ для $i = 1, \ldots, t$. Китайская теорема об остатках гарантирует, что такое n всегда существует. Таким образом, ψ — эпиморфизм.

Равенство $\psi(n) = 0$ имеет место в том и только том случае, когда $n \equiv 0\ (m_i)$, $i = 1, \ldots, t$, т. е. тогда и только тогда, когда n делится на $m = m_1 m_2 \ldots m_t$, что непосредственно следует из леммы 2. Таким образом, ядро ψ совпадает с идеалом $m\mathbf{Z}$.

Мы установили следующий результат:

Теорема 1′. *Отображение* ψ *индуцирует изоморфизм между* $\mathbf{Z}/m\mathbf{Z}$ *и* $\mathbf{Z}/m_1\mathbf{Z} \oplus \mathbf{Z}/m_2\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}/m_t\mathbf{Z}$.

Следствие. $U(\mathbf{Z}/m\mathbf{Z}) \approx U(\mathbf{Z}/m_1\mathbf{Z}) \times \ldots \times U(\mathbf{Z}/m_t\mathbf{Z})$.

Доказательство. Это утверждение непосредственно следует из теоремы 1′ и предложения 3.4.1. □

Обе изоморфные группы из только что формулированного следствия конечны. Порядок первой из них равен $\varphi(m)$, а порядок второй есть $\varphi(m_1)\varphi(m_2)\ldots\varphi(m_t)$. Таким образом, $\varphi(m) = \varphi(m_1)\varphi(m_2)\ldots\varphi(m_t)$.

Пусть $m = p_1^{a_1}p_2^{a_2}\ldots p_t^{a_t}$ — разложение числа m на простые множители. Тогда $\varphi(m) = \varphi(p_1^{a_1})\varphi(p_2^{a_2})\ldots\varphi(p_t^{a_t})$. Для степени простого числа p^a имеем $\varphi(p^a) = p^a - p^{a-1}$, поскольку числа, меньшие p^a и взаимно простые с p^a, взаимно просты с p. Так как $p^a/p = p^{a-1}$ из чисел, меньших p^a, делятся на p, то $p^a - p^{a-1}$ таких чисел взаимно просто с p. Заметим, что $p^a - p^{a-1} = p^a(1 - 1/p)$. Отсюда следует, что $\varphi(m) = m\prod(1 - 1/p)$. Эта формула была доказана в гл. 2 другим способом.

Подведем итоги. Понятие сравнимости оказывается исключительно полезным при исследовании многих арифметических вопросов. Оно привело нас к рассмотрению кольца $\mathbf{Z}/m\mathbf{Z}$ и его группы единиц $U(\mathbf{Z}/m\mathbf{Z})$. Для более глубокого проникновения в структуру этих алгебраических объектов мы использовали запись $m = p_1^{a_1}a_2^{a_2}\ldots p_t^{a_t}$ и получили с помощью китайской теоремы об остатках следующие изоморфизмы:

$$\mathbf{Z}/m\mathbf{Z} \approx \mathbf{Z}/p_1^{a_1}\mathbf{Z} \oplus \mathbf{Z}/p_2^{a_2}\mathbf{Z} \oplus \ldots \oplus \mathbf{Z}/p_t^{a_t}\mathbf{Z},$$

$$U(\mathbf{Z}/m\mathbf{Z}) \approx U(\mathbf{Z}/p_1^{a_1}\mathbf{Z}) \times U(\mathbf{Z}/p_2^{a_2}\mathbf{Z}) \times \ldots \times U(\mathbf{Z}/p_t^{a_t}\mathbf{Z}).$$

Для степеней простых чисел исследование можно значительно продолжить.

Замечания

Читателю было бы полезно познакомиться с другими изложениями приведенного здесь основного материала. См., например, хорошо написанную книгу [22] и (вновь) [40]. См. также [61], [60], [52] и [77].

Интересное обсуждение различных способов изложения этого материала можно найти у Самюэля (Samuel P. Sur l'organization d'un cours d'arithmetique. — L'enseignment Math., 1967, v. 13,

р. 223—231). Более глубокое исследование сравнений проводится в первой главе книги [9]; в этой книге показано также, насколько теория сравнений полезна при решении вопроса о разрешимости уравнений в целых числах. Мы отметим также прекрасное изложение материала в [69].

Исторически понятие сравнений было впервые введено и систематически использовано Гауссом в «Disquisitiones Arithmeticae» [136]. Понятие сравнения является ярким примером полезности использования «правильного» обозначения.

Что касается китайской теоремы об остатках, то в [40] отмечается, что Бахман в [4] указывает, что Сунь Цзу знал об этом результате в первом веке нашей эры. Эта теорема поддается далеко идущим обобщениям. Должным образом сформулированная, она верна в любом кольце с единичным элементом. Как ни странно, доказать ее в общем случае не более трудно, чем в частном случае, рассмотренном нами (см. предложение 12.3.1).

Упражнения

1. Показать, что существует бесконечно много простых чисел, сравнимых с -1 по модулю 6.

2. Написать таблицы сложения и умножения для колец $\mathbf{Z}/5\mathbf{Z}$, $\mathbf{Z}/8\mathbf{Z}$ и $\mathbf{Z}/10\mathbf{Z}$.

3. Пусть abc — десятичное представление некоторого целого числа между 1 и 1000. Показать, что abc делится на 3 тогда и только тогда, когда $a + b + c$ делится на 3. Показать, что тот же результат верен при замене 3 на 9. Показать, что abc делится на 11 тогда и только тогда, когда $a - b + c$ делится на 11. Обобщить эти результаты на любое число, записанное в десятичной системе.

4. Показать, что уравнение $3x^2 + 2 = y^2$ не имеет решений в целых числах.

5. Показать, что уравнение $7x^2 + 2 = y^3$ не имеет решений в целых числах.

6. Пусть задано целое число $n > 0$. Множество целых чисел $a_1, a_2, \ldots, a_{\varphi(n)}$ называется *приведенной системой вычетов по модулю* n, если они попарно несравнимы по модулю n и $(a_i, n) = 1$ при всех i. Если $(a, n) = 1$, то доказать, что $aa_1, aa_2, \ldots, aa_{\varphi(n)}$ опять будет приведенной системой вычетов по модулю n.

7. Использовать упр. 6 для другого доказательства теоремы Эйлера о том, что $a^{\varphi(n)} \equiv 1\ (n)$ при $(a, n) = 1$.

8. Пусть p — некоторое нечетное простое число. Если $k \in \{1, 2, \ldots, p-1\}$, то показать, что существует единственное b_k в этом множестве, для которого $kb_k \equiv 1\ (p)$. Показать, что $k \neq b_k$ за исключением случаев, когда $k = 1$ или $k = p - 1$.

9. При помощи упр. 7 показать, что $(p-1)! \equiv -1\ (p)$. Этот результат известен как теорема Вильсона.

10. Если n — не простое число, то показать, что $(n-1)! \equiv 0\ (n)$ за исключением случая $n = 4$.

11. Пусть $a_1, a_2, \ldots, a_{\varphi(n)}$ — приведенная система вычетов по модулю n и N — число решений сравнения $x^2 \equiv 1\ (n)$. Доказать, что $a_1 a_2 \ldots a_{\varphi(n)} \equiv (-1)^{N/2}\ (n)$.

12. Пусть $\binom{p}{k} = p!/(k!\,(p-k)!)$ — биномиальный коэффициент и p — простое число. Показать, что если $1 \leqslant k \leqslant p-1$, то p делит $\binom{p}{k}$. Вывести отсюда, что $(a+1)^p \equiv a^p + 1\ (p)$.

13. При помощи упр. 12 дать другое доказательство теоремы Ферма о том, что $a^{p-1} \equiv 1\ (p)$ при $p \nmid a$.

14. Пусть p и q — такие различные нечетные простые числа, что $p - 1$ делит $q - 1$. Если $(n, pq) = 1$, то показать, что $n^{q-1} \equiv 1\ (pq)$.

15. Показать, что для любого нечетного простого числа p числитель числа $1 + 1/2 + 1/3 + \ldots + 1/(p-1)$ делится на p. [*Указание.* Воспользоваться упр. 8 и 9.]

16. Использовать доказательство китайской теоремы об остатках для решения системы сравнений $x \equiv 1\ (7)$, $x = 4\ (9)$, $x \equiv 3\ (5)$.

17. Пусть $f(x) \in \mathbf{Z}[x]$ и $n = p_1^{a_1} \ldots p_t^{a_t}$. Показать, что сравнение $f(x) \equiv 0\ (n)$ имеет решение тогда и только тогда, когда $f(x) \equiv 0\ \left(p_i^{a_i}\right)$ имеет решение для $i = 1, 2, \ldots, t$.

18. Пусть N — число решений сравнения $f(x) \equiv 0\ (n)$ и N_i — число решений сравнения $f(x) \equiv 0\ \left(p_i^{a_i}\right)$. Доказать, что $N = N_1 N_2 \ldots N_t$.

19. Если p — некоторое нечетное простое число, то показать, что 1 и -1 — единственные решения сравнения $x^2 \equiv 1\ \left(p^a\right)$.

20. Показать, что сравнение $x^2 \equiv 1\ \left(2^b\right)$ имеет одно решение при $b = 1$, два решения при $b = 2$ и 4 решения при $b \geqslant 3$.

21. Воспользоваться упр. 18—20 для нахождения числа решений сравнения $x^2 \equiv 1\ (n)$.

22. Сформулировать и доказать китайскую теорему об остатках для области главных идеалов.

23. Распространить понятие сравнимости на кольцо $\mathbf{Z}[i]$ и доказать, что $a + bi$ всегда сравнимо с 0 или 1 по модулю $1 + i$.

24. Распространить понятие сравнимости на кольцо $\mathbf{Z}[\omega]$ и доказать, что $a + b\omega$ всегда сравнимо с -1, 1 или 0 по модулю $1 - \omega$.

25. Пусть $\lambda = 1 - \omega \in \mathbf{Z}[\omega]$. Доказать, что если $\alpha \in \mathbf{Z}[\omega]$ и $\alpha \equiv 1\ (\lambda)$, то $\alpha^3 \equiv 1\ (9)$. [*Указание.* Показать сначала, что $3 = -\omega^2\lambda^2$.]

26. При помощи упр. 25 показать, что если $\xi, \eta, \zeta \in \mathbf{Z}[\omega]$ отличны от нуля и $\xi^3 + \eta^3 + \zeta^3 = 0$, то λ делит по крайней мере один из элементов ξ, η, ζ.

Глава 4

СТРУКТУРА ГРУППЫ $U(\mathbf{Z}/n\mathbf{Z})$

Введя понятие сравнения и обсудив некоторые его свойства и приложения, мы теперь рассмотрим эти вопросы более глубоко. Ключевым результатом здесь является существование примитивных корней по модулю простого числа. Эта теорема использовалась математиками еще до Гаусса, но он первый дал ее доказательство. В терминологии гл. 3 существование примитивных корней эквивалентно тому, что $U(\mathbf{Z}/p\mathbf{Z})$ — циклическая группа, если p — простое число. Используя этот факт, мы получим явное описание группы $U(\mathbf{Z}/n\mathbf{Z})$ при произвольном n.

§ 1. Примитивные корни и структура группы $U(\mathbf{Z}/n\mathbf{Z})$

Как было показано в гл. 3, $U(\mathbf{Z}/n\mathbf{Z}) \approx U(\mathbf{Z}/p_1^{a_1}\mathbf{Z}) \times \ldots \times U(\mathbf{Z}/p_l^{a_l}\mathbf{Z})$, если $n = p_1^{a_1}p_2^{a_2}\ldots p_l^{a_l}$. Следовательно, для определения структуры группы $U(\mathbf{Z}/n\mathbf{Z})$ достаточно рассмотреть случай $U(\mathbf{Z}/p^a\mathbf{Z})$, где p — простое число. Мы начнем с рассмотрения простейшего случая $U(\mathbf{Z}/p\mathbf{Z})$.

Так как $\mathbf{Z}/p\mathbf{Z}$ — поле, будет полезно иметь в распоряжении следующую простую лемму о полях.

Лемма 1. *Пусть $f(x) \in k[x]$ и k — некоторое поле. Предположим, что $\deg f(x) = n$. Тогда f имеет не более n различных корней.*

Доказательство проводится индукцией по n. Для $n = 1$ утверждение тривиально. Предположим, что лемма верна для многочленов степени $n - 1$. Если $f(x)$ не имеет корней в k, то все в порядке. Если α — некоторый корень, то $f(x) = r + q(x)(x - \alpha)$, где r — константа. Полагая $x = \alpha$, получаем $r = 0$. Таким образом, $f(x) = q(x)(x - \alpha)$ и $\deg q(x) = n - 1$. Если $\beta \neq \alpha$ — другой корень многочлена $f(x)$, то $0 = f(\beta) = (\beta - \alpha)\, q(\beta)$, откуда следует, что $q(\beta) = 0$. Так как по индукции $q(x)$ имеет не более $n - 1$ различных корней, то $f(x)$ имеет не более n различных корней. □

Следствие. *Пусть* $f(x),\ g(x) \in k[x]$ *и* $n = \deg f(x) = \deg g(x)$. *Если* $f(\alpha_i) = g(\alpha_i)$ *для* $n+1$ *различных элементов* $\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1}$, *то* $f(x) = g(x)$.

Доказательство. Надо применить лемму 1 к многочлену $f(x) - g(x)$. □

Предложение 4.1.1. $x^{p-1} - 1 \equiv (x-1)(x-2)\ldots(x-p+1)\ (p)$.

Доказательство. Если $\bar{a}$ обозначает класс вычетов целого числа a в $\mathbf{Z}/p\mathbf{Z}$, то утверждение нашего предложения эквивалентно следующему:

$$x^{p-1} - \bar{1} = (x-\bar{1})(x-\bar{2})\ldots(x-\overline{(p-1)})$$

в $\mathbf{Z}/p\mathbf{Z}$. Пусть $f(x) = (x^{p-1} - \bar{1}) - (x-\bar{1})(x-\bar{2})\ldots(x-\overline{(p-1)})$. Многочлен $f(x)$ имеет степень, меньшую $p-1$ (старшие члены сокращаются), и $p-1$ корней $\bar{1}, \bar{2}, \ldots, \overline{p-1}$ (малая теорема Ферма). Следовательно, $f(x)$ тождественно равен нулю. □

Следствие. $(p-1)! \equiv -1\ (p)$.

Доказательство. Надо положить $x = 0$ в предложении 4.1.1. □

Этот результат известен как теорема Вильсона. Нетрудно доказать, что если $n > 4$ — не простое число, то $(n-1)! \equiv 0\ (n)$ (см. упр. 10 в гл. 3). Следовательно, сравнение $(n-1)! \equiv -1\ (n)$ характеризует простые числа. Теорема Вильсона будет использована позднее при обсуждении вопроса о квадратичных вычетах.

Предложение 4.1.2. *Если* $d \mid p-1$, *то сравнение* $x^d \equiv 1\ (p)$ *имеет точно* d *решений.*

Доказательство. Пусть $dd' = p-1$. Тогда

$$\frac{x^{p-1}-1}{x^d-1} = \frac{(x^d)^{d'}-1}{x^d-1} = (x^d)^{d'-1} + (x^d)^{d'-2} + \ldots + x^d + 1 = g(x).$$

Поэтому

$$x^{p-1} - 1 = (x^d - 1)\, g(x)$$

и

$$x^{p-1} - \bar{1} = (x^d - \bar{1})\, \bar{g}(x).$$

Если бы $x^d - \overline{1}$ имел менее чем d корней, то, согласно лемме 1, правая часть написанного равенства имела бы менее чем $p - 1$ корней. Однако левая часть имеет $p - 1$ корней $\overline{1}, \overline{2}, \ldots, \overline{p-1}$. Таким образом, $x^d \equiv 1\ (p)$ имеет точно d корней, как и утверждалось. □

Теорема 1. *$U(\mathbf{Z}/p\mathbf{Z})$ — циклическая группа.*

Доказательство. Для $d \mid p - 1$ пусть $\psi(d)$ — число элементов в $U(\mathbf{Z}/p\mathbf{Z})$ порядка d. Согласно предложению 4.1.2, элементы группы $U(\mathbf{Z}/p\mathbf{Z})$, удовлетворяющие уравнению $x^d = \overline{1}$, образуют группу порядка d. Таким образом, $\sum_{c \mid d} \psi(c) = d$.

Применяя теорему обращения Мёбиуса, получаем $\psi(d) = \sum_{c \mid d} \mu(c)\, d/c$. Правая часть этого равенства равна $\varphi(d)$, как мы убедились при доказательстве предложения 2.2.5. В частности, $\psi(p-1) = \varphi(p-1)$, что больше 1, если $p > 2$. Так как случай $p = 2$ тривиален, то мы во всех случаях показали, что существует элемент [на самом деле $\varphi(p-1)$ элементов] порядка $p - 1$. □

Теорема 1 исключительно важна. Первым ее доказал Гаусс. Мы введем ряд новых понятий, а затем наметим в общих чертах два других доказательства.

Определение. Целое число a называется *примитивным корнем по модулю p*, если $\bar{a}$ порождает группу $U(\mathbf{Z}/p\mathbf{Z})$. Эквивалентным образом, a является примитивным корнем по модулю p, если $p - 1$ — наименьшее целое положительное число, для которого $a^{p-1} \equiv 1\ (p)$.

Например, 2 — примитивный корень по модулю 5, так как наименьшие положительные вычеты чисел $2, 2^2, 2^3, 2^4$ суть 2, 4, 3 и 1. Таким образом, $4 = 5 - 1$ — наименьшее положительное целое число n, для которого $2^n \equiv 1\ (5)$.

Для $p = 7$ число 2 не является примитивным корнем, так как $2^3 \equiv 1\ (7)$, а 3 будет таковым, так как $3, 3^2, 3^3, 3^4, 3^5$ и 3^6 сравнимы с 3, 2, 6, 4, 5 и 1 по модулю 7.

Хотя теорема 1 и доказывает существование примитивных корней для заданного простого числа, нет простого способа их нахождения. Для небольших простых чисел метод проб и ошибок, по всей вероятности, ничем не хуже любого другого метода.

В знаменитой гипотезе Артина утверждается, что если $a > 1$ не является квадратом, то имеется бесконечно много простых чисел, по модулю которых a — примитивный корень. Хотя в этом

направлении и был в последние годы достигнут некоторый прогресс, сама гипотеза все еще далека от разрешения (см. [35]).

Ввиду важности теоремы 1 мы приведем набросок двух других ее доказательств. Дополнить детали предоставляется читателю.

Пусть $p - 1 = q_1^{e_1} q_2^{e_2} \dots q_t^{e_t}$ — разложение числа $p - 1$ на простые множители. Рассмотрим сравнения

(1) $x^{q_i^{e_i - 1}} \equiv 1 \ (p)$;

(2) $x^{q_i^{e_i}} \equiv 1 \ (p)$.

Каждое решение сравнения (1) будет решением сравнения (2). Более того, сравнение (2) имеет больше решений, чем сравнение (1). Пусть g_i — некоторое решение сравнения (2), которое не является решением сравнения (1), и положим $g = g_1 g_2 \dots g_t$. Элемент $\overline{g_i}$ порождает подгруппу в $U(\mathbf{Z}/p\mathbf{Z})$ порядка $q_i^{e_i}$. Отсюда следует, что $\bar{g}$ порождает подгруппу в $U(\mathbf{Z}/p\mathbf{Z})$ порядка $q_1^{e_1} q_2^{e_2} \dots$ $\dots q_t^{e_t} = p - 1$. Таким образом, g — примитивный корень и группа $U(\mathbf{Z}/p\mathbf{Z})$ циклическая.

Наконец, по теоретико-групповым соображениям $\psi(d) \leqslant \varphi(d)$ для $d \mid p - 1$. Оба числа $\sum_{d \mid p-1} \psi(d)$ и $\sum_{d \mid p-1} \varphi(d)$ равны $p - 1$. Отсюда следует, что $\psi(d) = \varphi(d)$ при всех $d \mid p - 1$. В частности, $\psi(p - 1) = \varphi(p - 1)$. Для $p > 2$ неравенство $\varphi(p - 1) > 1$ означает, что $\psi(p - 1) > 1$. Отсюда и вытекает доказываемый результат.

Понятие примитивного корня можно обобщить.

Определение. Пусть a, $n \in \mathbf{Z}$. Число a называется *примитивным корнем по модулю* n, если класс вычетов a по модулю n порождает $U(\mathbf{Z}/n\mathbf{Z})$ [1]). Это эквивалентно требованию, чтобы a и n были взаимно просты и чтобы $\varphi(n)$ было наименьшим положительным целым числом, для которого $a^{\varphi(n)} \equiv 1 \ (n)$.

В общем случае не верно, что группа $U(\mathbf{Z}/n\mathbf{Z})$ циклическая. Например, элементами группы $U(\mathbf{Z}/8\mathbf{Z})$ будут $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$ и $\overline{1}^2 = \overline{1}$, $\overline{3}^2 = \overline{1}$, $\overline{5}^2 = \overline{1}$, $\overline{7}^2 = 1$. Таким образом, в ней нет элементов порядка $4 = \varphi(8)$. Отсюда следует, что не каждое целое число обладает примитивными корнями. Мы определим вскоре, какие целые числа ими обладают.

Лемма 2. *Если p — некоторое простое число и $1 \leqslant k < p$, то биномиальный коэффициент $\binom{p}{k}$ делится на p.*

[1]) Если для данного n существует примитивный корень по модулю n, то мы будем говорить, что n обладает примитивными корнями. — *Прим. перев.*

Доказательство. Мы дадим два доказательства.
(a) По определению

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!}, \text{ так что } p! = k!\,(p-k)!\binom{p}{k}.$$

Далее, p делит $p!$, но p не делит $k!\,(p-k)!$, так как последнее выражение есть произведение целых чисел, меньших p, а потому и взаимно простых с ним. Таким образом, p делит $\binom{p}{k}$.

(b) Согласно малой теореме Ферма, $a^{p-1} \equiv 1\ (p)$, если $p \nmid a$. Отсюда следует, что $a^p \equiv a\ (p)$ для всех a. В частности, $(1+a)^p \equiv 1 + a\ (p) \equiv 1 + a^p\ (p)$ для всех a. Таким образом, $(1+x)^p - 1 - x^p \equiv 0\ (p)$ имеет p решений. Так как выписанный многочлен имеет степень, меньшую чем p, из следствия леммы 1 получаем, что $(\overline{1}+x)^p - \overline{1} - x^p$ тождественно равен нулю в $\mathbf{Z}/p\mathbf{Z}\,[x]$. Но

$$(1+x)^p - 1 - x^p = \sum_{k=1}^{p-1} \binom{p}{k} x^k.$$

Таким образом, $\overline{\binom{p}{k}} = \overline{0}$ для $1 \leqslant k \leqslant p-1$, откуда следует, что $p \mid \binom{p}{k}$. Это доказательство привлекательно лишь тем, что не предполагается никакой информации о $\binom{p}{k}$. □

Лемма 3. *Если* $l \geqslant 1$ *и* $a \equiv b\ (p^l)$, *то* $a^p \equiv b^p\ (p^{l+1})$.

Доказательство. Мы можем записать $a = b + cp^l$, $c \in \mathbf{Z}$. Поэтому $a^p = b^p + \binom{p}{1} b^{p-1} cp^l + A$, где A — целое число, делящееся на p^{l+2}. Второй член, очевидно, делится на p^{l+1}. Следовательно, $a^p \equiv b^p\ (p^{l+1})$. □

Следствие 1. *Если* $l \geqslant 2$ *и* $p \neq 2$, *то* $(1+ap)^{p^{l-2}} \equiv 1 + ap^{l-1}\ (p^l)$ *для всех* $a \in \mathbf{Z}$.

Доказательство. Применим индукцию по l. При $l = 2$ утверждение тривиально. Предположим, что оно верно для некоторого $l \geqslant 2$. Мы покажем, что тогда оно верно для $l+1$. Применяя лемму 3, получаем

$$(1+ap)^{p^{l-1}} \equiv (1+ap^{l-1})^p\ (p^{l+1}).$$

По формуле бинома

$$(1+ap^{l-1})^p = 1 + \binom{p}{1} ap^{l-1} + B,$$

где B есть сумма $p-2$ членов. Используя лемму 2, нетрудно убедиться в том, что все эти члены делятся на $p^{1+2(l-1)}$, за исключением, быть может, последнего члена $a^p p^{p(l-1)}$. Так как $l \geqslant 2$, то $1+2(l-1) \geqslant l+1$, а так как также $p \geqslant 3$, то $p(l-1) \geqslant l+1$. Таким образом, $p^{l+1} \mid B$ и $(1+ap)^{p^{l-1}} \equiv 1+ap^l\ (p^{l+1})$, что и требовалось. □

Прежде чем сформулировать второе следствие, надо ввести одно определение.

Определение. Пусть $a,\ n \in \mathbf{Z}$ и $(a, n)=1$. Мы говорим, что a имеет *порядок e по модулю n*, если e есть наименьшее целое положительное число, для которого $a^e \equiv 1\ (n)$. Это эквивалентно тому, что $\bar{a}$ имеет порядок e в группе $U(\mathbf{Z}/n\mathbf{Z})$.

Следствие 2. *Если $p \neq 2$ и $p \nmid a$, то p^{l-1} есть порядок числа $1+ap$ по модулю p^l.*

Доказательство. Согласно следствию 1,

$$(1+ap)^{p^{l-1}} \equiv 1+ap^l\ (p^{l+1}),$$

откуда получаем, что $(1+ap)^{p^{l-1}} \equiv 1\ (p^l)$ и, таким образом, $1+ap$ имеет порядок, делящий p^{l-1}. С другой стороны, $(1+ap)^{p^{l-2}} \equiv 1+ap^{l-1}\ (p^l)$ показывает, что p^{l-2} не является порядком числа $1+ap$ (именно здесь мы используем предположение $p \nmid a$). Следствие доказано. □

Теперь мы в состоянии обобщить теорему 1. При этом оказывается, что мы должны рассматривать простое число 2 отдельно от нечетных простых чисел. В теории чисел необходимость рассматривать 2 отдельно от других простых чисел возникает довольно часто.

Теорема 2. *Если p — нечетное простое число и $l \in \mathbf{Z}^+$, то $U(\mathbf{Z}/p^l\mathbf{Z})$ — циклическая группа, т. е. существуют примитивные корни по модулю p^l.*

Доказательство. Согласно теореме 1, существуют примитивные корни по модулю p. Если $g \in \mathbf{Z}$ — примитивный корень по модулю p, то примитивным корнем по модулю p будет и $g+p$. Если $g^{p-1} \equiv 1\ (p^2)$, то

$$(g+p)^{p-1} \equiv g^{p-1}+(p-1)\ g^{p-2}\,p \equiv 1+(p-1)\,g^{p-2}\,p\ (p^2).$$

Так как p^2 не делит $(p-1)\,g^{p-2}p$, мы с самого начала можем предполагать, что g — такой примитивный корень по модулю p, для которого $g^{p-1} \neq 1\ (p^2)$.

Мы утверждаем, что уже такой элемент g будет примитивным корнем по модулю p^l. Для доказательства этого достаточно показать, что если $g^n \equiv 1\ (p^l)$, то $\varphi(p^l) = p^{l-1}(p-1) \mid n$.

Далее, $g^{p-1} = 1 + ap$, где $p \nmid a$. Согласно следствию 2 леммы 3, p^{l-1} есть порядок элемента $1 + ap$ по модулю p^l. Так как $(1 + ap)^n \equiv 1\ (p^l)$, то $p^{l-1} \mid n$.

Пусть $n = p^{l-1}n'$. Тогда

$$g^n = (g^{p^{l-1}})^{n'} \equiv g^{n'}\ (p)$$

и потому $g^{n'} \equiv 1\ (p)$. Так как g — примитивный корень по модулю p, то $p - 1 \mid n'$. Мы доказали, что $p^{l-1}(p-1) \mid n$, как и требовалось. □

Теорема 2'. *2^l обладает примитивным корнем при $l = 1$ или 2, но не при $l \geqslant 3$. Если $l \geqslant 3$, то $\{(-1)^a 5^b \mid a = 0,\ 1$ и $0 \leqslant b < 2^{l-2}\}$ составляет приведенную систему вычетов по модулю 2^l. Отсюда следует, что для $l \geqslant 3$ группа $U(\mathbf{Z}/2^l\mathbf{Z})$ является прямым произведением двух циклических групп, одной порядка 2, другой порядка 2^{l-2}.*

Доказательство. 1 — примитивный корень по модулю 2, 3 — примитивный корень по модулю 4. Начиная с этого места, будем предполагать, что $l \geqslant 3$.

Мы утверждаем, что

$$5^{2^{l-3}} \equiv 1 + 2^{l-1}\ (2^l). \tag{1}$$

Это верно при $l = 3$. Предположим, что сравнение (1) верно при $l \geqslant 3$, и докажем, что оно верно при $l + 1$. Заметим сначала, что $(1 + 2^{l-1})^2 = 1 + 2^l + 2^{2l-2}$ и что $2l - 2 \geqslant l + 1$ при $l \geqslant 3$. Применяя лемму 3 к сравнению (1), получаем

$$5^{2^{l-2}} \equiv 1 + 2^l\ (2^{l+1}). \tag{2}$$

Наше утверждение доказано по индукции.

Из (2) следует, что $5^{2^{l-2}} \equiv 1\ (2^l)$, тогда как из (1) получаем, что $5^{2^{l-3}} \not\equiv 1\ (2^l)$. Таким образом, 2^{l-2} — порядок числа 5 по модулю 2^l.

Рассмотрим множество $\{(-1)^a 5^b \mid a = 0,\ 1$ и $0 \leqslant b < 2^{l-2}\}$. Мы утверждаем, что эти 2^{l-1} чисел несравнимы по модулю 2^l. Так как $\varphi(2^l) = 2^{l-1}$, это покажет, что наше множество на самом деле является приведенной системой вычетов по модулю 2^l.

Если $(-1)^a 5^b \equiv (-1)^{a'} 5^{b'}\ (2^l)$, $l \geqslant 3$, то $(-1)^a \equiv (-1)^{a'}$ (4), откуда получаем, что $a \equiv a'\ (2)$. Таким образом, $a = a'$. Далее, из $a = a'$ следует, что $5^b \equiv 5^{b'}\ (2^l)$ или $5^{b-b'} \equiv 1\ (2^l)$. Поэтому $b \equiv b'\ (2^{l-2})$, откуда получаем, что $b = b'$.

Наконец, заметим, что $(-1)^a 5^b$ в степени 2^{l-2} сравнимо с 1 по модулю 2^l. Таким образом 2^l не обладает примитивными корнями, если $l \geqslant 3$. □

Рассмотрим ситуацию для модуля 8. Числа 1, 3, 5 и 7 представляют приведенную систему вычетов. Имеем $5^0 \equiv 1$, $5^1 \equiv 5$, $-5^0 \equiv 7$ и $-5^1 \equiv 3$. Табл. 1 представляет ситуацию для модуля 16. Вторая строка состоит из наименьших положительных вычетов степеней числа 5, а третья строка — из наименьших положительных вычетов взятых с минусом степеней числа 5.

Таблица 1

	5^0	5^1	5^2	5^3
+	1	5	9	13
−	15	11	7	3

Теоремы 2 и 2′ позволяют дать фактически полное описание группы $U(\mathbf{Z}/n\mathbf{Z})$ для произвольного n.

Теорема 3. *Пусть* $n = 2^a p_1^{a_1} p_2^{a_2} \ldots p_l^{a_l}$ *— разложение числа* n *на простые множители. Тогда*

$$U(\mathbf{Z}/n\mathbf{Z}) \approx U(\mathbf{Z}/2^a\mathbf{Z}) \times U(\mathbf{Z}/p_1^{a_1}\mathbf{Z}) \times \ldots \times U(\mathbf{Z}/p_l^{a_l}\mathbf{Z}).$$

Группа $U(\mathbf{Z}/p_i^{a_i}\mathbf{Z})$ *— циклическая группа порядка* $p_i^{a_i-1}(p_i - 1)$, *а* $U(\mathbf{Z}/2^a\mathbf{Z})$ *— циклическая группа порядка* 1 *или* 2 *при* $a = 1$ *или* 2 *соответственно. Если* $a \geqslant 3$, *то она будет прямым произведением двух циклических групп, одной порядка* 2, *другой порядка* 2^{a-2}.

Доказательство получается из теорем 2, 2′ и следствия теоремы 1′ гл. 3. □

Мы закончим этот параграф ответом на вопрос: какие целые числа обладают примитивными корнями?

Предложение 4.1.3. *Число* n *обладает примитивными корнями тогда и только тогда, когда оно имеет вид* 2, 4, p^a *или* $2p^a$, *где* p *— нечетное простое число.*

Доказательство. По теореме 2′ можно предположить, что $n \neq 2^l$, $l \geqslant 3$. Если n не является числом одного из перечисленных в предложении видов, то, как нетрудно видеть, оно может

быть записано в виде произведения m_1m_2, где $(m_1, m_2) = 1$ и $m_1, m_2 > 2$. Тогда число $\varphi(m_1)$ и $\varphi(m_2)$ оба четные и $U(\mathbf{Z}/m\mathbf{Z}) \approx \approx U(\mathbf{Z}/m_1\mathbf{Z}) \times U(\mathbf{Z}/m_2\mathbf{Z})$. Обе группы $U(\mathbf{Z}/m_1\mathbf{Z})$ и $U(\mathbf{Z}/m_2\mathbf{Z})$ имеют элементы порядка 2. Это показывает, что $U(\mathbf{Z}/n\mathbf{Z})$ не циклическая, так как циклическая группа содержит не более одного элемента порядка 2.

Как мы уже знаем, 2, 4 и p^a обладают примитивными корнями. Так как

$$U(\mathbf{Z}/2p^a\mathbf{Z}) \approx U(\mathbf{Z}/2\mathbf{Z}) \times U(\mathbf{Z}/p^a\mathbf{Z}) \approx U(\mathbf{Z}/p^a\mathbf{Z}),$$

то $U(\mathbf{Z}/2p^a\mathbf{Z})$ — циклическая группа, т. е. $2p^a$ обладает примитивными корнями. □

§ 2. n-степенные вычеты

Определение. Если $m, n \in \mathbf{Z}^+$, $a \in \mathbf{Z}$ и $(a, m) = 1$, то мы говорим, что a есть *n-степенной вычет* по модулю m, если разрешимо сравнение $x^n \equiv a\ (m)$.

Предложение 4.2.1. *Если $m \in \mathbf{Z}^+$ обладает примитивными корнями и $(a, m) = 1$, то a будет n-степенным вычетом по модулю m тогда и только тогда, когда*

$$a^{\varphi(m)/d} \equiv 1\ (m), \text{ где } d = (n, \varphi(m)).$$

Доказательство. Пусть g — некоторый примитивный корень по модулю m и $a \equiv g^b\ (m)$, $x \equiv g^y\ (m)$. Тогда сравнение $x^n \equiv \equiv a\ (m)$ эквивалентно сравнению $g^{ny} \equiv g^b\ (m)$, что в свою очередь эквивалентно сравнению $ny \equiv b\ (\varphi(m))$. Последнее сравнение разрешимо в том и только том случае, когда $d \mid b$. Более того, полезно заметить, что если оно имеет хотя бы одно решение, то оно имеет их точно d.

Если $d \mid b$, то $a^{\varphi(m)/d} \equiv g^{b\varphi(m)/d} \equiv 1\ (m)$. Обратно, если $a^{\varphi(m)/d} \equiv 1\ (m)$, то $g^{b\varphi(m)/d} \equiv 1\ (m)$; значит, $\varphi(m)$ делит $b\varphi(m)/d$, или $d \mid b$. Это завершает доказательство. □

Приведенное доказательство дает следующую дополнительную информацию. Если сравнение $x^n \equiv a\ (m)$ разрешимо, то оно имеет точно $(n, \varphi(m))$ решений.

Предположим теперь, что $m = 2^e p_1^{e_1} \dots p_l^{e_l}$. Тогда сравнение $x^n \equiv a\ (m)$ разрешимо в том и только том случае, когда разрешима система сравнений

$$x^n \equiv a\ (2^e),\quad x^n \equiv a\ (p_1^{e_1}), \dots,\ x^n \equiv a\ (p_l^{e_l}).$$

Так как степени нечетных простых чисел обладают примитивными корнями, мы можем к последним l сравнениям применить пред-

ложение 4.2.1. Все свелось к рассмотрению сравнения $x^n \equiv a\ (2^e)$. Так как 2 и 4 обладают примитивными корнями, мы можем далее считать, что $e \geqslant 3$.

Предложение 4.2.2. *Предположим, что a нечетно, $e \geqslant 3$, и рассмотрим сравнение $x^n \equiv a\ (2^e)$. Если n нечетно, решение всегда существует и единственно.*

Если n четно, то решение существует тогда и только тогда, когда $a \equiv 1\ (4)$, $a^{2^{e-2}/d} \equiv 1\ (2^e)$, где $d = (n, 2^{e-2})$. Если существует хотя бы одно решение, то их существует точно $2d$.

Доказательство. Предлагается провести его в качестве упражнения. Следует начать с представлений $a \equiv (-1)^s 5^t\ (2^e)$ и $x \equiv (-1)^y 5^z\ (2^e)$. □

Предложения 4.2.1 и 4.2.2 дают фактически удовлетворительный ответ на вопрос: когда некоторое целое число a будет n-степенным вычетом по модулю m? В некоторых случаях возможно продвинуться немного далее.

Предложение 4.2.3. *Пусть p — нечетное простое число, $p \nmid a$ и $p \nmid n$. Тогда, если разрешимо сравнение $x^n \equiv a\ (p)$, то разрешимо и сравнение $x^n \equiv a\ (p^e)$ при всех $e \geqslant 1$. Все эти сравнения имеют одинаковое число решений.*

Доказательство. Если $n = 1$, утверждение тривиально, поэтому можно предположить, что $n \geqslant 2$. Предположим, что сравнение $x^n \equiv a\ (p^e)$ разрешимо. Пусть x_0 — некоторое решение и $x_1 = x_0 + bp^e$. Короткое вычисление показывает, что $x_1^n \equiv x_0^n + nbp^e x_0^{n-1}\ (p^{e+1})$. Мы хотим найти решения для $x_1^n \equiv a\ (p^{e+1})$. Это эквивалентно нахождению такого целого числа b, что $nx_0^{n-1}b \equiv ((a - x_0^n)/p^e)\ (p)$. Заметим, что $(a - x_0^n)/p^e$ — целое число и что $p \nmid nx_0^{n-1}$. Таким образом, это сравнение однозначно разрешимо относительно b и при этом значении b имеем $x_1^n \equiv a\ (p^{e+1})$.

Если $x^n \equiv a\ (p)$ не имеет решений, то и $x^n \equiv a\ (p^e)$ не имеет решений. С другой стороны, если $x^n \equiv a\ (p)$ имеет решение, то его имеет и $x^n \equiv a\ (p^e)$, как мы только что видели. Согласно замечанию, следующему за предложением 4.2.1, число решений сравнения $x^n \equiv a\ (p^e)$ равно $(n, \varphi(p^e))$, если хотя бы одно решение этого сравнения существует. Если $p \nmid n$, то нетрудно убедиться в том, что $(n, \varphi(p)) = (n, \varphi(p^e))$ для всех $e \geqslant 1$. Это завершает доказательство. □

Как обычно, результат для степеней числа 2 более сложный.

Предложение 4.2.4. *Пусть 2^l — высшая степень числа 2, делящая n. Предположим, что a нечетно и что $x^n \equiv a\ (2^{2l+1})$ разрешимо. Тогда $x^n \equiv a\ (2^e)$ разрешимо для всех $e \geqslant 2l+1$ (a следовательно, для всех $e \geqslant 1$). Более того, все эти уравнения имеют одинаковое число решений.*

Доказательство предлагается провести в качестве упражнения. Следует начать с предположения о том, что $x^n \equiv a\ (2^m)$, $m \geqslant 2l+1$, имеет некоторое решение x_0. Пусть $x_1 = x_0 + b2^{m-1}$. При подходящем выборе b будем иметь $x_1^n \equiv a\ (2^{m+1})$. □

Заметим, что сравнение $x^2 \equiv 5\ (2^2)$ разрешимо (например, $x = 1$), а $x^2 \equiv 5\ (8)$ — нет. С другой стороны, из предложения 4.2.4 нетрудно получить, что если $a \equiv 1\ (8)$, то сравнение $x^2 \equiv a\ (2^e)$ разрешимо для всех e, и наоборот.

Замечания

Лемма 1 и ее важное следствие, предложение 4.1.1, восходят к Лагранжу (1768 г.).

Теорема Ферма [о том, что $a^{p-1} \equiv 1\ (p)$ при $p \nmid a$] была доказана впервые Эйлером. Теорема Вильсона была сформулирована Варингом и доказана Лагранжем.

Важный результат о существовании примитивных корней по модулю простого числа был анонсирован Эйлером и, как мы упоминали, был доказан впервые Гауссом. Доказательства этого результата можно модифицировать для получения более общего утверждения о том, что конечная подгруппа в мультипликативной группе некоторого поля всегда является циклической, т. е. порождается одним элементом.

Относительно примитивных корней существует много интересных гипотез. Знаменитая гипотеза Артина состоит в том, что если задано некоторое целое число a, не являющееся квадратом и не равное -1, то существует бесконечно много простых чисел, по модулю которых a — примитивный корень. В случае $a = 10$ это утверждение восходит к Гауссу и равносильно тому, что существует бесконечно много простых чисел p, для которых период десятичного представления числа $1/p$ имеет длину $p - 1$. (Введение в теорию десятичных представлений чисел см. в гл. 4 из [64].) Как блестящую обзорную статью, посвященную гипотезе Артина и смежным вопросам, отметим [35].

Лемер обнаружил (см. [54]) следующий любопытный факт. Первое простое число вида $326n^2 + 3$, по модулю которого 326 не является примитивным корнем, должно быть больше 10 миллионов. Там же упоминаются другие результаты такого же типа.

Было бы интересно узнать, с чем связано такое странное поведение чисел.

Можно поставить вопрос, какова величина наименьшего положительного примитивного корня по модулю p для некоторого фиксированного простого числа p. Эта проблема привела к большому количеству исследований. Вклад Хуа состоит в том, что число, о котором идет речь, меньше чем $2^{m+1}p^{1/2}$, где m — число различных простых чисел, делящих $p-1$. Обсуждение этой проблемы и хорошую библиографию см. в [31]. Другие интересные результаты и проблемы можно найти в [76] и [12].

Много исследований имеется по вопросу существования наборов последовательных целых чисел, каждое из которых является k-й степенью по модулю p. Рассмотрим простые числа вида $kt+1$. Основной результат, принадлежащий Брауэру, состоит в том, что при заданном положительном целом числе m для всех достаточно больших простых чисел p такого вида существуют m последовательных чисел $r, r+1, \ldots, r+m-1$, которые все будут k-ми степенями по модулю p. Вопрос о нахождении наименьшего такого r при заданных p и m является проблемой, постоянно привлекающей внимание. Этот вопрос, а также обсуждение других открытых вопросов см. в статье [59].

Для заданного простого числа p можно поставить вопрос о величине наименьшего положительного числа, которое не является квадратом по модулю p. Интересная гипотеза состоит в следующем: для фиксированного n целое число, о котором идет речь, меньше, чем $\sqrt[n]{p}$, для всех достаточно больших p. Дополнительные данные см. в [31] и в гл. 3 из [18].

Наконец, упомянем, что аналог гипотезы Артина о примитивных корнях в кольце $k[x]$ был фактически доказан Билхарцем [8]. Билхарц доказал свою теорему в предположении, что гипотеза Римана справедлива для так называемой конгруэнц-дзета-функции (см. гл. 11). Это на самом деле и было доказано несколько лет спустя А. Вейлем. В последнее время Хули доказал, что первоначальная гипотеза Артина выполняется в предположении, что в полях алгебраических чисел справедлива расширенная гипотеза Римана [46]. Обсуждение классической гипотезы Римана и ее следствий см. в [18]. По-видимому, в настоящее время никто не имеет хоть какой-нибудь идеи по поводу того, как доказывать гипотезу Римана для полей алгебраических чисел, так что Хули оказался в не столь удачном положении, как Билхарц.

Упражнения

1. Показать, что 2 — примитивный корень по модулю 29.
2. Вычислить все примитивные корни по модулю $p = 11, 13, 17$ и 19.

3. Предположим, что a — примитивный корень по модулю p^n, p — нечетное простое число. Показать, что a — примитивный корень по модулю p.

4. Рассмотрим некоторое простое число p вида $4t + 1$. Показать, что a — примитивный корень по модулю p тогда и только тогда, когда $-a$ — примитивный корень по модулю p.

5. Рассмотрим простое число p вида $4t + 3$. Показать, что a является примитивным корнем по модулю p в том и только том случае, когда $-a$ имеет порядок $(p - 1)/2$.

6. Показать, что если $p = 2^n + 1$ — простое число Ферма, то 3 — примитивный корень по модулю p.

7. Предположим, что p — простое число вида $8t + 3$ и что $q = (p - 1)/2$ тоже простое число. Показать, что 2 — примитивный корень по модулю p.

8. Пусть p — некоторое нечетное простое число. Показать, что a является примитивным корнем по модулю p тогда и только тогда, когда $a^{(p-1)/q} \not\equiv 1\ (p)$ для всех простых делителей q числа $p - 1$.

9. Показать, что произведение всех примитивных корней по модулю p сравнимо с $(-1)^{\varphi(p-1)}$ по модулю p.

10. Показать, что сумма всех примитивных корней по модулю p сравнима с $\mu(p - 1)$ по модулю p.

11. Доказать, что $1^k + 2^k + \ldots + (p - 1)^k \equiv 0\ (p)$, если $p - 1 \nmid k$, и $\equiv -1\ (p)$, если $p - 1 \mid k$.

12. Воспользоваться существованием примитивного корня для другого доказательства теоремы Вильсона о том, что $(p - 1)! \equiv -1\ (p)$.

13. Пусть G — конечная циклическая группа и $g \in G$ — какой-то ее образующий. Показать, что все другие ее образующие будут иметь вид g^k, где $(k, n) = 1$, причем n — порядок группы G.

14. Пусть A — конечная абелева группа и a и b — элементы порядков m и n соответственно. Доказать, что если $(m, n) = 1$, то ab имеет порядок mn.

15. Пусть K — поле и $G \subseteq K^*$ — конечная подгруппа мультипликативной группы этого поля. С помощью аргументов, использованных при доказательстве теоремы 1, показать, что G — циклическая группа.

16. Найти решения сравнений $x^3 \equiv 1$ (19) и $x^4 \equiv 1$ (17).

17. Воспользоваться тем, что 2 — примитивный корень по модулю 29 для нахождения семи решений сравнения $x^7 \equiv 1$ (29).

18. Решить сравнение $1 + x + x^2 + \ldots + x^6 \equiv 0$ (29).

19. Найти числа a, для которых сравнение $x^3 \equiv a\ (p)$ разрешимо при $p = 7$, 11 и 13.

20. Пусть p — некоторое простое число и d — делитель $p - 1$. Показать, что d-е степени образуют подгруппу в $U(\mathbf{Z}/p\mathbf{Z})$ порядка $(p - 1)/d$. Вычислить эту подгруппу для $p = 11$, $d = 5$; $p = 17$, $d = 4$; $p = 19$, $d = 6$.

21. Если g — некоторый примитивный корень по модулю p и $d \mid p - 1$, то показать, что $g^{(p-1)/d}$ имеет порядок d. Показать также, что a будет d-й степенью тогда и только тогда, когда $a \equiv g^{kd}\ (p)$ при некотором k. Проделать упр. 16—20, используя эти замечания.

22. Показать, что если a имеет порядок 3 по модулю p, то $1 + a$ имеет порядок 6.

23. Показать, что $x^2 \equiv -1\ (p)$ имеет решение тогда и только тогда, когда $p \equiv 1$ (4), и $x^4 = -1\ (p)$ имеет решение тогда и только тогда, когда $p \equiv 1$ (8).

24. Показать, что $ax^m + by^n \equiv c\ (p)$ имеет то же число решений, что и $ax^{m'} + by^{n'} \equiv c\ (p)$, где $m' = (m, p - 1)$ и $n' = (n, p - 1)$.

25. Доказать предложения 4.2.2 и 4.2.4.

Глава 5

КВАДРАТИЧНЫЙ ЗАКОН ВЗАИМНОСТИ

Вопрос о разрешимости сравнения $x^2 \equiv a\ (p)$ *для простого числа* p *достаточно прост. Оно разрешимо тогда и только тогда, когда* $a^{(p-1)/2} \equiv 1\ (p)$ [1]. *Дальнейший полный анализ при знании этого факта — несложное дело. Однако при обращении поставленного вопроса проблема значительно усложняется. Предположим, что* a *— целое число. Для каких простых чисел* p *разрешимо сравнение* $x^2 \equiv a\ (p)$? *Ответ дается квадратичным законом взаимности. Сформулирован этот закон был Эйлером и Лежандром, но лишь Гаусс впервые дал полное его доказательство. Этим результатом Гаусс был в высшей степени горд. Он назвал его* «Theorema Aureum» (*золотая теорема*).

§ 1. Квадратичные вычеты

Пусть $(a, m) = 1$. Тогда a называется *квадратичным вычетом по модулю* m, если разрешимо сравнение $x^2 \equiv a\ (m)$. Если же оно неразрешимо, то a называется *квадратичным невычетом по модулю* m.

Например, 2 — квадратичный вычет по модулю 7, а 3 — нет. Действительно, 1^2, 2^2, 3^2, 4^2, 5^2 и 6^2 сравнимы с 1, 4, 2, 2, 4 и 1 соответственно. Таким образом, 1, 2 и 4 — квадратичные вычеты, а 3, 5 и 6 — нет.

Для любого фиксированного положительного числа m квадратичные вычеты можно определить, просто перечислив положительные целые числа, меньшие и взаимно простые с m, возведя их в квадрат и приведя затем по модулю m. Это и было только что нами проделано для $m = 7$.

Менее утомительный способ решения вопроса о том, является ли данное целое число квадратичным вычетом по модулю m, дается следующим предложением.

Предложение 5.1.1. *Пусть* $m = 2^e p_1^{e_1} \dots p_l^{e_l}$ *— разложение числа* m *на простые множители, и предположим, что* $(a, m) = 1$.

[1]) Здесь нужно предположить, что $a \not\equiv 0\ (p)$ и $p > 2$. См. ниже предложение 5.1.1. — *Прим. ред.*

Тогда $x^2 \equiv a\ (m)$ *разрешимо в том и только том случае, когда выполняются следующие условия*:

(a) *Если* $e = 2$, *то* $a \equiv 1\ (4)$;
если $e \geqslant 3$, *то* $a \equiv 1\ (8)$.

(b) *Для каждого* i *имеем* $a^{(p_i-1)/2} \equiv 1\ (p_i)$.

Доказательство. Ввиду китайской теоремы об остатках сравнение $x^2 \equiv a\ (m)$ эквивалентно системе

$$x^2 \equiv a\ (2^e), \quad x^2 \equiv a\ (p_1^{e_1}), \ldots, \quad x^2 \equiv a\ (p_l^{e_l}).$$

Рассмотрим сравнение $x^2 \equiv a\ (2^e)$. Ясно, что 1 — единственный квадратичный вычет по модулю 4 и 1 — единственный квадратичный вычет по модулю 8. Таким образом, это сравнение разрешимо тогда и только тогда, когда $a \equiv 1\ (4)$ при $e = 2$ и $a \equiv 1\ (8)$ при $e = 3$. Прямое применение предложения 4.2.4. показывает, что $x^2 \equiv a\ (8)$ разрешимо в том и только том случае, когда $x^2 \equiv a\ (2^e)$ разрешимо для всех $e \geqslant 3$.

Рассмотрим теперь сравнение $x^2 \equiv a\ (p_i^{e_i})$. Так как $(2, p_i) = 1$, из предложения 4.2.3 следует, что оно разрешимо тогда и только тогда, когда $x^2 \equiv a\ (p_i)$ разрешимо. К последнему сравнению применяем предложение 4.2.1 с $n = 2$, $m = p_i$ и $d = (n, \varphi(m)) = (2, p_i - 1) = 2$. Получаем, что $x^2 \equiv a\ (p_i)$ разрешимо в том и только том случае, когда $a^{(p_i-1)/2} \equiv 1\ (p_i)$. □

Этот результат сводит вопросы о квадратичных вычетах к соответствующим вопросам для простых модулей. В дальнейшем p будет обозначать некоторое нечетное простое число.

Определение. Символ (a/p) имеет значение 1, если a — квадратичный вычет по модулю p, -1, если a — квадратичный невычет по модулю p, и нуль, если $p \mid a$. Он называется *символом Лежандра*.

Символ Лежандра — в высшей степени удобный инструмент при рассуждениях о квадратичных вычетах. Мы перечислим некоторые из его свойств.

Предложение 5.1.2.

(a) $a^{(p-1)/2} \equiv (a/p)\ (p)$.

(b) $(ab/p) = (a/p)\,(b/p)$.

(c) *Если* $a \equiv b\ (p)$, *то* $(a/p) = (b/p)$.

Доказательство. Если p делит a или b, то все три утверждения тривиальны. Предположим, что $p \nmid a$ и $p \nmid b$.

Мы знаем, что $a^{p-1} \equiv 1\ (p)$; поэтому

$$(a^{(p-1)/2} + 1)\,(a^{(p-1)/2} - 1) = a^{p-1} - 1 \equiv 0\ (p).$$

Отсюда следует, что $a^{(p-1)/2} \equiv \pm 1\ (p)$. Согласно предложению 5.1.1, $a^{(p-1)/2} \equiv 1\ (p)$ тогда и только тогда, когда a — квадратичный вычет по модулю p. Это доказывает ч. (a).

Для доказательства ч. (b) применим ч. (a). Имеем

$$(ab)^{(p-1)/2} \equiv \left(\frac{ab}{p}\right)\ (p),$$

$$(ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\ (p).$$

Таким образом, $(ab/p) \equiv (a/p)(b/p)\ (p)$, откуда следует, что $(ab/p) = (a/p)(b/p)$.

Часть (c) очевидна из определения. □

Следствие 1. *Вычетов и невычетов по модулю p имеется одинаковое количество* [1]).

Доказательство. Сравнение $a^{(p-1)/2} \equiv 1\ (p)$ имеет $(p-1)/2$ решений. Поэтому имеется $(p-1)/2$ вычетов и $p - 1 - ((p-1)/2) = (p-1)/2$ невычетов. □

Следствие 2. *Произведение двух вычетов будет вычетом, произведение двух невычетов будет вычетом и произведение вычета и невычета будет невычетом.*

Доказательство. Все это легко получается из ч. (b). □

Следствие 3. $(-1)^{(p-1)/2} = (-1/p)$.

Доказательство. Следует подставить $a = -1$ в ч. (a). □

Особенно интересно следствие 3. Каждое нечетное целое число имеет вид $4k + 1$ или $4k + 3$. Используя это, следствие 3 можно переформулировать таким образом: $x^2 \equiv (-1)\ (p)$ имеет решение тогда и только тогда, когда p имеет вид $4k + 1$. Таким образом, -1 будет вычетом по модулю простых чисел 5, 13, 17, 29, ... и невычетом по модулю простых чисел 3, 7, 11, 19, ... Читателю рекомендуется проверить некоторые из этих утверждений, проведя соответствующие вычисления.

Этот результат приводит к постановке более общего вопроса. Пусть a — некоторое целое число. Для каких p оно будет квадратичным вычетом по модулю p? Ответ на этот вопрос дается квадратичным законом взаимности, к формулировке и доказательству которого мы вскоре перейдем.

---

[1]) В оставшейся части этой главы «вычет» и «невычет» означают соответственно квадратичный вычет и квадратичный невычет.

Следствие 3 дает возможность доказать, что существует бесконечно много простых чисел вида $4k + 1$. Предположим, что $p_1, p_2, \ldots, p_m$ — какое-то конечное множество таких чисел, и рассмотрим $(2p_1p_2 \ldots p_m)^2 + 1$. Предположим, что p делит это целое число. Тогда -1 будет квадратичным вычетом по модулю p и, следовательно, p будет иметь вид $4k + 1$. Но p не находится среди чисел p_i, так как $(2p_1p_2 \ldots p_m)^2 + 1$ дает остаток 1 при делении на p_i. Мы доказали, что каждое конечное множество простых чисел вида $4k + 1$ не содержит некоторого числа этого вида. Таким образом, множество таких простых чисел бесконечно.

Возвращаясь к теории квадратичных вычетов, мы хотим ввести теперь другую характеризацию символа (a/p), которая была получена Гауссом.

Рассмотрим множество $S = \{-(p-1)/2, -(p-3)/2, \ldots, -1, 1, 2, \ldots, (p-1)/2\}$. Оно называется *множеством наименьших вычетов по модулю* p. При $p \nmid a$ пусть μ обозначает число тех наименьших вычетов чисел $a, 2a, 3a, \ldots, ((p-1)/2)\,a$, которые отрицательны. Например, пусть $p = 7$ и $a = 4$. Тогда $(p-1)/2 = 3$ и $1 \cdot 4$, $2 \cdot 4$ и $3 \cdot 4$ сравнимы с -3, 1 и -2 соответственно. Таким образом, в этом случае $\mu = 2$.

Лемма (лемма Гаусса). $(a/p) = (-1)^{\mu}$.

Доказательство. Пусть $\pm m_l$ — наименьший вычет для la, где m_l положительно. Когда l пробегает значения между 1 и $(p-1)/2$, μ будет числом получившихся при этом знаков минус. Мы утверждаем, что $m_l \neq m_k$ для $l \neq k$ и $1 \leqslant l,\ k \leqslant (p-1)/2$. Действительно, если $m_l = m_k$, то $la \equiv \pm ka\ (p)$, и из $p \nmid a$ следует, что $l \pm k \equiv 0\ (p)$. Последнее сравнение невозможно, так как $l \neq k$ и $|\, l \pm k \,| \leqslant l + k \leqslant p - 1$. Отсюда вытекает, что множества $\{1, 2, \ldots, (p-1)/2\}$ и $\{m_1, m_2, \ldots, m_{(p-1)/2}\}$ совпадают. Перемножая сравнения $1 \cdot a \equiv \pm m_1\ (p)$, $2 \cdot a \equiv \pm m_2\ (p)$, ..., $((p-1)/2) \cdot a \equiv \pm m_{(p-1)/2}\ (p)$, получаем

$$\left(\frac{p-1}{2}\right)!\, a^{(p-1)/2} \equiv (-1)^{\mu} \left(\frac{p-1}{2}\right)!\ (p).$$

Значит, $a^{(p-1)/2} \equiv (-1)^{\mu}\ (p)$. Согласно предложению 5.1.2, $a^{(p-1)/2} \equiv (a/p)\ (p)$, откуда и следует доказываемый результат. □

Лемма Гаусса — очень мощный инструмент. Наше первое доказательство квадратичного закона взаимности мы проведем на ее основе. Прежде чем приступить к этому, мы уже сейчас можем дать характеризацию тех простых чисел, по модулю которых 2 является квадратичным вычетом.

Предложение 5.1.3. *Число 2 будет квадратичным вычетом по модулю простых чисел вида $8k + 1$ и $8k + 7$. Оно будет квадра-*

тичным невычетом по модулю простых чисел вида $8k + 3$ *и* $8k + 5$. *Эта информация суммируется формулой*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Доказательство. Мы предоставляем читателю показать, что приведенная формула эквивалентна первым двум утверждениям.

Пусть p — некоторое нечетное простое число (как обычно), и заметим, что число μ равно числу элементов множества $2 \cdot 1$, $2 \cdot 2$, ..., $2 \cdot (p-1)/2$, которые превосходят $(p-1)/2$. Пусть m определяется двумя условиями: $2m \leqslant (p-1)/2$ и $2(m+1) > (p-1)/2$. Тогда $\mu = ((p-1)/2) - m$.

Если $p = 8k + 1$, то $(p-1)/2 = 4k$ и $m = 2k$. Таким образом, $\mu = 4k - 2k = 2k$ четно и $(2/p) = 1$.

Если $p = 8k + 7$, то $(p-1)/2 = 4k + 3$, $m = 2k + 1$ и $\mu = 4k + 3 - (2k + 1) = 2k + 2$ четно. Таким образом, $(2/p) = 1$ и в этом случае.

Если $p = 8k + 3$, то $(p-1)/2 = 4k + 1$, $m = 2k$ и $\mu = 4k + 1 - 2k = 2k + 1$ нечетно. Таким образом, $(2/p) = -1$.

Наконец, если $p = 8k + 5$, то $(p-1)/2 = 4k + 2$, $m = 2k + 1$ и $\mu = 4k + 2 - (2k + 1) = 2k + 1$ нечетно. Таким образом, $(2/p) = -1$, и доказательство завершено. □

В качестве примера рассмотрим $p = 7$ и $p = 17$. Эти простые числа сравнимы с 7 и 1 по модулю 8 соответственно и, действительно, $3^2 \equiv 2\ (7)$ и $6^2 \equiv 2\ (17)$. С другой стороны, $p = 19$ и $p = 5$ сравнимы с 3 и 5 по модулю 8 соответственно и непосредственно проверяется, что 2 не будет квадратичным вычетом по модулю обоих этих чисел.

Предложение 5.1.3 можно использовать для доказательства того, что существует бесконечно много простых чисел вида $8k + 7$. Пусть $p_1, \ldots, p_m$ — некоторое конечное множество таких простых чисел, и рассмотрим $(4p_1p_2 \ldots p_m)^2 - 2$. Нечетные простые делители этого числа имеют вид $8k + 1$ или $8k + 7$, так как для таких простых делителей 2 будет квадратичным вычетом. Не все нечетные простые делители этого числа имеют вид $8k + 1$ (доказать это). Пусть p — какой-либо делитель вида $8k + 7$. Тогда p не содержится в множестве $\{p_1, p_2, \ldots, p_m\}$ и утверждение доказано.

§ 2. Квадратичный закон взаимности

Теорема 1 (квадратичный закон взаимности). *Пусть* p *и* q — *нечетные простые числа. Тогда*

(a) $(-1/p) = (-1)^{(p-1)/2}$.

(b) $(2/p) = (-1)^{(p^2-1)/8}$.

(c) $(p/q)(q/p) = (-1)^{((p-1)/2)((q-1)/2)}$.

Доказательство этой теоремы мы отложим до § 3. В гл. 6 мы докажем ее еще раз с другой точки зрения, а также остановимся на ее истории. Она принадлежит к самым глубоким и красивым результатам элементарной теории чисел и находится в начале того ряда теорем о законах взаимности, который достигает своей высшей точки в весьма общем законе взаимности Артина, пожалуй, наиболее впечатляющей теореме во всей теории чисел. Даже формулировка закона взаимности Артина увела бы нас далеко за рамки этой книги, однако в гл. 9 мы сформулируем и докажем кубичный и биквадратичный законы взаимности.

Пункты (a) и (b) теоремы 1 были уже доказаны и некоторые из их следствий обсуждены. Займемся п. (c).

Если хотя бы одно из чисел p и q имеет вид $4k + 1$, то $((p - 1)/2)((q - 1)/2) \equiv 0$ (2). Если оба числа p и q имеют вид $4k + 3$, то $((p - 1)/2)((q - 1)/2) \equiv 1$ (2). Это позволяет переформулировать п. (c) следующим образом:

(1) Если хотя бы одно из чисел p и q имеет вид $4k + 1$, то p является квадратичным вычетом по модулю q тогда и только тогда, когда q — квадратичный вычет по модулю p.

(2) Если оба числа p и q имеют вид $4k + 3$, то p является квадратичным вычетом по модулю q тогда и только тогда, когда q — квадратичный невычет по модулю p.

В качестве первого применения квадратичного закона взаимности мы покажем, как он, объединенный с предложением 5.1.2, может быть использован при вычислении символа Лежандра. Для иллюстрации этого метода будет достаточно одного примера.

Мы собираемся вычислить (79/101). Так как $101 \equiv 1$ (4), то $(79/101) = (101/79) = (22/79)$. Последнее равенство следует из сравнения $101 \equiv 22$ (79). Далее, $(22/79) = (2/79)(11/79)$. Но $79 \equiv 7$ (8). Поэтому $(2/79) = 1$. Так как оба числа 11 и 79 сравнимы с 3 по модулю 4, то $(11/79) = -(79/11) = -(2/11)$. Наконец, $11 \equiv 3$ (8) означает, что $(2/11) = -1$. Поэтому $(79/101) = 1$, т. е. 79 — квадратичный вычет по модулю 101. В самом деле, $33^2 \equiv 79$ (101).

Следующее приложение, пожалуй, более важное. Мы отметили ранее, что -1 есть квадратичный вычет по модулю простых чисел вида $4k + 1$ и что 2 есть квадратичный вычет по модулю простых чисел вида $8k + 1$ или $8k + 7$. Если a — произвольное целое число, то для каких p оно будет квадратичным вычетом по модулю p? Мы теперь в состоянии дать ответ на этот вопрос. Для начала мы рассмотрим случай, когда $a = q$, т. е. a — нечетное простое число.

Теорема 2. *Пусть q — нечетное простое число.*

(a) *Если* $q \equiv 1$ (4), *то оно является квадратичным вычетом по модулю* p *в том и только том случае, когда* $p \equiv r$ (q), *где* r — *квадратичный вычет по модулю* q.

(b) *Если* $q \equiv 3$ (4), *то оно является квадратичным вычетом по модулю* p *в том и только том случае, когда* $p \equiv \pm b^2$ $(4q)$, *где* b — *некоторое нечетное целое число, взаимно простое с* q.

Доказательство. Если $q \equiv 1$ (4), то по теореме 1 $(q/p) = (p/q)$. Пункт (a), таким образом, установлен.

Если $q \equiv 3$ (4), то теорема 1 дает $(q/p) = (-1)^{(p-1)/2}(p/q)$. Предположим сначала, что $p \equiv \pm b^2$ $(4q)$, где b нечетно. Если взять знак плюс, то $p \equiv b^2$ (4) $\equiv 1$ (4) и $p \equiv b^2$ (q). Таким образом, $(-1)^{(p-1)/2} = 1$ и $(p/q) = 1$, что дает $(q/p) = 1$. Если взять знак минус, то $p \equiv -b^2$ (4) $\equiv -1$ (4) $\equiv 3$ (4) и $p \equiv -b^2$ (q). Первое сравнение показывает, что $(-1)^{(p-1)/2} = -1$. Второе показывает, что $(p/q) \equiv (-b^2/q) = (-1/q)(b/q)^2 = (-1/q) = -1$, так как $q \equiv 3$ (4). Опять мы получаем $(q/p) = 1$.

Для доказательства обратного утверждения предположим, что $(q/p) = 1$. Следует рассмотреть две возможности:

(1) $(-1)^{(p-1)/2} = -1$ и $(p/q) = -1$.

(2) $(-1)^{(p-1)/2} = 1$ и $(p/q) = 1$.

Во втором случае $p \equiv b^2$ (q) и $p \equiv 1$ (4). Число b можно считать нечетным, ибо если это не так, то вместо него можно использовать $b' = b + q$. Если b нечетно, то $b^2 \equiv 1$ (4) и $p \equiv b^2$ (4), а потому $p \equiv b^2$ $(4q)$, как и требовалось.

В первом случае $p \equiv 3$ (4) и $p \equiv -b^2$ (q). Последнее сравнение вытекает из того, что при $q \equiv 3$ (4) любой невычет будет некоторым вычетом, взятым со знаком минус (доказать это). Опять можно считать, что b нечетно. В этом случае $-b^2 \equiv 3$ (4), так что $p \equiv -b^2$ (4) и $p \equiv -b^2$ $(4q)$. Это завершает доказательство. □

В качестве первой иллюстрации возьмем $q = 3$. Согласно п. (b) теоремы 2, мы должны найти вычеты по модулю 12 квадратов нечетных чисел, взаимно простых с 3. Числа 1^2, 5^2, 7^2 и 11^2 все сравнимы с 1. Таким образом, 3 будет квадратичным вычетом по модулю простых чисел, сравнимых с ± 1 (12), и невычетом по модулю простых чисел, сравнимых с ± 5 (12).

Следующим рассмотрим $q = 5$. Так как $5 \equiv 1$ (4), то мы находимся в более простой ч. (a) теоремы 2. Числа 1 и 4 — вычеты по модулю 5, а 2 и 3 — невычеты. Таким образом, 5 будет вычетом по модулю простых чисел, сравнимых с 1 или 4 по модулю 5, и невычетом по модулю простых чисел, сравнимых с 2 или 3 по модулю 5.

«Числа, сравнимые с b по модулю m» и «числа вида $mk + b$» — выражения для описания одного и того же множества $\{b, b \pm m, b \pm 2m, \ldots\}$. Это множество есть арифметическая прогрессия с на-

чальным членом b и разностью m. Пока в наших исследованиях мы видели, что ответ на вопрос о том, по модулю каких простых чисел p число a является квадратичным вычетом, сводился к тому, что такие простые числа p содержатся в некотором конечном наборе фиксированных арифметических прогрессий. Это самая общая ситуация. Вместо того чтобы формулировать этот результат в виде теоремы (формулировка была бы довольно сложной), мы приведем несколько числовых примеров.

Для $a = -3$ имеем $(-3/p) = (-1/p)(3/p)$. Таким образом, -3 будет квадратичным вычетом по модулю p либо при $(-1/p) = 1$ и $(3/p) = 1$, либо при $(-1/p) = -1$ и $(3/p) = -1$.

Согласно предыдущим результатам, первый случай получается, если $p \equiv 1$ (4) и $p \equiv \pm 1$ (12). Если $p \equiv -1$ (12), то $p \equiv -1$ (4). Простыми числами, удовлетворяющими обоим сравнениям, будут лишь те, которые сравнимы с 1 по модулю 12.

Во втором случае $p \equiv 3$ (4) и $p \equiv \pm 5$ (12). Если $p \equiv 5$ (12), то $p \equiv 1$ (4). Таким образом, простыми числами, удовлетворяющими обоим этим сравнениям, будут лишь те, которые сравнимы с -5 по модулю 12.

Объединяя предыдущее, получаем, что -3 есть квадратичный вычет по модулю p тогда и только тогда, когда p сравнимо с 1 или -5 по модулю 12.

Рассмотрим теперь $a = 6$. Так как $(6/p) = (2/p)(3/p)$, мы опять имеем две возможности: $(2/p) = 1$ и $(3/p) = 1$ или $(2/p) = -1$ и $(3/p) = -1$. Первый случай выполняется при $p \equiv 1, 7$ (8) и $p \equiv 1, 11$ (12). Единственными парами совместных сравнений будут

$$p \equiv 1 \ (8) \text{ и } p \equiv 1 \ (12);$$
$$p \equiv 7 \ (8) \text{ и } p \equiv 11 \ (12).$$

С помощью стандартной техники (см. гл. 3) получаем, что простые числа, удовлетворяющие этим сравнениям, сравнимы с 1 или 23 по модулю 24.

Во втором случае следует рассмотреть сравнения $p \equiv 3, 5$ (8) и $p \equiv 5, 7$ (12). Разделяя их на четыре пары сравнений, видим, что решениями будут лишь числа, сравнимые с 5 или 19 по модулю 24.

Подведем итог: 6 будет квадратичным вычетом по модулю p в том и только том случае, когда $p \equiv 1, 5, 19, 23$ (24).

Для простых чисел 73, 5, 19 и 23 приведем числовые контрольные примеры: $15^2 \equiv 6$ (73), $1^2 \equiv 6$ (5), $5^2 \equiv 6$ (19) и $11^2 \equiv 6$ (23).

В качестве последнего приложения квадратичного закона взаимности мы исследуем вопрос: если a есть квадратичный вычет по модулю всех простых чисел, не делящих a, то что можно сказать об a? Если a — квадрат, то оно будет квадратичным вычетом по модулю всех простых чисел, не делящих a. Оказывается, что

верно также и обращение последнего утверждения. Сначала, однако, необходимо определить и исследовать хотя бы кратко некоторый новый символ.

Определение. Пусть b — нечетное положительное целое число и a — произвольное целое число. Пусть $b = p_1 p_2 \ldots p_m$, где p_i суть (не обязательно различные) простые числа. Символ (a/b), определенный формулой

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\ldots\left(\frac{a}{p_m}\right),$$

называется *символом Якоби*.

Свойства символа Якоби очень близки к свойствам символа Лежандра, который он обобщает. Будет полезно, однако, сделать одно предупреждение. Символ (a/b) может быть равным 1 и тогда, когда a не является квадратичным вычетом по модулю b. Например, $(2/15) = (2/3)(2/5) = (-1)(-1) = 1$, то 2 не является квадратичным вычетом по модулю 15. Верно, однако, что если $(a/b) = -1$, то a не будет квадратичным вычетом по модулю b.

Предложение 5.2.1.
(a) $(a_1/b) = (a_2/b)$, *если* $a_1 \equiv a_2$ (b).
(b) $(a_1 a_2/b) = (a_1/b)(a_2/b)$.
(c) $(a/b_1 b_2) = (a/b_1)(a/b_2)$.

Доказательство. Пункты (a) и (b) непосредственно следуют из соответствующих свойств символа Лежандра. Пункт (c) очевиден по определению. □

Лемма. *Пусть r и s — нечетные целые числа. Тогда*
(a) $(rs - 1)/2 \equiv ((r-1)/2) + ((s-1)/2)$ (2).
(b) $(r^2 s^2 - 1)/8 \equiv ((r^2-1)/8) + ((s^2-1)/8)$ (2).

Доказательство. Так как $(r-1)(s-1) \equiv 0$ (4), то $rs - 1 \equiv (r-1) + (s-1)$ (4). Часть (a) получается отсюда с помощью деления на 2.

$r^2 - 1$ и $s^2 - 1$ оба делятся на 4. Поэтому $(r^2-1)(s^2-1) \equiv 0$ (16) и $r^2 s^2 - 1 \equiv (r^2-1) + (s^2-1)$ (16). Часть (b) получается отсюда при помощи деления на 8. □

Следствие. *Пусть $r_1, r_2, \ldots, r_m$ — нечетные целые числа. Тогда*

(a) $\sum_{i=1}^{m} (r_i - 1)/2 \equiv (r_1 r_2 \ldots r_m - 1)/2$ (2).

(b) $\sum_{i=1}^{m} (r_i^2 - 1)/8 \equiv (r_1^2 r_2^2 \ldots r_m^2 - 1)/8$ (2).

Доказательство. Доказательство проводится простой индукцией по m с применением предыдущей леммы. □

Предложение 5.2.2.
(a) $(-1/b) = (-1)^{(b-1)/2}$.
(b) $(2/b) = (-1)^{(b^2-1)/8}$.
(c) *Если оба числа a и b нечетные и положительные, то*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{((a-1)/2)((b-1)/2)}.$$

Доказательство. Имеем

$$(-1/b) = (-1/p_1)(-1/p_2)\ldots(-1/p_m) =$$
$$= (-1)^{(p_1-1)/2}\ldots(-1)^{(p_m-1)/2} = (-1)^{\sum (p_i-1)/2}.$$

Согла́сно лемме, $\sum (p_i - 1)/2 \equiv (p_1 p_2 \ldots p_m - 1)/2$ (2) $\equiv$ $\equiv (b-1)/2$ (2). Это доказывает п. (a).

Пункт (b) доказывается точно так же.

Далее, если $a = q_1 q_2 \ldots q_l$, то

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \prod_i \prod_j \left(\frac{q_i}{p_j}\right)\left(\frac{p_j}{q_i}\right) = (-1)^{\sum\limits_i \sum\limits_j ((q_i-1)/2)((p_j-1)/2)}.$$

Произведение и сумма берутся по индексам $1 \leqslant i \leqslant l$ и $1 \leqslant$ $\leqslant j \leqslant m$. Опять применяя лемму, получаем

$$\sum_i \sum_j \left(\frac{(p_j-1)}{2}\right)\left(\frac{(q_i-1)}{2}\right) \equiv \frac{(a-1)}{2} \sum_i \frac{(p_i-1)}{2} \equiv$$
$$\equiv \left(\frac{(a-1)}{2}\right)\left(\frac{(b-1)}{2}\right) (2).$$

Это доказывает п. (c). □

Символ Якоби имеет много приложений. Укажем хотя бы на то, что он является удобным средством для вычисления символа Лежандра. Мы используем его сейчас для доказательства следующей теоремы.

Теорема 3. *Пусть a — целое число, не являющееся квадратом. Тогда существует бесконечно много простых чисел p, по модулю которых a — квадратичный невычет.*

Доказательство. Как нетрудно убедиться, можно считать, что a свободно от квадратов. Пусть $a = 2^e q_1 q_2 \ldots q_n$, где q_i — различные нечетные простые числа и $e = 0$ или 1. Случай $a = 2$ следует рассмотреть отдельно. Поэтому вначале мы предположим, что $n \geqslant 1$, т. е. что a делится на какое-то нечетное простое число.

Пусть $\{l_1, l_2, \ldots, l_k\}$ — некоторое конечное множество нечетных простых чисел, не содержащее ни одного q_i. Пусть s — какой-нибудь невычет по модулю q_n. Найдем некоторое решение системы сравнений

$$x \equiv 1 \ (l_i), \ i = 1, \ldots, k,$$
$$x \equiv 1 \ (8),$$
$$x \equiv 1 \ (q_i), \ i = 1, 2, \ldots, n-1,$$
$$x \equiv s \ (q_n).$$

Обозначим это решение через b. Число b нечетно. Предположим, что $b = p_1 p_2 \ldots p_m$ — его разложение на простые множители. Так как $b \equiv 1 \ (8)$, то $(2/b) = 1$ и $(q_i/b) = (b/q_i)$ ввиду предложения 5.2.2. Таким образом,

$$\left(\frac{a}{b}\right) = \left(\frac{2}{b}\right)^e \left(\frac{q_1}{b}\right) \ldots \left(\frac{q_{n-1}}{b}\right) \left(\frac{q_n}{b}\right) =$$
$$= \left(\frac{b}{q_1}\right) \ldots \left(\frac{b}{q_{n-1}}\right) \left(\frac{b}{q_n}\right) = \left(\frac{1}{q_1}\right) \ldots \left(\frac{1}{q_{n-1}}\right) \left(\frac{1}{q_n}\right).$$

С другой стороны, по определению (a/b)

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2}\right) \ldots \left(\frac{a}{p_m}\right).$$

Отсюда следует, что $(a/p_i) = -1$ для некоторого i.

Заметим, что l_j не делят b. Таким образом, $p_i \notin \{l_1, l_2, \ldots, l_k\}$.

Подведем итог: если a — не квадрат и делится на некоторое нечетное простое число, то мы нашли простое число p, не лежащее в данном конечном множестве простых чисел $\{2, l_1, l_2, \ldots, l_k\}$, для которого $(a/p) = -1$. Это доказывает теорему 3 для данного случая.

Остается рассмотреть случай $a = 2$. Пусть $\{l_1, \ldots, l_k\}$ — некоторое конечное множество простых чисел, не содержащее 3, и $(2/l_i) = -1$. Положим $b = 8l_1 l_2 \ldots l_k + 3$. Число b не делится ни на 3, ни на какое-либо из l_i. Так как $b \equiv 3 \ (8)$, то $(2/b) = (-1)^{(b^2-1)/2} = -1$. Пусть $b = p_1 p_2 \ldots p_m$ — разложение на простые множители. Тогда, как и прежде, $(2/p_i) = -1$ для некоторого i. Число p_i не лежит в $\{3, l_1, l_2, \ldots, l_k\}$. Это доказывает теорему 3 для $a = 2$. □

§ 3. Доказательство квадратичного закона взаимности

Гаусс нашел восемь разных доказательств квадратичного закона взаимности. Теперь их имеется более ста. Конечно, не все они различаются по существу. Многие отличаются друг от друга лишь небольшими деталями. Мы приведем достаточно простое доказательство, принадлежащее Эйзенштейну. Более элементарное стандартное доказательство см. в [61].

Комплексное число ζ называется *корнем степени n из единицы*, если $\zeta^n = 1$ для некоторого целого числа $n > 0$. Если n — наименьшее целое число с этим свойством, то ζ называется *примитивным* (или *первообразным*) корнем степени n из единицы.

Корни степени n из единицы суть 1, $e^{2\pi i/n}$, $e^{(2\pi i/n)\,2}$, ..., $e^{(2\pi i/n)\,(n-1)}$. Среди них примитивными корнями степени n из единицы будут $e^{(2\pi i/n)\,k}$, где $(k, n) = 1$.

Если ζ — корень степени n из единицы и $m \equiv l\ (n)$, то $\zeta^m = \zeta^l$. *Если ζ — примитивный корень степени n из единицы и $\zeta^m = \zeta^l$, то $m \equiv l\ (n)$.*

Доказать эти элементарные свойства нетрудно.

Рассмотрим функцию $f(z) = e^{2\pi iz} - e^{-2\pi iz} = 2i \sin 2\pi z$. Она удовлетворяет тождествам $f(z+1) = f(z)$ и $f(-z) = -f(z)$. Кроме того, ее единственными вещественными нулями являются все полуцелые числа. Другими словами, если r — некоторое вещественное число и $2r \notin \mathbf{Z}$, то $f(r) \neq 0$.

Мы хотим доказать для $f(z)$ важное тождество, но сначала нам понадобится одна алгебраическая лемма.

Лемма. *Если $n > 0$ нечетно, то*

$$x^n - y^n = \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y), \text{ где } \zeta = e^{2\pi i/n}.$$

Доказательство. $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ — все корни многочлена $z^n - 1$. Так как их n и все они различны, то

$$z^n - 1 = \prod_{k=0}^{n-1} (z - \zeta^k).$$

Положив $z = x/y$ и умножив обе части равенства на y^n, получим

$$x^n - y^n = \prod_{k=0}^{n-1} (x - \zeta^k y).$$

Так как n нечетно, то вместе с k полную систему вычетов по модулю n будет пробегать и $-2k$. Таким образом,

$$\begin{aligned} x^n - y^n &= \prod_{k=0}^{n-1} (x - \zeta^{-2k} y) = \\ &= \zeta^{-(1+2+\ldots+n-1)} \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y) = \\ &= \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y). \end{aligned}$$

При последнем шаге мы использовали тот факт, что $1 + 2 + 3 + \cdots + (n-1) = n((n-1)/2)$ делится на n. □

Предложение 5.3.1. *Если n — положительное нечетное целое число и $f(z) = e^{2\pi iz} - e^{-2\pi iz}$, то*

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) f\left(z - \frac{k}{n}\right).$$

Доказательство. В лемме произведем подстановку $x = e^{2\pi iz}$ и $y = e^{-2\pi iz}$. В результате получим

$$f(nz) = \prod_{k=0}^{n-1} f\left(z + \frac{k}{n}\right).$$

Заметим, что $f(z + k/n) = f(z + k/n - 1) = f(z - (n - k)/n)$. Если k пробегает значения от $(n + 1)/2$ до $n-1$, то $n - k$ пробегает значения от $(n - 1)/2$ до 1. Таким образом,

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) \prod_{k=(n+1)/2}^{n-1} f\left(z + \frac{k}{n}\right) =$$

$$= \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) \prod_{k=(n+1)/2}^{n-1} f\left(z - \frac{n-k}{n}\right) =$$

$$= \prod_{k=1}^{(n-1)/2} f\left(z + \frac{k}{n}\right) f\left(z - \frac{k}{n}\right). \qquad \square$$

Предложение 5.3.2. *Если p — некоторое нечетное простое число, $a \in \mathbf{Z}$ и $p \nmid a$, то*

$$\prod_{l=1}^{(p-1)/2} f\left(\frac{la}{p}\right) = \left(\frac{a}{p}\right) \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right).$$

Доказательство. Как в лемме из § 1, $la \equiv \pm m_l \ (p)$, где $1 \leqslant m_l \leqslant (p-1)/2$. Таким образом, la/p и $\pm m_l/p$ отличаются на целое число. Это означает, что

$$f(la/p) = f(\pm m_l/p) = \pm f(m_l/p).$$

Результат получается теперь, если взять произведение обеих частей при l, меняющемся от 1 до $(p-1)/2$, и применить лемму Гаусса. $\square$

Мы в состоянии теперь доказать квадратичный закон взаимности. Пусть p и q — нечетные простые числа. Тогда, согласно предложению 5.3.2,

$$\prod_{l=1}^{(p-1)/2} f\left(\frac{lq}{p}\right) = \left(\frac{q}{p}\right) \prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}\right).$$

Согласно предложению 5.3.1,

$$\frac{f(ql/p)}{f(l/p)} = \prod_{m=1}^{(q-1)/2} f\left(\frac{l}{p}+\frac{m}{q}\right) f\left(\frac{l}{p}-\frac{m}{q}\right).$$

Объединяя эти два равенства, получаем

$$\left(\frac{q}{p}\right) = \prod_{m=1}^{(q-1)/2}\prod_{l=1}^{(p-1)/2} f\left(\frac{l}{p}+\frac{m}{q}\right) f\left(\frac{l}{p}-\frac{m}{q}\right).$$

Тем же способом находим, что

$$\left(\frac{p}{q}\right) = \prod_{m=1}^{(q-1)/2}\prod_{l=1}^{(p-1)/2} f\left(\frac{m}{q}+\frac{l}{p}\right) f\left(\frac{m}{q}-\frac{l}{p}\right).$$

Так как $f(m/q - l/p) = -f(l/p - m/q)$, мы видим, что

$$(-1)^{((p-1)/2)((q-1)/2)}\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right),$$

а потому

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{((p-1)/2)((q-1)/2)}.$$

Доказательство завершено. □

Мы закончим эту главу эквивалентной формулировкой квадратичного закона взаимности.

Предложение 5.3.3. *Пусть p и q — различные нечетные простые числа и $a \geqslant 1$ — некоторое целое число. Тогда следующие утверждения эквивалентны:*

(a) $(p/q)(q/p) = (-1)^{((p-1)/2)((q-1)/2)}$.

(b) *Если* $p \equiv \pm q \ (4a)$, $p \nmid a$, *то* $(a/p) = (a/q)$.

Доказательство. Чтобы показать, что из (a) следует (b), достаточно в силу мультипликативности показать, что (b) выполняется в случае, когда a — простое число. Для $a = 2$ результат следует из предложения 5.1.3. Если a — нечетное простое число, то по п. (a)

$$(a/p) = (-1)^{((p-1)/2)((a-1)/2)}(p/a).$$

Если $p \equiv q \ (4a)$, то $(p/a) = (q/a)$, так что

$$\left(\frac{a}{p}\right) = (-1)^{((p-1)/2)((a-1)/2)}\left(\frac{q}{a}\right) =$$

$$= (-1)^{((p-1)/2)((a-1)/2)}(-1)^{((q-1)/2)((a-1)/2)}\left(\frac{a}{q}\right) =$$

$$= (-1)^{((a-1)/2)((p+q-2)/2)}\left(\frac{a}{q}\right).$$

Но $p \equiv q$ $(4a)$ означает, что $p + q - 2 \equiv 0$ (4), откуда и следует доказываемый результат. Если, с другой стороны, $p \equiv -q$ $(4a)$, то подобное рассуждение показывает, что

$$\left(\frac{a}{p}\right) = (-1)^{((a-1)/2)\,((p+q)/2)} \left(\frac{a}{q}\right).$$

Так как $p + q \equiv 0$ (4), результат получается и в этом случае.

Чтобы показать, что из (b) следует (a), предположим сначала, что $p \equiv q$ и $p \equiv q$ (4). Тогда $p = q + 4a$, $a \geqslant 1$. Таким образом,

$$\left(\frac{p}{q}\right) \left(\frac{q+4a}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right) =$$

$$= \left(\frac{p-q}{p}\right) = \left(\frac{-q}{p}\right) = (-1)^{(p-1)/2} \left(\frac{q}{p}\right).$$

Если $p \equiv 1$ (4), то $(p/q) = (q/p)$, что дает (a). Если $p \equiv 3$ (4), то $q \equiv 3$ (4) и $(p/q) = -(q/p)$, что совпадает в этом случае с (a). Наконец, если $p \equiv -q$ (4), то $p + q = 4a$ и

$$\left(\frac{p}{q}\right) = \left(\frac{-q+4a}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{p+q}{p}\right) = \left(\frac{q}{p}\right).$$

Таким образом, $(p/q) = (q/p)$, что совпадает с утверждением п. (a), так как в этом случае хотя бы одно из чисел p или q сравнимо с 1 по модулю 4. Доказательство завершено. □

Заметим, что в силу п. (b) только что доказанного предложения, если $(r, 4a) = 1$, то квадратичный характер[1]) для *всех* простых чисел в арифметической прогрессии $r + 4at$, $t \in \mathbf{Z}$, один и тот же. В гл. 16 мы убедимся в том, что существует бесконечно много таких простых чисел. Заметим также, что квадратичный характер для любого простого числа вида $r + 4at$ принимает то же значение, что и для любого простого числа вида $-r + 4at$. Этот замечательный закон был впервые открыт Эйлером именно в таком виде.

Замечания

Как заметил Кронекер, квадратичный закон взаимности непосредственно следует из одной гипотезы Эйлера, которая содержится в статье «Theoremata circa divisores numerorum in hac forma $pa^2 + qb^2$ contentorum» (1744—1746). Явно он появляется в более поздней статье Эйлера, озаглавленной «Observationes circa divisionem quadratorum per numeros primos». Воспользо-

[1]) Квадратичным характером (числа a) здесь и далее называется символ Лежандра (a/p) как *функция* числа a. Смысл этого названия проясняется в гл. 8, § 1. — *Прим. ред.*

вавшись достаточными условиями разрешимости уравнения $ax^2 + by^2 + cz^2 = 0$ (см. предложение 17.3.2), Лежандр (в 1785 г.) смог доказать этот результат в частных случаях. Например, рассмотрение уравнения $x^2 + py^2 = qz^2$, где $p \equiv 1$ (4) и $q \equiv 3$ (4), приводит к заключению о том, что если q — квадрат по модулю p, то p — квадрат по модулю q. Первое полное доказательство квадратичного закона взаимности принадлежит Гауссу, который сообщает дату доказательства в своем дневнике от 8 апреля 1796 г. При жизни Гаусс опубликовал шесть доказательств этого замечательного закона [1]). Доказательство в этой главе взято из статьи Эйзенштейна «Applications de l'Algèbre à l'Arithmétique transcendante». Куммер в историческом очерке о законах взаимности ссылается на это доказательство как на одно из самых красивых («... einen der schönsten Beweise dieses von den ausgezeichnetsten Mathematikern viel bewiesenen Theorems. . .»).

Заменяя тригонометрическую функцию некоторыми эллиптическими функциями, Эйзенштейн смог без особенных дополнительных трудностей доказать кубический и биквадратичный законы взаимности.

В XIX в. различные математики, включая Коши, Эйзенштейна, Дирихле, Дедекинда и Кронекера, давали новые доказательства квадратичного закона взаимности. Согласно Бахману, к 1921 г. существовало 56 известных доказательств. Новые доказательства продолжают появляться даже в последнее время. См., например, статьи [128] и [75]. С другой стороны, первое доказательство Гаусса было недавно пересмотрено Брауном [99].

Символ Якоби — одно из обобщений символа Лежандра. Интересное обобщение в другом направлении см. в статье [14].

Квадратичный закон взаимности можно сформулировать не только в кольце $\mathbf{Z}$. Для кольца гауссовых целых чисел $\mathbf{Z}[i]$ такая теорема была доказана Дирихле. Гильберт смог доказать, что квадратичный закон взаимности выполняется в любом поле алгебраических чисел, и это явилось важным шагом по направлению к теории полей классов. С другой стороны, можно показать, что закон взаимности выполняется в кольце $k[x]$, где k — конечное поле. См. [2] и [10]. Этот результат был сформулирован (хотя и не доказан) уже Дедекиндом в 1857 г.

Обобщение теоремы 3 на более высокие степени было открыто впервые Тростом в 1934 г. [2]). Позднее его сформулировал в ка-

---

[1]) Предложенные Гауссом доказательства квадратичного закона взаимности см., помимо [34], в [10*] и [12*]. Неожиданная интерпретация первого доказательства Гаусса (которое ранее считалось не слишком интересным) была дана Дж. Тейтом [17*, стр. 107—117]. Еще два доказательства см. в гл. 7, § 3, и гл. 8, § 6. — *Прим. ред.*

[2]) Trost E. Zur Theorie der Potenzreste. — Nieuw Arch. Wiskunde, 1934, v. 18, p. 15—61.

честве гипотезы Чоула, а затем доказали Анкени и Роджерс [1]). Они доказали, что если $x^n \equiv a\ (p)$ имеет решение для почти всех простых чисел, то либо $a = b^n$, либо $n \mid 8$ и $a = 2^{n/8}b^n$. Если n свободно от квадратов и $(a, n) = 1$, то этот результат, как можно показать, следует из закона взаимности Эйзенштейна; это было сделано в [211] (доказательство будет приведено в гл. 14). См. также [134], где этот результат обобщается на поля алгебраических чисел и поля алгебраических функций от одной переменной над конечным полем.

Упражнения

1. Воспользоваться леммой Гаусса для нахождения (5/7), (3/11), (6/13) и $(-1/p)$.

2. Показать, что число решений сравнения $x^2 \equiv a\ (p)$ равно $1 + (a/p)$.

3. Предположим, что $p \nmid a$. Показать, что число решений сравнения $ax^2 + bx + c \equiv 0\ (p)$ равно $1 + ((b^2 - 4ac)/p)$.

4. Доказать, что $\sum_{a=1}^{p-1} (a/p) = 0$.

5. Доказать, что $\sum_{x=1}^{p-1} ((ax + b)/p) = 0$, если $p \nmid a$.

6. Показать, что число решений сравнения $x^2 - y^2 \equiv a\ (p)$ равно $\sum_{y=0}^{p-1} (1 + ((y^2 + a)/p))$.

7. Прямым вычислением показать, что число решений сравнения $x^2 - y^2 \equiv a\ (p)$ равно $p - 1$ при $p \nmid a$ и $2p - 1$ при $p \mid a$. [*Указание.* Воспользоваться заменой переменных $u = x + y$, $v = x - y$.]

8. Объединяя результаты упр. 6 и 7, показать, что

$$\sum_{y=0}^{p-1} \left(\frac{y^2 + a}{p}\right) = \begin{cases} -1 & \text{при } p \nmid a, \\ p - 1 & \text{при } p \mid a. \end{cases}$$

9. Используя теорему Вильсона, показать, что $1^2 3^2 5^2 \ldots (p-2)^2 \equiv (-1)^{(p+1)/2}\ (p)$.

10. Пусть $r_1, r_2, \ldots, r_{(p-1)/2}$ — квадратичные вычеты между 1 и p. Показать, что их произведение сравнимо с 1 по модулю p при $p \equiv 3\ (4)$ и с -1 при $p \equiv 1\ (4)$.

11. Предположим, что $p \equiv 3\ (4)$ и что $q = 2p + 1$ — тоже простое число. Доказать, что $2^p - 1$ — не простое число. [*Указание.* Воспользоваться квадратичным характером числа 2, чтобы показать, что $q \mid 2^p - 1$.] Следует предположить, что $p > 3$.

12. Пусть $f(x) \in \mathbf{Z}[x]$. Мы говорим, что простое число p делит $f(x)$, если существует целое число n, для которого $p \mid f(n)$. Описать простые делители многочленов $x^2 + 1$ и $x^2 - 2$.

13. Показать, что любой простой делитель многочлена $x^4 - x^2 + 1$ сравним с 1 по модулю 12.

---

[1]) Ankeny N. C., Rogers C. A. A conjecture of Chowla. — Ann. Math., 1951, v. 53, № 3, p. 541 — 550.

14. Использовать тот факт, что группа $U(\mathbf{Z}/p\mathbf{Z})$ циклическая, для получения прямого доказательства равенства $(-3/p) = 1$ при $p \equiv 1$ (3). [*Указание.* В $U(\mathbf{Z}/p\mathbf{Z})$ существует элемент ρ порядка 3. Показать, что $(2\rho + 1)^2 = -3$.]

15. При $p \equiv 1$ (5) показать непосредственно по методу упр. 14, что $(5/p) = 1$. [*Указание.* Пусть ρ — элемент группы $U(\mathbf{Z}/p\mathbf{Z})$ порядка 5. Показать, что $(\rho + \rho^4)^2 + (\rho + \rho^4) - \bar{1} = \bar{0}$ и т. д.]

16. Используя квадратичный закон взаимности, найти простые числа, для которых 7 будет квадратичным вычетом. То же самое проделать для 15.

17. Восстановить детали доказательства предложения 5.2.1 и следствия идущей за ним леммы.

18. Пусть D — свободное от квадратов нечетное и положительное целое число. Показать, что существует целое число b, взаимно простое с D, для которого $(b/D) = -1$.

19. Пусть D такое же, как в упр. 18. Показать, что $\sum (a/D) = 0$, где сумма берется по приведенной системе вычетов по модулю D (см. упр. 6 гл. 3). Получить отсюда, что ровно половина элементов в $U(\mathbf{Z}/D\mathbf{Z})$ удовлетворяет условию $(a/D) = 1$.

20 (продолжение). Пусть $a_1, a_2, \ldots, a_{\varphi(D)/2}$ — целые числа между 1 и D, для которых $(a_i, D) = 1$ и $(a_i/D) = 1$. Доказать, что D будет квадратичным вычетом по модулю некоторого простого p, такого, что $p \nmid D$, $p \equiv 1$ (4), в том и только том случае, когда $p \equiv a_i$ (D) для некоторого i.

21. Применить метод упр. 19 и 20 для нахождения простых чисел, для которых 21 будет квадратичным вычетом. [*Ответ.* Это числа $p \equiv 1, 4, 5, 16, 17$ и 20 (21).]

22. Воспользоваться символом Якоби для нахождения (113/997), (215/761), (514/1093) и (401/757).

23. Предположим, что $p \equiv 1$ (4). Показать, что существуют такие целые числа s и t, что $pt = 1 + s^2$. Вывести отсюда, что p — не простой элемент в $\mathbf{Z}[i]$. Напомним, что в $\mathbf{Z}[i]$ имеет место однозначное разложение на простые множители.

24. Показать, что если $p \equiv 1$ (4), то p будет суммой двух квадратов, т. е. $p = a^2 + b^2$, где $a, b \in \mathbf{Z}$. [*Указание.* $p = \alpha\beta$, где α, β — не единицы в $\mathbf{Z}[i]$. Взять абсолютное значение от обеих частей и возвести в квадрат.] Этот важный результат был открыт Ферма.

25. Целое число называется *биквадратичным вычетом* по модулю p, если оно сравнимо с четвертой степенью. Воспользовавшись тождеством $x^4 + 4 = ((x + 1)^2 + 1)((x - 1)^2 + 1)$, показать, что -4 будет биквадратичным вычетом по модулю p тогда и только тогда, когда $p \equiv 1$ (4).

26. Это упражнение и упр. 27 и 28 содержат красивое доказательство Дирихле того, что 2 будет биквадратичным вычетом по модулю p тогда и только тогда, когда p может быть записано в виде $A^2 + 64B^2$, где $A, B \in \mathbf{Z}$. Предположим, что $p \equiv 1$ (4). Тогда $p = a^2 + b^2$, согласно упр. 24. Будем считать a нечетным. Доказать следующие утверждения:

(a) $(a/p) = 1$.

(b) $((a + b)/p) = (-1)^{((a+b)^2-1)/8}$.

(c) $(a + b)^2 \equiv 2ab$ (p).

(d) $(a + b)^{(p-1)/2} \equiv (2ab)^{(p-1)/4}$ (p).

[*Указание.* $2p = (a + b)^2 + (a - b)^2$.]

27. Предположим, что f таково, что $b \equiv af$ (p). Показать, что $f^2 \equiv -1$ (p) и что $2^{(p-1)/4} \equiv f^{ab/2}$ (p).

28. Показать, что сравнение $x^4 \equiv 2$ (p) обладает решением тогда и только тогда, когда p имеет вид $A^2 + 64B^2$.

29. Пусть (RR) — число таких пар $(n, n + 1)$ в множестве 1, 2, 3, ..., $p - 1$, что n и $n + 1$ — оба квадратичные вычеты по модулю p. Пусть (NR) — число таких пар $(n, n + 1)$ в множестве 1, 2, 3, ..., $p - 1$, что n — квадратичный невычет и $n + 1$ — квадратичный вычет. Подобно этому определяются

(RN) и (NN). Найти суммы $(RR)+(RN)$, $(NR)+(NN)$, $(RR)+(NR)$ и $(RN)+(NN)$.

30. Показать, что $(RR)+(NN)-(RN)-(NR)=\sum_{n=1}^{p-1}(n(n+1)/p)$. Показать, что эта сумма равна -1. [*Указание.* Полезен результат упр. 8.]

31. Воспользовавшись результатами упр. 29 и 30, показать, что $(RR)=(1/4)(p-4-\varepsilon)$, где $\varepsilon=(-1)^{(p-1)/2}$.

32. Для нечетного простого числа p показать, что $(2/p)=\prod_{j=1}^{(p-1)/2}2\cos(2\pi j/p)$. Воспользоваться этим результатом для другого доказательства предложения 5.1.3.

33. Воспользоваться предложением 5.3.2 для получения квадратичного характера числа -1.

34. Для нечетного простого числа $p\neq 3$ показать, что $(3/p)=\prod_{j=1}^{(p-1)/2}(3-4\sin^2(2\pi j/p))$.

35. Используя предыдущее упражнение, показать, что 3 будет квадратом по модулю p тогда и только тогда, когда p сравнимо с 1 или -1 по модулю 12.

36. Показать, что ч. (c) предложения 5.2.2 имеет место в случае, когда a отрицательно и b положительно (оба они все еще нечетны).

37. Показать, что если a отрицательно, то из $p\equiv q\ (4a)$, $p\nmid a$, следует, что $(a/p)=(a/q)$.

38. Пусть p — некоторое нечетное число. Получить значение квадратичного характера числа 2 по модулю p, проверяя следующие шаги, содержащие символы Якоби:

$$\left(\frac{2}{p}\right)=\left(\frac{8-p}{p}\right)=\left(\frac{p}{p-8}\right)=\left(\frac{2}{p-8}\right).$$

Обобщить это рассуждение и показать, что

$$\left(\frac{a}{p}\right)=\left(\frac{a}{p-4a}\right),\qquad a>0,\qquad p\nmid a.$$

Глава 6

КВАДРАТИЧНЫЕ СУММЫ ГАУССА

Изящный метод, примененный при доказательстве квадратичного закона взаимности в гл. 5, нелегко использовать в более общих ситуациях. В этой главе мы дадим новое доказательство, основанное на методе, который может быть использован для доказательства высших законов взаимности. В частности, мы введем понятие гауссовых сумм, которое будет играть важную роль в оставшейся части этой книги.

В § 1 вводятся алгебраические числа и целые алгебраические числа. Все доказательства носят технический характер. При первом чтении читатель может лишь бегло просмотреть этот параграф.

§ 1. Алгебраические числа и целые алгебраические числа

Определение. *Алгебраическим числом* называется комплексное число α, являющееся корнем некоторого многочлена $a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$, где $a_0, a_1, a_2, \ldots, a_n \in \mathbf{Q}$ и $a_0 \neq 0$.

Целым алгебраическим числом называется комплексное число ω, являющееся корнем некоторого многочлена $x^n + b_1x^{n-1} + \cdots + b_n$, где $b_1, b_2, \ldots, b_n \in \mathbf{Z}$.

Очевидно, что всякое целое алгебраическое число будет алгебраическим числом. Обратное утверждение, как мы увидим, неверно.

Предложение 6.1.1. *Рациональное число $r \in \mathbf{Q}$ будет целым алгебраическим числом тогда и только тогда, когда $r \in \mathbf{Z}$.*

Доказательство. Если $r \in \mathbf{Z}$, то r будет корнем уравнения $x - r = 0$. Таким образом, r — целое алгебраическое число.

Предположим, что $r \in \mathbf{Q}$ есть целое алгебраическое число, т. е. r удовлетворяет уравнению $x^n + b_1x^{n-1} + \cdots + b_n = 0$ с $b_1, \ldots, b_n \in \mathbf{Z}$. Тогда $r = c/d$, где $c, d \in \mathbf{Z}$, и можно считать, что c и d взаимно просты. Подставляя c/d в выписанное уравнение и умножая обе части полученного равенства на d^n, получаем

$$c^n + b_1c^{n-1}d + \ldots + b_nd^n = 0.$$

Значит, d делит c^n, а так как $(d, c) = 1$, то $d \mid c$. Снова воспользовавшись тем, что $(d, c) = 1$, получаем, что $d = \pm 1$, а потому $r = c/d \in \mathbf{Z}$. □

Отсюда следует, например, что 2/5 не является целым алгебраическим числом.

Основные результаты этого параграфа состоят в том, что множество алгебраических чисел образует поле, а множество целых алгебраических чисел — кольцо. Нам понадобятся некоторые вспомогательные результаты.

Определение. Подмножество $V \subset \mathbf{C}$ комплексных чисел называется $\mathbf{Q}$-*модулем*, если

(a) из того, что $\gamma_1\gamma_2 \in V$, следует, что $\gamma_1 \pm \gamma_2 \in V$;

(b) из того, что $\gamma \in V$ и $r \in \mathbf{Q}$, следует, что $r\gamma \in V$;

(c) существуют такие элементы $\gamma_1, \gamma_2, \ldots, \gamma_l \in V$, что каждый элемент $\gamma \in V$ представляется в виде $\sum_{i=1}^{l} r_i\gamma_i$, где $r_i \in \mathbf{Q}$.

Короче говоря, подмножество $V \subset \mathbf{C}$ есть $\mathbf{Q}$-модуль, если оно является конечномерным векторным пространством над $\mathbf{Q}$.

Если $\gamma_1, \gamma_2, \ldots, \gamma_l \in \mathbf{C}$, то множество всех выражений $\sum_{i=1}^{l} r_i\gamma_i$, $r_1, r_2, \ldots, r_l \in \mathbf{Q}$, как нетрудно убедиться, образует $\mathbf{Q}$-модуль. Мы обозначаем этот $\mathbf{Q}$-модуль через $[\gamma_1, \gamma_2, \ldots, \gamma_l]$.

Предложение 6.1.2. *Пусть* $V = [\gamma_1, \gamma_2, \ldots, \gamma_l]$, *и предположим, что* $\alpha \in \mathbf{C}$ *обладает тем свойством, что* $\alpha\gamma \in V$ *для всех* $\gamma \in V$. *Тогда* α *будет алгебраическим числом.*

Доказательство. Имеем $\alpha\gamma_i \in V$ для $i = 1, 2, \ldots, l$. Таким образом, $\alpha\gamma_i = \sum_{j=1}^{l} a_{ij}\gamma_j$, где $a_{ij} \in \mathbf{Q}$. Отсюда следует, что $0 = \sum_{j=1}^{l} (a_{ij} - \delta_{ij}\alpha)\gamma_j$, где $\delta_{ij} = 0$ при $i \neq j$ и $\delta_{ij} = 1$ при $i = j$. Из стандартных результатов линейной алгебры мы знаем, что $\det(a_{ij} - \delta_{ij}\alpha) = 0$. Выписывая определитель, мы видим, что α является корнем многочлена степени l с рациональными коэффициентами. Таким образом, α — алгебраическое число. □

Предложение 6.1.3. *Множество алгебраических чисел образует поле.*

Доказательство. Предположим, что α_1 и α_2 — алгебраические числа. Мы покажем, что $\alpha_1\alpha_2$ и $\alpha_1 + \alpha_2$ суть алгебраические числа.

Предположим, что $\alpha_1^n + r_1\alpha_1^{n-1} + r_2\alpha_1^{n-2} + \cdots + r_n = 0$ и $\alpha_2^m + s_1\alpha_2^{m-1} + s_2\alpha_2^{m-2} + \cdots + s_m = 0$, где r_i, $s_j \in \mathbf{Q}$. Пусть V будет $\mathbf{Q}$-модулем, состоящим из всех $\mathbf{Q}$-линейных комбинаций элементов $\alpha_1^i\alpha_2^j$, где $0 \leqslant i < n$ и $0 \leqslant j < m$. Для $\gamma \in V$ имеют место включения $\alpha_1\gamma \in V$ и $\alpha_2\gamma \in V$ (докажите это). Значит, кроме того, $(\alpha_1 + \alpha_2)\gamma \in V$ и $(\alpha_1\alpha_2)\gamma \in V$. В силу предложения 6.1.2 отсюда следует, что $\alpha_1 + \alpha_2$ и $\alpha_1\alpha_2$ суть алгебраические числа.

Наконец, если α — алгебраическое число, отличное от нуля, то мы должны показать, что α^{-1} — алгебраическое число. Предположим, что $a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$, где $a_i \in \mathbf{Q}$. В таком случае $a_n\alpha^{-n} + a_{n-1}\alpha^{-(n-1)} + \cdots + a_0 = 0$, откуда и следует доказываемый результат. □

Чтобы установить, что множество целых алгебраических чисел образует кольцо, следует лишь слегка изменить приведенное выше доказательство.

Определение. Подмножество $W \subset \mathbf{C}$ называется **Z-*модулем***, если

(a) из того, что γ_1, $\gamma_2 \in W$, следует, что $\gamma_1 \pm \gamma_2 \in W$;

(b) существуют такие элементы γ_1, γ_2, ..., γ_l, что каждый элемент $\gamma \in W$ имеет вид $\sum_{i=1}^{l} b_i\gamma_i$, где $b_i \in \mathbf{Z}$.

Предложение 6.1.4. *Пусть W — некоторый $\mathbf{Z}$-модуль, и предположим, что элемент $\omega \in \mathbf{C}$ таков, что $\omega\gamma \in W$ для всех $\gamma \in W$. Тогда ω будет целым алгебраическим числом.*

Доказательство. Доказательство проводится точно так же, как и доказательство предложения 6.1.2, только теперь $a_{ij} \in \mathbf{Z}$. Равенство $\det(a_{ij} - \delta_{ij}\omega) = 0$ показывает, что ω удовлетворяет приведенному уравнению степени l с целыми коэффициентами. Таким образом, ω — целое алгебраическое число. □

Предложение 6.1.5. *Множество целых алгебраических чисел образует кольцо.*

Доказательство. Оно получается из предложения 6.1.4 точно таким же способом, каким предложение 6.1.3 получается из предложения 6.1.2. Восстановить детали мы предоставляем читателю.

Пусть Ω обозначает кольцо целых алгебраических чисел. Если ω_1, ω_2, $\gamma \in \Omega$, то мы говорим, что $\omega_1 \equiv \omega_2$ (γ) (ω_1 *сравнимо с* ω_2 *по модулю* γ), если $\omega_1 - \omega_2 = \gamma\alpha$, где $\alpha \in \Omega$. Это понятие сравнимости удовлетворяет всем формальным свойствам сравнимости в $\mathbf{Z}$.

Если a, b, $c \in \mathbf{Z}$, $c \neq 0$, то сравнение $a \equiv b$ (c) имеет теперь два смысла, ибо оно обозначает сравнение как в $\mathbf{Z}$, так и в Ω. Однако эта двусмысленность лишь кажущаяся. Если $a - b = c\alpha$, где $\alpha \in \Omega$, то α будет одновременно рациональным числом и целым алгебраическим числом. Таким образом, в силу предложения 6.1.1 α — обычное целое число.

Нам понадобится следующее предложение.

Предложение 6.1.6. *Если* ω_1, $\omega_2 \in \Omega$ *и* $p \in \mathbf{Z}$ — *простое число, то*

$$(\omega_1 + \omega_2)^p \equiv \omega_1^p + \omega_2^p \ (p).$$

Доказательство. Имеем

$$(\omega_1 + \omega_2)^p = \sum_{k=0}^{p} \binom{p}{k} \omega_1^k \omega_2^{p-k}.$$

В силу леммы 2 из гл. 4 $p \Big| \binom{p}{k}$ для $1 \leqslant k \leqslant p-1$. Наш результат получается отсюда и из того факта, что Ω — кольцо. □

Корень из единицы есть решение уравнения вида $x^n - 1 = 0$. Таким образом, корни из единицы — целые алгебраические числа, а потому целыми алгебраическими числами будут и $\mathbf{Z}$-линейные комбинации корней из единицы.

В заключение этого параграфа мы приводим несколько важных свойств алгебраических чисел. Если α — некоторое алгебраическое число, то очевидно, что любой ненулевой многочлен $f(x) \in \mathbf{Q}[x]$ наименьшей степени, для которого $f(\alpha) = 0$, должен быть неприводимым.

Предложение 6.1.7. *Если* α — *алгебраическое число, то оно является корнем единственного приведенного неприводимого многочлена* $f(x) \in \mathbf{Q}[x]$. *Кроме того, если* $g(x) \in \mathbf{Q}[x]$, $g(\alpha) = 0$, *то* $f(x) \mid g(x)$.

Доказательство. Пусть $f(x)$ — какой-нибудь приведенный неприводимый многочлен, такой, что $f(\alpha) = 0$. Докажем сначала второе утверждение. Если $f(x) \nmid g(x)$, то $(f(x), g(x)) = 1$. В силу леммы 4 из § 2 гл. 2 можно записать $f(x)h(x) + g(x)t(x) = 1$, где $h(x)$, $t(x) \in \mathbf{Q}[x]$. Подстановка $x = \alpha$ приводит к противоречию. Единственность следует отсюда непосредственно. □

Многочлен, определенный в предложении 6.1.7, зависит поэтому лишь от α. Он называется *минимальным многочленом* числа α. Если степень минимального многочлена числа α равна n, то α

называется алгебраическим числом *степени* n. Если $f(x)$ — неприводимый многочлен степени n, то, используя основную теорему алгебры и упр. 16, мы получаем, что $f(x)$ — минимальный многочлен для каждого из своих n корней. Если α, β суть корни многочлена $f(x)$, то α и β называются *сопряженными*.

Множество комплексных чисел $g(\alpha)/h(\alpha)$, где $g(x)$, $h(x) \in \mathbf{Q}[x]$, $h(\alpha) \neq 0$, образует поле, обозначаемое через $\mathbf{Q}(\alpha)$. Обозначим через $\mathbf{Q}[\alpha]$ кольцо многочленов от α с рациональными коэффициентами. Тогда имеет место следующий важный результат.

Предложение 6.1.8. *Если* $\alpha \in \Omega$, *то* $\mathbf{Q}(\alpha) = \mathbf{Q}[\alpha]$.

Доказательство. Очевидно, что $\mathbf{Q}[\alpha] \subset \mathbf{Q}(\alpha)$. Если $h(\alpha) \in \mathbf{Q}[\alpha]$, $h(\alpha) \neq 0$, то, согласно предложению 6.1.7, $f(x) \nmid h(x)$, где $f(x)$ — минимальный многочлен числа α. Таким образом, $(f(x), g(x)) = 1$, так что по лемме 4 (§ 2, гл. 1) $s(x) f(x) + t(x) h(x) = 1$ для элементов $s(x)$, $t(x) \in \mathbf{Q}[x]$. Положив $x = \alpha$, получим $t(\alpha) h(\alpha) = 1$. Таким образом, $h(\alpha)^{-1} \in \mathbf{Q}[\alpha]$. Если $\beta \in \mathbf{Q}(\alpha)$, то $\beta = g(\alpha) h(\alpha)^{-1}$ для $g(x)$, $h(x) \in \mathbf{Q}[x]$ и потому $\beta \in \mathbf{Q}[\alpha]$. □

Следствие. *Если* α — *некоторое алгебраическое число степени* n, *то* $[\mathbf{Q}(\alpha) : \mathbf{Q}] = n$.

Доказательство. Согласно предложению 6.1.8, достаточно показать, что $[\mathbf{Q}[\alpha] : \mathbf{Q}] = n$. Так как $f(\alpha) = 0$, то нетрудно убедиться в том, что $1, \ldots, \alpha^{n-1}$ порождают $\mathbf{Q}[\alpha]$. Если, с другой стороны, $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} = 0$, $a_i \in \mathbf{Q}$, то $g(\alpha) = 0$ для $g(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$. Тогда, согласно предложению 6.1.7, $f(x) \mid g(x)$. Но $\deg(g(x)) < \deg(f(x))$, откуда получаем, что $a_0 = a_1 = \ldots = a_{n-1} = 0$. Поэтому $1, \alpha, \ldots, \alpha^{n-1}$ линейно независимы над $\mathbf{Q}$. □

§ 2. Квадратичный характер числа 2 [1])

Пусть $\zeta = e^{2\pi i/8}$. Тогда ζ — примитивный корень степени 8 из единицы. Таким образом, $0 = \zeta^8 - 1 = (\zeta^4 - 1)(\zeta^4 + 1)$. Так как $\zeta^4 \neq 1$, то $\zeta^4 = -1$. Умножая это равенство на ζ^{-2} и прибавляя ζ^{-2} к обеим частям, получаем $\zeta^2 + \zeta^{-2} = 0$. Это равенство легко получить также, если заметить, что $\zeta^2 = e^{i(\pi/2)} = i$.

Квадратичный характер числа 2 будет получен теперь из соотношения

$$(\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = 2.$$

[1]) См. примечание к гл. 5, конец § 3. — *Прим. ред.*

Положим $\tau = \zeta + \zeta^{-1}$ и заметим, что ζ и τ — целые алгебраические числа. Следовательно, мы можем работать со сравнениями в кольце целых алгебраических чисел.

Пусть p — некоторое нечетное простое число из $\mathbf{Z}$. Заметим, что

$$\tau^{p-1} = (\tau^2)^{(p-1)/2} = 2^{(p-1)/2} \equiv (2/p) \ (p).$$

Отсюда следует, что $\tau^p \equiv (2/p)\,\tau \ (p)$. Согласно предложению 6.1.6, $\tau^p = (\zeta + \zeta^{-1})^p \equiv \zeta^p + \zeta^{-p} \ (p)$.

Вспоминая, что $\zeta^8 = 1$, получаем $\zeta^p + \zeta^{-p} = \zeta + \zeta^{-1}$ для $p \equiv \pm 1$ (8) и $\zeta^p + \zeta^{-p} = \zeta^3 + \zeta^{-3}$ для $p \equiv \pm 3$ (8). В последнем случае результат может быть упрощен, если заметить, что из $\zeta^4 = -1$ следует, что $\zeta^3 = -\zeta^{-1}$. Таким образом, $\zeta^p + \zeta^{-p} = -(\zeta + \zeta^{-1})$ при $p \equiv \pm 3$ (8). В итоге получаем

$$\zeta^p + \zeta^{-p} = \begin{cases} \tau & \text{при } p \equiv \pm 1 \ (8), \\ -\tau & \text{при } p \equiv \pm 3 \ (8). \end{cases}$$

Подставляя этот результат в соотношение $\tau^p \equiv (2/p)\,\tau \ (p)$, приходим к сравнению

$$(-1)^\varepsilon \tau \equiv \left(\frac{2}{p}\right) \tau \ (p), \text{ где } \varepsilon \equiv \frac{p^2-1}{8} \ (2).$$

Умножим обе части этого сравнения на τ. В результате получим

$$(-1)^\varepsilon 2 \equiv \left(\frac{2}{p}\right) 2 \ (p),$$

откуда следует, что

$$(-1)^\varepsilon \equiv \left(\frac{2}{p}\right) \ (p).$$

Последнее означает, что $(2/p) = (-1)^\varepsilon$, а это мы и хотели установить.

В одной ранней статье Эйлер (1707—1783) доказал, что 2 есть квадратичный вычет по модулю простых чисел $p \equiv 1$ (8). Его метод содержит ключевую идею приведенного выше доказательства.

Эйлер высказал гипотезу о том, что $U(\mathbf{Z}/p\mathbf{Z})$ — циклическая группа. Первым дал строгое доказательство этого факта Гаусс (см. теорему 1 гл. 4). Пусть λ — некоторый образующий группы $U(\mathbf{Z}/p\mathbf{Z})$. Положим $\gamma = \lambda^{(p-1)/8}$. Тогда γ имеет порядок 8, так что $\gamma^4 = -\overline{1}$ и $\gamma^2 + \gamma^{-2} = 0$. Поэтому $(\gamma + \gamma^{-1})^2 = \gamma^2 + \overline{2} + \gamma^{-2} = \overline{2}$. Это показывает, что $\overline{2}$ — квадрат в $U(\mathbf{Z}/p\mathbf{Z})$. Последнее же эквивалентно тому, что 2 — квадратичный вычет по модулю p.

При $p \not\equiv 1$ (8) это доказательство не может быть даже начато. Однако теория конечных полей позволяет при помощи идеи Эйлера провести полное доказательство квадратичного закона взаимности. Теория конечных полей будет развита в гл. 7.

§ 3. Квадратичные суммы Гаусса

Установив соотношение $(\zeta + \zeta^{-1})^2 = 2$, можно спросить, существует ли подобное соотношение, если заменить 2 на некоторое нечетное простое число. Ответ утвердительный, и, более того, из этого нового соотношения при помощи метода, использованного в § 2, следует полный квадратичный закон взаимности.

Всюду в этом параграфе ζ будет обозначать $e^{2\pi i/p}$, примитивный корень степени p из единицы.

Лемма 1. *Сумма* $\sum_{t=0}^{p-1} \zeta^{at}$ *равна* p *при* $a \equiv 0\ (p)$. *В противном случае она равна нулю.*

Доказательство. Если $a \equiv 0\ (p)$, то $\zeta^a = 1$, а потому $\sum_{t=0}^{p-1} \zeta^{at} = p$. Если $a \not\equiv 0\ (p)$, то $\zeta^a \neq 1$ и $\sum_{t=0}^{p-1} \zeta^{at} = (\zeta^{ap} - 1)/(\zeta^a - 1) = 0$.

Следствие. $p^{-1} \sum_{t=0}^{p-1} \zeta^{t(x-y)} = \delta(x, y)$, *где* $\delta(x, y) = 1$ *при* $x \equiv y\ (p)$ *и* $\delta(x, y) = 0$ *при* $x \not\equiv y\ (p)$.

Доказательство. Доказательство сразу же получается из леммы 1. □

Все суммирования до конца этого параграфа будут распространяться на индексы от нуля до $p - 1$. Это позволяет упростить обозначения.

Лемма 2. $\sum_t (t/p) = 0$, *где* (t/p) — *символ Лежандра.*

Доказательство. По определению $(0/p) = 0$. Из оставшихся $p - 1$ членов суммы половина равна $+1$, а другая половина равна -1, ибо, согласно следствию 1 предложения 5.1.2, квадратичных вычетов по модулю p имеется столько же, сколько невычетов. □

Мы теперь в состоянии ввести понятие суммы Гаусса.

Определение. $g_a = \sum_t (t/p)\, \zeta^{at}$ называется *квадратичной суммой Гаусса.*

Предложение 6.3.1. $g_a = (a/p)\, g_1$.

Доказательство. Если $a \equiv 0\ (p)$, то $\zeta^{at} = 1$ для всех t и $g_a = \sum (t/p) = 0$ по лемме 2. Это дает нужный результат в случае, когда $a \equiv 0\ (p)$.

Предположим теперь, что $a \not\equiv 0\ (p)$. Тогда

$$\left(\frac{a}{p}\right) g_a = \sum_t \left(\frac{at}{p}\right) \zeta^{at} = \sum_x \left(\frac{x}{p}\right) \zeta^x = g_1.$$

Мы воспользовались тем фактом, что at пробегает полную систему вычетов по модулю p, когда t ее пробегает, и что (x/p) и ζ^x зависят лишь от класса вычетов x по модулю p.

Так как $(a/p)^2 = 1$ при $a \not\equiv 0\ (p)$, наш результат получается умножением обеих частей равенства $(a/p)\, g_a = g_1$ на (a/p). □

В дальнейшем мы будем обозначать g_1 через g. Из предложения 6.3.1 следует, что $g_a^2 = g^2$, если $a \not\equiv 0\ (p)$. Сейчас мы вычислим это общее значение.

Предложение 6.3.2. $g^2 = (-1)^{(p-1)/2} p$.

Доказательство. Идея доказательства состоит в вычислении суммы $\sum_a g_a g_{-a}$ двумя способами.

Если $a \not\equiv 0\ (p)$, то $g_a g_{-a} = (a/p)\,(-a/p)\, g^2 = (-1/p)\, g^2$. Отсюда вытекает, что

$$\sum_a g_a g_{-a} = \left(\frac{-1}{p}\right)(p-1)\, g^2.$$

Далее заметим, что

$$g_a g_{-a} = \sum_x \sum_y \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \zeta^{a(x-y)}.$$

Суммируя обе части по a и используя следствие леммы 1, получаем

$$\sum_a g_a g_{-a} = \sum_{x,\ y} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \delta(x,\ y)\, p = (p-1)\, p.$$

Объединяя эти результаты, получаем $(-1/p)\,(p-1)\, g^2 = (p-1)\, p$. Поэтому $g^2 = (-1/p)\, p$. □

Пусть $p^* = (-1)^{(p-1)/2} p$. Равенство $g^2 = p^*$ и есть искомый аналог равенства $\tau^2 = 2$. Пусть $q \neq p$ — некоторое другое нечетное простое число. Мы приступим к доказательству квадратичного закона взаимности с помощью сравнений по модулю q в кольце целых алгебраических чисел:

$$g^{q-1} = (g^2)^{(q-1)/2} = p^{*\,(q-1)/2} \equiv \left(\frac{p^*}{q}\right)\ (q).$$

Таким образом,

$$g^q \equiv \left(\frac{p^*}{q}\right) g\ (q),$$

Используя предложение 6.1.6, убеждаемся в том, что

$$g^q = \left(\sum \left(\frac{t}{p}\right) \zeta^t\right)^q \equiv \sum \left(\frac{t}{p}\right)^q \zeta^{qt} = g_q\ (q).$$

Отсюда следует, что $g^q \equiv g_q\ (q) \equiv (q/p)\ g\ (q)$, а значит,

$$\left(\frac{q}{p}\right) g \equiv \left(\frac{p^*}{q}\right) g\ (q).$$

Умножим обе части этого равенства на g и используем тот факт, что $g^2 = p^*$:

$$\left(\frac{q}{p}\right) p^* \equiv \left(\frac{p^*}{q}\right) p^*\ (q),$$

откуда получаем

$$\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right)\ (q)$$

и, наконец,

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right).$$

Чтобы убедиться в том, что этот результат и есть то, что мы хотели получить, заметим, что

$$\left(\frac{p^*}{q}\right) = \left(\frac{-1}{q}\right)^{(p-1)/2} \left(\frac{p}{q}\right) = (-1)^{((q-1)/2)\ ((p-1)/2)} \left(\frac{p}{q}\right).$$

Использованное нами понятие квадратичной гауссовой суммы можно существенно обобщить. Некоторые из этих обобщений мы изложим после того, как разовьем теорию конечных полей. Кубические гауссовы суммы будут использованы для доказательства кубического закона взаимности, а биквадратичные суммы — для доказательства биквадратичного закона взаимности.

§ 4. Знак квадратичной суммы Гаусса[1])

Согласно предложению 6.3.2, квадратичная гауссова сумма имеет значение $\pm\sqrt{p}$ при $p \equiv 1\ (4)$ и $\pm i\sqrt{p}$ при $p \equiv 3\ (4)$. Таким образом, $g\ (\chi)$ определена с точностью до знака. Определение знака является значительно более трудной проблемой. Гипотеза о том, что во всех случаях имеет место знак плюс, была выдвинута Гауссом. Он занес ее в дневник в мае 1801 г., но лишь спустя четыре

[1]) В этом параграфе гауссова сумма g будет обозначаться через $g\ (\chi)$, где по определению $\chi\ (t) = (t/p)$.

года нашел ее доказательство. 30 августа 1805 г. Гаусс записывает в своем дневнике, что доказательство «очень элегантной теоремы, упомянутой в 1801 г., наконец-то получено». Он написал своему другу Олберсу 3 сентября 1805 г., что за эти четыре года редко выдавалась неделя, в течение которой он не пытался бы доказать свою гипотезу. Наконец, согласно Гауссу, «Wie der Blitz einschlägt, hat sich das Räthsel gelöst ...» (решение задачи возникло как вспышка молнии).

Затем доказательства были получены Дирихле, Коши, Кронекером, Мертенсом, Шуром и другими. В этом параграфе мы излагаем одно из доказательств Кронекера.

Как и в предыдущем параграфе, $\zeta = e^{2\pi i/p}$. Тогда $1, \zeta, \ldots, \zeta^{p-1}$ суть корни многочлена $x^p - 1$.

Предложение 6.4.1. *Многочлен* $1 + x + \ldots + x^{p-1}$ *неприводим в* $\mathbf{Q}[x]$.

Доказательство. Согласно упр. 4 в конце этой главы (лемма Гаусса), достаточно показать, что $1 + x + \ldots + x^{p-1}$ не имеет нетривиального разложения в $\mathbf{Z}[x]$. Предположим, что утверждение неверно и $1 + x + \ldots + x^{p-1} = f(x)\,g(x)$, где $f(x), g(x) \in \mathbf{Z}[x]$ и каждый из многочленов $f(x), g(x)$ имеет степень больше 0. Полагая $x = 1$, получим $p = f(1)\,g(1)$. Поэтому можно считать, что $g(1) = 1$. Используя черту для обозначения приведения по модулю p, получаем, что $\overline{g}(\overline{1}) \neq \overline{0}$. С другой стороны, так как $p \Big| \binom{p}{j}$, $j = 1, \ldots, p-1$, то $x^p - 1 \equiv (x-1)^p \ (p)$ и деление обеих частей на $x - 1$ показывает, что $1 + x + \ldots + x^{p-1} \equiv (x-1)^{p-1} \ (p)$. В силу теоремы 2 из гл. 1 и предложения 3.3.2 отсюда следует, что $g(x) \equiv (x-1)^s \ (p)$ для некоторого положительного целого числа s. Однако это противоречит тому факту, что $\overline{g}(\overline{1}) \neq \overline{0}$. Доказательство завершено. □

Объединяя полученное предложение с предложением 6.1.7, получаем, что если $g(\zeta) = 0$ для многочлена $g(x) \in \mathbf{Q}[x]$, то $1 + x + \ldots + x^{p-1} \mid g(x)$. Это наблюдение будет в дальнейшем полезно.

Предложение 6.4.2. $\prod_{k=1}^{(p-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)})^2 = (-1)^{(p-1)/2} p.$

Доказательство. Имеет место равенство $x^p - 1 = (x-1) \prod_{j=1}^{p-1} (x - \zeta^j)$, где произведение берется по любой полной системе представителей ненулевых классов вычетов по модулю p. Не-

трудно убедиться, что целые числа $\pm(4k-2)$, $k=1, 2, \ldots, (p-1)/2$, будут такой системой вычетов. Таким образом,

$$p = \prod(1-\zeta^{4k-2})\prod(1-\zeta^{-(4k-2)}) =$$
$$= \prod(\zeta^{-(2k-1)}-\zeta^{2k-1})\prod(\zeta^{2k-1}-\zeta^{-(2k-1)}) =$$
$$= (-1)^{(p-1)/2}\prod(\zeta^{2k-1}-\zeta^{-(2k-1)})^2,$$

где все произведения берутся по $k=1, 2, \ldots, (p-1)/2$. □

Предложение 6.4.3.

$$\prod_{k=1}^{(p-1)/2}(\zeta^{2k-1}-\zeta^{-(2k-1)}) = \begin{cases} \sqrt{p}, & \text{если } p \equiv 1\ (4), \\ i\sqrt{p}, & \text{если } p \equiv 3\ (4). \end{cases}$$

Доказательство. В силу предложения 6.4.2 мы должны вычислить лишь знак произведения. Оно равно

$$i^{(p-1)/2}\prod_{k=1}^{(p-1)/2} 2\sin\frac{(4k-2)\pi}{p}.$$

Но $\sin((4k-2)/p)\pi < 0$, если $(p+2)/4 < k \leqslant (p-1)/2$. Отсюда следует, что произведение имеет $(p-1)/2 - [(p+2)/4]$ отрицательных членов, что равно $(p-1)/4$ или $(p-3)/4$ в зависимости от того, справедливо сравнение $p \equiv 1\ (4)$ или сравнение $p \equiv 3\ (4)$. Доказываемый результат следует отсюда непосредственно. □

Из предложений 6.3.2 и 6.4.2 вытекает, что

$$g(\chi) = \varepsilon \prod_{k=1}^{(p-1)/2}(\zeta^{2k-1}-\zeta^{-(2k-1)}), \qquad (1)$$

где $\varepsilon = \pm 1$. Если мы сможем показать, что $\varepsilon = +1$, то вычисление гауссовой суммы будет завершено, согласно предложению 6.4.3. Следующее рассуждение Кронекера показывает, что именно так дело и обстоит. См. также упр. 22.

Предложение 6.4.4. $\varepsilon = +1$.

Доказательство. Рассмотрим многочлен

$$f(x) = \prod_{j=1}^{p-1}\chi(j)\,x^j - \varepsilon\prod_{k=1}^{(p-1)/2}(x^{2k-1}-x^{p-(2k-1)}). \qquad (2)$$

Тогда $f(\zeta) = 0$ по (1) и $f(1) = 0$ в силу леммы 2. Согласно замечанию, предшествующему предложению 6.4.2, и тому факту, что

$1 + x + \ldots + x^{p-1}$ и $x - 1$ взаимно просты, $f(x)$ делится на $x^p - 1$. Записав $f(x) = (x^p - 1)\,h(x)$ и подставив e^z вместо x, получим

$$\sum_{j=1}^{p-1} \chi(j)\, e^{jz} = \varepsilon \prod_{k=1}^{(p-1)/2} \left(e^{(2k-1)z} - e^{z(p-(2k-1))}\right) = (e^{pz} - 1)\,h(e^z). \quad (3)$$

Коэффициент при $z^{(p-1)/2}$ в левой части равенства (3), как нетрудно убедиться, равен

$$\frac{\sum_{j=1}^{p-1} \chi(j)\, j^{(p-1)/2}}{((p-1)/2)!} = \varepsilon \prod_{k=1}^{(p-1)/2} (4k - p - 2).$$

С другой стороны, согласно упр. 21, коэффициент при $z^{(p-1)/2}$ в правой части равенства (3) равен pA/B, где $p \nmid B$, причем A и B — целые числа. Приравнивая коэффициенты, умножая на B $((p-1)/2)!$ и приводя по модулю p, получаем, что

$$\begin{aligned}\sum_{j=1}^{p-1} \chi(j)\, j^{(p-1)/2} &\equiv \varepsilon \left(\frac{p-1}{2}\right)! \prod_{k=1}^{(p-1)/2} (4k-2) \pmod p \equiv \\ &\equiv \varepsilon\,(2\cdot 4\cdot 6 \ldots (p-1)) \prod_{k=1}^{(p-1)/2} (2k-1) \pmod p \equiv \\ &\equiv \varepsilon\,(p-1)! \pmod p \equiv \\ &\equiv -\varepsilon \pmod p,\end{aligned}$$

если воспользоваться теоремой Вильсона (следствие предложения 4.1.1).

По предложению 5.1.2 $j^{(p-1)/2} \equiv \chi(j) \pmod p$, так что

$$\sum_{j=1}^{p-1} \chi(j)^2 \equiv (p-1) \pmod p \equiv -\varepsilon \pmod p$$

и потому

$$\varepsilon \equiv 1 \pmod p.$$

Так как $\varepsilon = \pm 1$, то мы, наконец, приходим к равенству $\varepsilon = 1$. Это завершает доказательство. □

Полученный результат может быть сформулирован следующим образом.

Теорема 1. *Величина квадратичной суммы Гаусса $g(\chi)$ выражается формулой*

$$g(\chi) = \begin{cases} \sqrt{p} & \text{при } p \equiv 1 \pmod 4, \\ i\sqrt{p} & \text{при } p \equiv 3 \pmod 4. \end{cases}$$

Замечания

В знаменитом одиннадцатом дополнении к книге Дирихле [127] (1893 г.) Дедекинд ввел понятие *алгебраического числа* (§ 164), а также понятие целого алгебраического числа (§ 173). Однако значительно раньше некоторые целые алгебраические числа, как, например, гауссовы суммы, использовались при доказательстве квадратичного закона взаимности Эйзенштейном, Якоби и другими. Среди различных доказательств этой теоремы, полученных Гауссом, особенно важны четвертое (1811 г.) и шестое (1818 г.). Четвертое доказательство является следствием замечательного вычисления Гауссом значения классической гауссовой суммы. Хотя, как мы упоминали в § 4, он доказал этот результат в 1805 г., опубликовано доказательство было лишь в 1811 г. в знаменитой статье [34]. В этой статье он установил более общий результат, а именно: если n — любое целое положительное число, то $\sum_{t=0}^{n-1} \zeta^{t^2}$ принимает значения $\sqrt{n}$ или $i\sqrt{n}$ в зависимости от того, справедливо сравнение $n \equiv 1\ (4)$ или сравнение $n \equiv 3\ (4)$. Здесь $\zeta = e^{2\pi i/n}$. Рассуждения в этой статье весьма изобретательные. Изложение этого доказательства на английском языке имеется в [60], с. 174—180. Из этого результата нетрудно получить квадратичный закон взаимности (см., например, [125], с. 253—256).

Шестое и последнее опубликованное Гауссом доказательство квадратичного закона взаимности появилось в печати в 1818 г. под заглавием «Neue Beweise und Erweiterungen des Fundamentalsatzes in der Lehre von den Quadratischen Resten» («Новые *доказательства и обобщения основной теоремы учения о квадратичных* вычетах») [34], с. 636—654. Во введении к этой статье он упоминает о том, что в течение нескольких лет разыскивал такой метод, который обобщался бы на кубический и биквадратичный случаи, и что, наконец, его непрерывные усилия увенчались успехом. Он утверждает, что цель публикации этого шестого доказательства состоит в том, чтобы привести ту часть высшей арифметики, которая касается квадратичных вычетов, в законченный вид и, в некотором смысле, проститься с ней («...und so diesem Teile der höheren Arithmetik gewissermassen Lebewohl zu sagen»). В этом доказательстве Гаусс рассматривает многочлен $f_k(x) = \sum_{t=0}^{p-1} \chi(t)\, x^{kt}$ и доказывает без использования корней из единицы, что $1 + x + \ldots + x^{p-1}$ делит как $f_1(x)^2 - (-1)^{(p-1)/2} p$, так и $f_q(x) - (q/p)\, f_1(x)$. Закон взаимности следует из замечания, что $f_q(x) \equiv f_1(x)^q\ (q)$. Доказательство, приведенное нами в § 3, сводится к подстановке $x = \zeta$, $\zeta^p = 1$, в то, что получено, и к работе затем со сравнениями в кольце целых алгебраических чисел. Это наблюдение было сде-

лано (по крайней мере) Коши, Эйзенштейном и Якоби (в таком порядке) и представляет прочное основание для перехода к изучению высших законов взаимности посредством гауссовых сумм.

Начинающему изучение следует познакомиться с несколькими классическими введениями в теорию алгебраических чисел. Кроме упомянутых выше, мы сошлемся на [165] и [44]. Много изложений различной степени трудности появилось в последнее время. Мы упомянем здесь [84], [180] и [63].

Упражнения

1. Показать, что $\sqrt{2}+\sqrt{3}$ — целое алгебраическое число.

2. Пусть α — некоторое алгебраическое число. Показать, что существует такое целое число n, что $n\alpha$ будет целым алгебраическим числом.

3. Доказать, что если α и β — целые алгебраические числа, то любое решение уравнения $x^2+\alpha x+\beta=0$ будет целым алгебраическим числом. Обобщить этот результат.

4. Многочлен $f(x)\in \mathbf{Z}[x]$ называется *примитивным*, если наибольший общий делитель его коэффициентов равен 1. Доказать, что произведение примитивных многочленов примитивно. [*Указание*. Пусть $f(x)=a_0x^n+a_1x^{n-1}+\ldots$ $\ldots+a_n$ и $g(x)=b_0x^m+b_1x^{m-1}+\ldots+b_m$ примитивны. Если p—некоторое простое число, то пусть a_i и b_j—коэффициенты с наименьшими индексами, для которых $p\nmid a_i$ и $p\nmid b_j$. Показать, что коэффициент при $x^{n+m-i-j}$ в $f(x)\,g(x)$ не делится на p.] Это один из многих результатов, известных как лемма Гаусса.

5. Пусть α — некоторое целое алгебраические число и $f(x)\in \mathbf{Q}(x)$ — приведенный многочлен наименьшей степени, для которого $f(\alpha)=0$. Воспользовавшись упр. 4, показать, что $f(x)\in \mathbf{Z}[x]$.

6. Пусть $x^2+mx+n\in \mathbf{Z}[x]$ неприводим и α — его корень. Показать, что $\mathbf{Q}[\alpha]=\{r+s\alpha \mid r,\ s\in \mathbf{Q}\}$ будет кольцом (на самом деле это поле). Пусть $m^2-4n=D_0^2D$, где D свободно от квадратов. Показать, что $\mathbf{Q}[\alpha]=\mathbf{Q}[\sqrt{D}]$.

7 (продолжение). Если $D\equiv 2,\ 3\ (4)$, то показать, что все целые алгебраические числа в $\mathbf{Q}[\sqrt{D}]$ имеют вид $a+b\sqrt{D}$, где $a,\ b\in \mathbf{Z}$. Если $D\equiv 1\ (4)$, то показать, что все целые алгебраические числа в $\mathbf{Q}[\sqrt{D}]$ имеют вид $a+b\left((-1+\sqrt{D})/2\right)$, где $a,\ b\in \mathbf{Z}$. [*Указание*. Показать, что $r+s\sqrt{D}$ удовлетворяет уравнению $x^2-2rx+(r^2-Ds^2)=0$. Поэтому, согласно упр. 5, $r+s\sqrt{D}$ является целым алгебраическим числом тогда и только тогда, когда $2r$ и r^2-Ds^2 принадлежат $\mathbf{Z}$.]

8. Пусть $\omega=e^{2\pi i/3}$. Это число удовлетворяет уравнению $x^3-1=0$. Показать, что $(2\omega+1)^2=-3$, и использовать это для определения $(-3/p)$ методом из § 2.

9. Явно проверить предложение 6.3.2 для $p=3$ и $p=5$, т. е. выписать гауссовы суммы и возвести их в квадрат.

10. Чему равно $\sum_{a=1}^{p-1} g_a$?

11. Вычисляя $\sum_t (1+(t/p))\,\zeta^t$ двумя способами, доказать, что $g=\sum_t \zeta^{t^2}$.

12. Положим $\psi_a=\zeta^{at}$. Показать, что

(a) $\overline{\psi_a(t)}=\psi_a(-t)=\psi_{-a}(t)$;

(b) $p^{-1}\sum_a \psi_a(t-s)=\delta(t,s)$.

13. Пусть f — некоторое отображение из $\mathbf{Z}$ в комплексные числа. Предположим, что p — простое число и что $f(n+p) = f(n)$ для всех $n \in \mathbf{Z}$. Пусть $\hat{f}(a) = p^{-1} \sum_t f(t)\, \psi_{-a}(t)$. Доказать, что $f(t) = \sum_a \hat{f}(a)\, \psi_a(t)$. Этот результат аналогичен соответствующему результату в теории рядов Фурье.

14. В упр. 13 взять в качестве f символ Лежандра и показать, что $\hat{f}(a) = p^{-1} g_{-a}$.

15. Показать, что $\left| \sum_{t=m}^{n} (t/p) \right| < \sqrt{p} \ln p$. Неравенство выполняется для сумм по любому интервалу. Это замечательное неравенство связано с именами Пойа и И. М. Виноградова (см. [22*], с. 789, [10*], гл. III, § 2. — *Ред.*). [*Указание.* Воспользоваться соотношением $(t/p)g = g_t$ и просуммировать. Будет полезным также неравенство $\sin x \geqslant (2/\pi)\, x$ для любого острого угла.]

16. Пусть α — некоторое алгебраическое число с минимальным многочленом $f(x)$. Показать, что $f(x)$ не имеет в $\mathbf{C}$ кратных корней.

17. Показать, что минимальным многочленом для $\sqrt[3]{2}$ будет $x^3 - 2$.

18. Показать, что существуют алгебраические числа произвольно высокой степени.

19. Найти сопряженные для числа $\cos 2\pi/5$.

20. Пусть F — некоторое подполе в $\mathbf{C}$, являющееся конечномерным векторным пространством над $\mathbf{Q}$ размерности n. Показать, что каждый элемент из F алгебраичен и степени не больше n. [*Замечание.* Труднее доказать существование элемента степени точно n. (См. упр. 17 из гл. 12.)]

21. Пусть $f(x) = \sum_{n=0}^{\infty} a_n x^n/n!$ и $g(x) = \sum_{n=0}^{\infty} b_n x^n/n!$ — степенные ряды с целыми a_n и b_n. Показать, что если p — такое простое число, что $p \mid a_i$ для $i = 0, \ldots, p-1$, то каждый коэффициент c_t в произведении $f(x)\, g(x) = \sum_{n=0}^{\infty} c_n x^n$ для $t = 0, \ldots, p-1$ может быть записан в виде $p\,(A/B)$, $p \nmid B$.

22. Показать, что соотношение $\varepsilon \equiv 1\ (p)$ в предложении 6.4.4 может быть также получено при подстановке вместо x не e^z, а $1 + t$.

23. Показать, что если $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$, $a_i \in \mathbf{Z}$, и p — такое простое число, что $p \mid a_i$, $i = 1, \ldots, n$, $p^2 \nmid a_n$, то $f(x)$ неприводим над $\mathbf{Q}$ (критерий неприводимости Эйзенштейна).

Глава 7

КОНЕЧНЫЕ ПОЛЯ

С примерами конечных полей мы уже встречались, а именно с полями $\mathbf{Z}/p\mathbf{Z}$, *где* p — *некоторое простое число. В этой главе мы докажем, что существует значительно больше конечных полей, и исследуем их свойства. Эта красивая теория, интересная и сама по себе, является, кроме того, очень полезным инструментом в теоретико-числовых исследованиях. В качестве иллюстрации последнего утверждения мы приведем еще одно доказательство квадратичного закона взаимности. Позднее будут указаны и другие приложения.*

Еще одно замечание. До сих пор в большей части наших доказательств было использовано очень мало результатов из абстрактной алгебры. Хотя нигде в этой книге и не используются очень сложные результаты из алгебры, начиная с этого места, мы будем предполагать, что читатель имеет некоторое знакомство с материалом стандартного студенческого курса по этому предмету.

§ 1. Основные свойства конечных полей

В этом параграфе мы обсуждаем свойства конечных полей, не задаваясь вопросом об их существовании. Построением конечных полей мы займемся в § 2.

Пусть F — некоторое конечное поле из q элементов. Мультипликативная группа F^* поля F имеет $q-1$ элементов. Поэтому каждый элемент $\alpha \in F^*$ удовлетворяет уравнению $x^{q-1} = 1$ (здесь 1 обозначает мультипликативную единицу поля F, а не целое число 1), а каждый элемент в F — уравнению $x^q = x$.

Предложение 7.1.1. $x^q - x = \prod_{\alpha \in F} (x - \alpha)$.

Доказательство. Оба многочлена следует рассматривать как элементы из $F[x]$.

Каждый элемент $\alpha \in F$ является корнем многочлена $x^q - x$. Так как F имеет q элементов и степень $x^q - x$ равна q, наш результат доказан. □

Следствие 1. *Пусть* $F \subset K$, *где* K — *некоторое поле. Элемент* $\alpha \in K$ *принадлежит* F *в том и только том случае, когда* $\alpha^q = \alpha$.

Доказательство. Равенство $\alpha^q = \alpha$ имеет место тогда и только тогда, когда α есть корень многочлена $x^q - x$. Согласно предложению 7.1.1, корни многочлена $x^q - x$ — это в точности элементы поля F. □

Следствие 2. *Если многочлен $f(x)$ делит $x^q - x$, то он имеет d различных корней, где d — степень $f(x)$.*

Доказательство. Пусть $f(x)\,g(x) = x^q - x$. Многочлен $g(x)$ имеет степень $q - d$. Если бы $f(x)$ имел менее чем d различных корней, то по лемме 1 гл. 4 $f(x)\,g(x)$ имел бы менее, чем $d + (q - d) = q$ различных корней, что не так. □

Теорема 1. *Мультипликативная группа конечного поля циклична.*

Доказательство. Эта теорема есть обобщение теоремы 1 из гл. 4. Доказательства их почти совпадают.

Если $d \mid q - 1$, то $x^d - 1$ делит $x^{q-1} - 1$, и из следствия 2 получаем, что $x^d - 1$ имеет d различных корней. Таким образом, подгруппа в F^*, состоящая из элементов, удовлетворяющих уравнению $x^d = 1$, имеет порядок d.

Пусть $\psi(d)$ обозначает число элементов в F^* порядка d. Тогда $\sum_{c \mid d} \psi(c) = d$. По формуле обращения Мёбиуса

$$\psi(d) = \sum_{c \mid d} \mu(c) \frac{d}{c} = \varphi(d).$$

В частности, $\psi(q - 1) = \varphi(q - 1) > 1$, если только перед нами не тривиальный случай $q = 2$. □

Тот факт, что группа F^* циклическая, когда F конечно, позволяет дать следующее частичное обобщение предложения 4.2.1.

Предложение 7.1.2. *Пусть $\alpha \in F^*$. Тогда уравнение $x^n = \alpha$ имеет решение в том и только том случае, когда $\alpha^{(q-1)/d} = 1$, где $d = (n, q - 1)$. Если решения имеются, то их будет точно d.*

Доказательство. Пусть γ — образующий элемент группы F^*, положим $\alpha = \gamma^a$ и $x = \gamma^y$. Тогда равенство $x^n = \alpha$ эквивалентно сравнению $ny \equiv a\,(q - 1)$. Доказываемый результат следует теперь из предложения 3.3.1. □

Стоит посмотреть, что произойдет в крайних случаях $n \mid q - 1$ и $(n, q - 1) = 1$.

Если $n \mid q-1$, то имеется точно $(q-1)/n$ элементов в F^*, которые являются n-ми степенями, и если α есть n-я степень, то уравнение $x^n = \alpha$ имеет n решений.

Если $(n, q-1) = 1$, то каждый элемент представляется n-й степенью единственным образом, т. е. для $\alpha \in F^*$ уравнение $x^n = \alpha$ имеет одно и только одно решение.

Мы исследовали структуру группы F^*. Обратим теперь наше внимание на аддитивную группу поля F.

Лемма 1. *Пусть F — конечное поле. Целочисленные кратные единичного элемента образуют подполе в F, изоморфное $\mathbf{Z}/p\mathbf{Z}$ для некоторого простого числа p.*

Доказательство. Во избежание недоразумений временно обозначим единицу группы F^* через e вместо 1. Отобразим $\mathbf{Z}$ в F посредством соответствия $n \to ne$. Как нетрудно убедиться, это будет кольцевой гомоморфизм. Его образом будет конечное подкольцо в F, так что, в частности, оно будет областью целостности. Его ядро есть некоторый ненулевой простой идеал. Следовательно, образ изоморфен $\mathbf{Z}/p\mathbf{Z}$ для некоторого простого числа p. □

Мы будем отождествлять $\mathbf{Z}/p\mathbf{Z}$ с его образом в F и представлять F в виде конечномерного векторного пространства над $\mathbf{Z}/p\mathbf{Z}$. Пусть n обозначает его размерность и $\omega_1, \omega_2, \ldots, \omega_n$ — базис. Тогда каждый элемент $\omega \in F$ может быть однозначно представлен в виде $a_1\omega_1 + a_2\omega_2 + \ldots + a_n\omega_n$, где $a_i \in \mathbf{Z}/p\mathbf{Z}$. Отсюда следует, что F имеет p^n элементов. Мы доказали

Предложение 7.1.3. *Число элементов в конечном поле есть степень некоторого простого числа.*

Если e — единичный элемент конечного поля F, то пусть p — наименьшее целое число со свойством $pe = 0$. Как мы убедились, p должно быть простым числом. Оно называется *характеристикой* поля F. Для $\alpha \in F$ имеем $p\alpha = p(e\alpha) = (pe)\alpha = 0 \cdot \alpha = 0$. Это наблюдение приводит к следующему очень полезному предложению.

Предложение 7.1.4. *Если F имеет характеристику p, то $(\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d}$ для всех $\alpha, \beta \in F$ и всех положительных целых чисел d.*

Доказательство. Применяем индукцию по d. При $d = 1$

$$(\alpha+\beta)^p = \alpha^p + \sum_{k=1}^{p-1} \binom{p}{k} \alpha^{p-k}\beta^k + \beta^p = \alpha^p + \beta^p.$$

Все средние члены равны нулю, так как $p \left| \binom{p}{k} \right.$ для $1 \leqslant k \leqslant p-1$ в силу леммы 2 гл. 4.

Для перехода от d к $d+1$ следует просто возвести обе части равенства $(\alpha+\beta)^{p^d} = \alpha^{p^d} + \beta^{p^d}$ в степень p. □

Предположим, что F — поле размерности n над $\mathbf{Z}/p\mathbf{Z}$. Мы хотим выяснить, какие поля E лежат между $\mathbf{Z}/p\mathbf{Z}$ и F. Если d — размерность E над $\mathbf{Z}/p\mathbf{Z}$, то из общей теории полей следует, что $d \mid n$. Другое доказательство этого факта мы приводим ниже. Оказывается, что существует одно и только одно промежуточное поле, соответствующее каждому делителю d числа n.

Лемма 2. *Пусть F — некоторое поле. Тогда $x^l - 1$ делит $x^m - 1$ в $F(x)$ в том и только том случае, когда l делит m.*

Доказательство. Пусть $m = ql + r$, где $0 \leqslant r < l$. Тогда

$$\frac{x^m-1}{x^l-1} = x^r \frac{x^{ql}-1}{x^l-1} + \frac{x^r-1}{x^l-1}.$$

Так как $(x^{ql}-1)/(x^l-1) = (x^l)^{q-1} + (x^l)^{q-2} + \ldots + x^l + 1$, правая часть написанного выше равенства будет многочленом в том и только том случае, когда $(x^r-1)/(x^l-1)$ есть многочлен. Как нетрудно убедиться, это имеет место тогда и только тогда, когда $r = 0$. Отсюда и следует наш результат. □

Лемма 3. *Если a — некоторое положительное целое число, то $a^l - 1$ делит $a^m - 1$ тогда и только тогда, когда l делит m.*

Доказательство. Оно аналогично доказательству леммы 2, причем число a играет роль x. Восстановить детали предоставляется читателю. □

Предложение 7.1.5. *Пусть F — поле размерности n над $\mathbf{Z}/p\mathbf{Z}$. Подполя поля F находятся во взаимно однозначном соответствии с делителями n.*

Доказательство. Предположим, что E — некоторое подполе поля F, и пусть d — его размерность над $\mathbf{Z}/p\mathbf{Z}$. Мы покажем, что $d \mid n$.

Так как E^* имеет $p^d - 1$ элементов, удовлетворяющих уравнению $x^{p^d-1} - 1 = 0$, то мы получаем, что $x^{p^d-1} - 1$ делит $x^{p^n-1} - 1$. В силу леммы 2 $p^d - 1$ делит $p^n - 1$, а следовательно, в силу леммы 3 d делит n.

Предположим теперь, что $d \mid n$. Пусть $E = \{\alpha \in F \mid \alpha^{p^d} = \alpha\}$. Мы утверждаем, что E есть поле. Действительно, если $\alpha, \beta \in E$, то

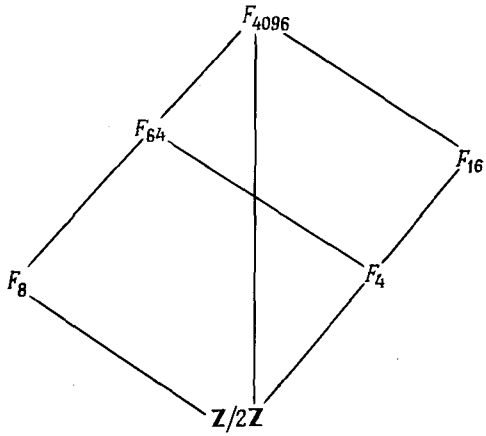
(a) $(\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d} = \alpha + \beta$;
(b) $(\alpha\beta)^{p^d} = \alpha^{p^d}\beta^{p^d} = \alpha\beta$;
(c) $(\alpha^{-1})^{p^d} = (\alpha^{p^d})^{-1} = \alpha^{-1}$ для $\alpha \neq 0$.

В п. (a) мы воспользовались предложением 7.1.4.

Далее, E есть множество решений уравнения $x^{p^d} - x = 0$. Так как $d \mid n$, то $p^d - 1 \mid p^n - 1$ и $x^{p^d-1} - 1 \mid x^{p^n-1} - 1$, согласно леммам 2 и 3. Таким образом, $x^{p^d} - x$ делит $x^{p^n} - x$, и в силу следствия 2 предложения 7.1.1 отсюда вытекает, что E имеет p^d элементов и, значит, имеет размерность d над $\mathbf{Z}/p\mathbf{Z}$.

Наконец, если E' — другое подполе в F размерности d над $\mathbf{Z}/p\mathbf{Z}$, то элементы из E' должны удовлетворять уравнению $x^{p^d} - x = 0$, т. е. E' должно совпадать с E. □

Пусть F_q обозначает конечное поле из q элементов. В качестве иллюстрации предложения 7.1.5 рассмотрим F_{4096} (в § 2 будет доказано существование такого поля). Так как $4096 = 2^{12}$, мы имеем следующую диаграмму вложений:



§ 2. Существование конечных полей

В § 1 мы доказали, что число элементов в некотором конечном поле имеет вид p^n, где p — простое число. Сейчас мы покажем, что для заданного числа p^n существует конечное поле из p^n элементов.

Для этого нам понадобятся некоторые результаты из теории полей, которые связывают нашу проблему с существованием неприводимых многочленов. Затем мы докажем теорему, восходящую к Гауссу (опять!), которая показывает, что $\mathbf{Z}/p\mathbf{Z}\,[x]$ содержит неприводимые многочлены любой степени.

Пусть k — произвольное поле и $f(x)$ — некоторый неприводимый многочлен в $k[x]$.

Предложение 7.2.1. *Существует такое поле K, содержащее k, и элемент $\alpha \in K$, что $f(\alpha) = 0$.*

Доказательство. В гл. 1 мы доказали, что $k[x]$ — область главных идеалов. Отсюда следует, что $(f(x))$ — максимальный идеал, а следовательно, $k[x]/(f(x))$ — поле. Пусть $K' = k[x]/(f(x))$ и φ — гомоморфизм, отображающий $k[x]$ на K' посредством взятия класса вычетов по модулю $(f(x))$. Мы имеем диаграмму

$$\begin{array}{ccc} k[x] & \xrightarrow{\varphi} & K' \\ \cup & & \cup \\ k & \xrightarrow{\varphi} & \varphi(k) \end{array}$$

$\varphi(k)$ есть подполе в K'. Мы утверждаем, что $\varphi(k)$ изоморфно k. Достаточно показать, что φ на k взаимно однозначно. Пусть $a \in k$. Если $\varphi(a) = 0$, то $a \in (f(x))$. Если $a \neq 0$, то этот элемент есть единица и не может принадлежать собственному идеалу. Таким образом, $a = 0$, что и следовало показать.

Так как φ — изоморфизм на k, мы можем отождествить k с $\varphi(k)$. После того как это сделано, мы обозначим K' через K. Пусть α — класс вычетов элемента x в K. Тогда $0 = \varphi(f(x)) = f(\varphi(x)) = f(\alpha)$, т. е. α — корень многочлена $f(x)$ в K. □

Мы обозначим поле K, построенное в предложении 7.2.1, через $k(\alpha)$. Будет полезным следующее утверждение о $k(\alpha)$.

Предложение 7.2.2. *Элементы $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ образуют базис векторного пространства $k(\alpha)$ над k, где n — степень многочлена $f(x)$.*

Доказательство этого предложения аналогично доказательству предложения 6.1.8 и его следствия. Следует заменить $\mathbf{Q}$ на k и комплексное число α этого предложения на α, введенное выше.

Если идти в обратном направлении, то это предложение показывает, что если мы хотим найти расширение K поля k степени n, то достаточно построить некоторый неприводимый многочлен $f(x) \in k[x]$ степени n.

В $\mathbf{Z}/p\mathbf{Z}[x]$ имеется конечное число многочленов заданной степени. Пусть $F_d(x)$ обозначает произведение всех приведенных неприводимых многочленов в $\mathbf{Z}/p\mathbf{Z}$ степени d.

Теорема 2. $x^{p^n} - x = \prod_{d \mid n} F_d(x)$.

Доказательство. Заметим сначала, что если $f(x)$ делит $x^{p^n} - x$, то $f(x)^2$ не делит $x^{p^n} - x$. Это следует из того, что если бы $x^{p^n} - x = f(x)^2 g(x)$, то формальным дифференцированием мы получили бы

$$-1 = 2f(x)\, f'(x)\, g(x) + f(x)^2 g'(x).$$

Последнее равенство невозможно, ибо оно означает, что $f(x)$ делит 1.

Остается доказать, что если $f(x)$ — некоторый приведенный неприводимый многочлен степени d, то $f(x) \mid x^{p^n} - x$ тогда и только тогда, когда $d \mid n$.

Рассмотрим поле $K = \mathbf{Z}/p\mathbf{Z}(\alpha)$, где α — корень многочлена $f(x)$, как в предложении 7.2.2. Оно имеет размерность d над $\mathbf{Z}/p\mathbf{Z}$ и, следовательно, p^d элементов. Элементы поля K удовлетворяют уравнению $x^{p^d} - x = 0$.

Предположим, что $x^{p^n} - x = f(x)\, g(x)$. Тогда $\alpha^{p^n} - \alpha = 0$. Если $b_1\alpha^{d-1} + b_2\alpha^{d-2} + \ldots + b_d$ — произвольный элемент поля K, то

$$(b_1\alpha^{d-1} + \cdots + b_d)^{p^n} = b_1 (\alpha^{p^n})^{d-1} + \cdots + b_d = b_1\alpha^{d-1} + \cdots + b_d.$$

Следовательно, элементы поля K удовлетворяют уравнению $x^{p^n} - x = 0$. Отсюда следует, что $x^{p^d} - x$ делит $x^{p^n} - x$ и $d \mid n$ в силу лемм 2 и 3 § 1.

Предположим теперь, что $d \mid n$. Так как $\alpha^{p^d} = \alpha$ и $f(x)$ — приведенный неприводимый многочлен для α, то $f(x) \mid x^{p^d} - x$. Поскольку $d \mid n$, то $x^{p^d} - x \mid x^{p^n} - x$ по леммам 2 и 3 § 1. Следовательно, $f(x) \mid x^{p^n} - x$. □

Пусть N_d — число приведенных неприводимых многочленов степени d в $\mathbf{Z}/p\mathbf{Z}[x]$. Приравнивание степеней обеих частей равенства в теореме 2 дает

Следствие 1. $p^n = \sum_{d \mid n} dN_d$.

Следствие 2. $N_n = n^{-1} \sum_{d \mid n} \mu(n/d)\, p^d$.

Доказательство. Применить формулу обращения Мёбиуса (теорема 1 гл. 2) к равенству из следствия 1. □

Следствие 3. *Для каждого целого числа $n \geqslant 1$ в $\mathbf{Z}/p\mathbf{Z}\,[x]$ существует неприводимый многочлен степени n.*

Доказательство. Имеем $N_n = n^{-1}(p^n - \ldots + p\mu(n))$ по следствию 2. Член в скобках не может быть равен нулю, так как он есть сумма различных степеней p с коэффициентами 1 и -1. □

Подводя итоги, получаем такой результат:

Теорема 3. *Пусть $n \geqslant 1$ — целое число и p — простое число. Тогда существует конечное поле из p^n элементов.*

§ 3. Приложение к квадратичным вычетам

В гл. 6 квадратичный закон взаимности был доказан с использованием сумм Гаусса и элементов теории алгебраических чисел. Мы приведем теперь исключительно короткое доказательство того же характера, но использующее теорию конечных полей.

Пусть p и q — различные нечетные простые числа. Так как $(p, q) = 1$, существует такое целое число n (например, $p - 1$), что $q^n \equiv 1\ (p)$. Пусть F — конечное поле размерности n над $\mathbf{Z}/q\mathbf{Z}$. Тогда группа F^* циклическая порядка $q^n - 1$. Пусть γ — некоторый образующий группы F^*, и положим $\lambda = \gamma^{(q^n-1)/p}$. Элемент λ имеет порядок p. Пусть $\tau_a = \sum_{t=0}^{p-1} (t/p)\lambda^{at}$, где $a \in \mathbf{Z}$. Элемент τ_a поля F является аналогом квадратичной гауссовой суммы, введенной в гл. 6. Положим $\tau_1 = \tau$. Тогда доказательства предложений 6.3.1 и 6.3.2 могут быть использованы для того, чтобы показать, что

(1) $\tau_a = (a/p)\,\tau$;

(2) $\tau^2 = (-1)^{(p-1)/2}\,\bar{p}$.

В соотношении (2) $\bar{p}$ обозначает класс элемента p в $\mathbf{Z}/q\mathbf{Z}$. Пусть $p^* = (-1)^{(p-1)/2}p$. В таком случае соотношение 2 может быть записано в виде $\tau^2 = \overline{p^*}$. Это соотношение означает, что $(p^*/q) = 1$ тогда и только тогда, когда $\tau \in \mathbf{Z}/q\mathbf{Z}$. В силу следствия 1 предложения 7.1.1 последнее выполняется в том и только том случае, когда $\tau^q = \tau$. Далее,

$$\tau^q = \left(\sum_t \left(\frac{t}{p}\right)\lambda^t\right)^q = \sum_t \left(\frac{t}{p}\right)\lambda^{qt} = \tau_q.$$

Согласно соотношению 1, $\tau_q = (q/p)\,\tau$. Таким образом, $\tau^q = \tau$ тогда и только тогда, когда $(q/p) = 1$.

Мы доказали, что

$$\left(\frac{p^*}{q}\right) = 1, \text{ если и только если } \left(\frac{q}{p}\right) = 1.$$

Это и есть квадратичный закон взаимности.

С использованием той же техники можно доказать, что $(2/q) = (-1)^{(q^2-1)/8}$. В гл. 6 мы привели доказательство Эйлера того факта, что $(2/q) = 1$, если $q \equiv 1\ (8)$. Если $q \not\equiv 1\ (8)$, то тем не менее верно, что $q^2 \equiv 1\ (8)$. В этом случае можно получить доказательство, работая в конечном поле F размерности 2 над $\mathbf{Z}/q\mathbf{Z}$. Восстановить детали мы предоставляем читателю.

Замечания

Первое систематическое изложение теории конечных полей было дано Диксоном [25], хотя еще Галуа аксиоматически вывел некоторые из их свойств в своей заметке «Sur la théorie des nombres» («Из теории чисел») [33]. Так как существование конечного поля из p^n элементов эквивалентно существованию некоторого неприводимого многочлена степени n в кольце $\mathbf{Z}/p\mathbf{Z}[x]$, мы должны опять сослаться на Гаусса как на основателя. В статье «Die Lehre von den Reste» («Учение об остатках») им получена приведенная нами формула для числа неприводимых многочленов степени n (см. [34]).

На возможность использования конечных полей для доказательства квадратичного закона взаимности обратили внимание многие математики, например, Хауснер [43] и Хольцер [45, с. 76—78].

Наше изложение теории конечных полей в этой книге гораздо элементарнее, чем обычное современное изложение. Чаще всего начинают с полного развития теории Галуа для полей, а затем применяют общие результаты этой теории к частному случаю конечных полей. Именно так построена компактная книга Альберта [1]. Ее преимущество для читателей, уже знакомых с теорией полей, состоит в том, что автор подробно изучает конечные поля в последней главе и приводит весьма обширную библиографию по этому предмету. В ней указано много очень интересных работ.

Упражнения

1. Используя метод доказательства теоремы 1, показать, что конечная подгруппа мультипликативной группы любого поля циклическая.

2. Пусть $\mathbf{R}$ и $\mathbf{C}$ — вещественные и комплексные числа соответственно. Найти конечные подгруппы в $\mathbf{R}^*$ и $\mathbf{C}^*$ и непосредственно показать, что они циклические.

3. Пусть F — поле из q элементов; предположим, что $q \equiv 1\ (n)$. Показать, что для $\alpha \in F^*$ уравнение $x^n = \alpha$ либо не имеет решений, либо имеет n решений.

4 (продолжение). Показать, что множество элементов $\alpha \in F^*$, для которых уравнение $x^n = \alpha$ разрешимо, является подгруппой, состоящей из $(q-1)/n$ элементов.

5 (продолжение). Пусть K — поле, содержащее F, и $[K:F] = n$. Показать, что для любого $\alpha \in F^*$ уравнение $x^n = \alpha$ имеет n решений в K. [*Указание.* Показать, что $q^n - 1$ делится на $n(q-1)$, и воспользоваться тем, что $\alpha^{q-1} = 1$.]

6. Пусть $K \supset F$ — конечные поля, причем $[K:F] = 3$. Показать, что если $\alpha \in F$ — не квадрат в F, то он — не квадрат в K.

7. Обобщая упр. 6, показать, что если элемент α — не квадрат в F, то он не будет квадратом ни в каком расширении поля F нечетной степени и будет квадратом в каждом расширении четной степени.

8. Описать подгруппу квадратов в поле из 2^n элементов.

9. Показать, что если $K \supset F$ — конечные поля, $|F| = q$ [1]), $\alpha \in F$, $q \equiv 1\ (n)$ и $x^n = \alpha$ не разрешимо в F, то $x^n = \alpha$ не разрешимо в K, когда $(n, [K:F]) = 1$.

10. Пусть $K \supset F$ — конечные поля и $[K:F] = 2$. Показать, что если $\beta \in K$, то $\beta^{1+q} \in F$ и, более того, каждый элемент в F имеет вид β^{1+q} для некоторого $\beta \in K$.

11. В ситуации упр. 10 предположим, что $\alpha \in F$ имеет порядок $q-1$. Показать, что существует элемент $\beta \in K$ порядка $q^2 - 1$, для которого $\beta^{1+q} = \alpha$.

12. Воспользовавшись предложением 7.2.1, показать, что для заданных поля k и многочлена $f(x) \in k[x]$ существует такое поле $K \supset k$, что степень $[K:k]$ конечна и $f(x) = (x-\alpha_1)(x-\alpha_2)\ \ldots\ (x-\alpha_n)$ в $K[x]$.

13. Применить упр. 12 к $k = \mathbf{Z}/p\mathbf{Z}$ и $f(x) = x^{p^n} - x$ и получить другое доказательство теоремы 2.

14. Пусть F — поле из q элементов и n — некоторое положительное целое число. Показать, что в $F[x]$ существуют неприводимые многочлены степени n.

15. Пусть $x^n - 1 \in F[x]$, где F — конечное поле из q элементов. Предположим, что $(q, n) = 1$. Показать, что $x^n - 1$ разлагается на линейные множители в некотором расширении поля F и что наименьшая степень такого расширения совпадает с наименьшим числом f, для которого $q^f \equiv 1\ (n)$.

16. Найти приведенные неприводимые многочлены степени 4 в $\mathbf{Z}/2\mathbf{Z}[x]$.

17. Пусть q и p — различные нечетные простые числа. Показать, что число приведенных неприводимых многочленов степени q в $\mathbf{Z}/p\mathbf{Z}$ равно $q^{-1}(p^q - p)$.

18. Пусть p — простое число, такое, что $p \equiv 3\ (4)$. Показать, что классы вычетов по модулю p в $\mathbf{Z}[i]$ образуют поле из p^2 элементов.

19. Пусть F — конечное поле из q элементов. Если $f(x) \in F[x]$ имеет степень t, положим $|f| = q^t$. Проверить формальное тождество $\sum_f |f|^{-s} = (1 - q^{1-s})^{-1}$. Сумма берется по всем приведенным многочленам.

20. В обозначениях упр. 19 пусть $d(f)$ — число приведенных делителей многочлена f и $\sigma(f) = \sum_{g \mid f} |g|$, где сумма берется по приведенным делителям f. Проверить следующие тождества:

(a) $\sum_f d(f)\,|f|^{-s} = (1 - q^{1-s})^{-2}$;

(b) $\sum_f \sigma(f)\,|f|^{-s} = (1 - q^{1-s})^{-1}(1 - q^{2-s})^{-1}$.

---

[1]) $|F|$ обозначает число элементов поля F. — *Прим. ред.*

21. Пусть F — поле из $q = p^n$ элементов. Для $\alpha \in F$ положим $f(x) = (x-\alpha)(x-\alpha^p)(x-\alpha^{p^2}) \ldots (x-\alpha^{p^{n-1}})$. Показать, что $f(x) \in \mathbf{Z}/p\mathbf{Z}[x]$. В частности, $\alpha + \alpha^p + \ldots + \alpha^{p^{n-1}}$ и $\alpha\alpha^p \ldots \alpha^{p^{n-1}}$ принадлежат $\mathbf{Z}/p\mathbf{Z}$.

22 (продолжение). Положим $\mathrm{tr}(\alpha) = \alpha + \alpha^p + \ldots + \alpha^{p^{n-1}}$. Доказать, что
(a) $\mathrm{tr}(\alpha) + \mathrm{tr}(\beta) = \mathrm{tr}(\alpha + \beta)$;
(b) $\mathrm{tr}(a\alpha) = a\,\mathrm{tr}(\alpha)$ для $a \in \mathbf{Z}/p\mathbf{Z}$;
(c) существует такой элемент $\alpha \in F$, что $\mathrm{tr}(\alpha) \neq 0$.

23 (продолжение). Рассмотрим многочлен $x^p - x - \alpha \in F[x]$, где $\alpha \in F$. Показать, что этот многочлен либо неприводим, либо является произведением линейных множителей. Доказать, что последнее имеет место тогда и только тогда, когда $\mathrm{tr}(\alpha) = 0$.

24. Предположим, что $f(x) \in \mathbf{Z}/p\mathbf{Z}[x]$ обладает свойством $f(x+y) = f(x) + f(y) \in \mathbf{Z}/p\mathbf{Z}[x, y]$. Показать, что $f(x)$ должен иметь вид $a_0x + a_1x^p + a_2x^{p^2} + \ldots + a_mx^{p^m}$.

Глава 8

СУММЫ ГАУССА И ЯКОБИ

В гл. 6 мы ввели понятие квадратичной гауссовой суммы. В этой главе будет введено более общее понятие гауссовой суммы. Эти суммы имеют много приложений. Они будут использованы в гл. 9 как инструмент для доказательства кубического и биквадратичного законов взаимности. Мы будем также рассматривать проблему подсчета числа решений уравнений с коэффициентами в некотором конечном поле. В связи с этим вопросом естественно возникает понятие суммы Якоби. Суммы Якоби интересны и сами по себе, и мы рассмотрим некоторые из их свойств.

Для простоты изложения мы ограничимся полем $\mathbf{Z}/p\mathbf{Z} = F_p$ *и лишь позднее обратимся к задаче определения гауссовых сумм над произвольными конечными полями.*

§ 1. Мультипликативные характеры

Мультипликативным характером на поле F_p (или *поля* F_p) называется отображение χ из F_p^* в множество отличных от нуля комплексных чисел, удовлетворяющее условию

$$\chi(ab) = \chi(a)\chi(b) \text{ для всех } a, b \in F_p^*.$$

Символ (a/p) является примером такого характера, если его рассматривать как функцию класса вычетов элемента a по модулю p.

Другой пример — тривиальный мультипликативный характер, определенный соотношением $\varepsilon(a) = 1$ для всех $a \in F_p^*$.

Часто бывает полезным расширить область определения мультипликативного характера до всего поля F_p. Если $\chi \neq \varepsilon$, то мы полагаем по определению $\chi(0) = 0$. Для ε мы полагаем $\varepsilon(0) = 1$. Польза этих определений обнаружится позднее.

Предложение 8.1.1. *Пусть* χ *— некоторый мультипликативный характер и* $a \in F_p^*$. *Тогда*

(a) $\chi(1) = 1$;

(b) $\chi(a)$ *— корень степени* $p - 1$ *из единицы;*

(c) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

[*В п.* (a) 1 *в левой части есть единичный элемент поля* F_p, *в то время как* 1 *в правой части — это комплексное число* 1. *Черта в п.* (c) *означает комплексное сопряжение.*]

Доказательство. Имеем $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$. Таким образом, $\chi(1) = 1$, так как $\chi(1) \neq 0$.

Для доказательства п. (b) заметим, что если $a^{p-1} = 1$, то $1 = \chi(1) = \chi(a^{p-1}) = \chi(a)^{p-1}$.

Для доказательства п. (c) заметим, что $1 = \chi(1) = \chi(a^{-1}a) = \chi(a^{-1})\chi(a)$. Это показывает, что $\chi(a^{-1}) = \chi(a)^{-1}$. Равенство $\chi(a)^{-1} = \overline{\chi(a)}$ следует из того факта, что $\chi(a)$ — комплексное число с абсолютным значением 1 в силу (b). □

Предложение 8.1.2. *Пусть* χ — *мультипликативный характер. Если* $\chi \neq \varepsilon$, *то* $\sum_t \chi(t) = 0$, *где сумма берется по всем* $t \in F_p$. *Если* $\chi = \varepsilon$, *то значение этой суммы есть* p.

Доказательство. Последнее утверждение очевидно, а поэтому можно считать, что $\chi \neq \varepsilon$. В этом случае существует такое $a \in F_p^*$, что $\chi(a) \neq 1$. Пусть $T = \sum_t \chi(t)$. Тогда

$$\chi(a)T = \sum_t \chi(\alpha)\chi(t) = \sum_t \chi(at) = T.$$

Последнее равенство получается из того, что когда t пробегает все элементы поля F_p, at также пробегает все элементы этого поля. Так как $\chi(a) \neq 1$ и $\chi(a)T = T$, то $T = 0$. □

С помощью следующих определений на множестве мультипликативных характеров можно ввести структуру группы. В дальнейшем будем опускать слово *мультипликативный*.

(1) Если χ и λ — характеры, то $\chi\lambda$ есть отображение, которое переводит $a \in F_p^*$ в $\chi(a)\lambda(a)$.

(2) Если χ — характер, то χ^{-1} есть отображение, которое переводит $a \in F_p^*$ в $\chi(a)^{-1}$.

Мы предоставляем читателю проверку того, что $\chi\lambda$ и χ^{-1} — характеры и что эти определения превращают множество характеров в группу. Единицей этой группы будет, конечно, характер ε.

Предложение 8.1.3. *Группа характеров является циклической группой порядка* $p - 1$. *Если* $a \in F_p^*$ *и* $a \neq 1$, *то существует такой характер* χ, *что* $\chi(a) \neq 1$.

Доказательство. Мы знаем, что группа F_p^* циклическая (см. теорему 1 гл. 4). Пусть $g \in F_p^*$ — образующий элемент. Тогда каждый элемент $a \in F_p^*$ будет степенью g. Если $a = g^l$ и χ — характер, то $\chi(a) = \chi(g)^l$. Это показывает, что χ полностью определяется значением $\chi(g)$. Так как $\chi(g)$ есть корень степени $p-1$ из единицы и так как их имеется точно $p-1$, отсюда следует, что группа характеров имеет порядок не больше $p-1$.

Определим теперь функцию λ равенством $\lambda(g^k) = e^{2\pi i (k/(p-1))}$. Нетрудно проверить, что λ определена корректно и является характером. Мы утверждаем, что $p-1$ — наименьшее целое число n со свойством $\lambda^n = \varepsilon$. Если $\lambda^n = \varepsilon$, то $\lambda^n(g) = \varepsilon(g) = 1$. Но $\lambda^n(g) = \lambda(g)^n = e^{2\pi i (n/(p-1))}$. Отсюда следует, что $p-1$ делит n. Так как $\lambda^{p-1}(a) = \lambda(a)^{p-1} = \lambda(a^{p-1}) = \lambda(1) = 1$, то $\lambda^{p-1} = \varepsilon$. Мы получили, что характеры $\varepsilon, \lambda, \lambda^2, \ldots, \lambda^{p-2}$ все различны. Так как по первой части доказательства имеется не более $p-1$ характеров, мы получили, что существует точно $p-1$ характеров и что эта группа циклическая с λ в качестве образующего.

Если $a \in F_p^*$ и $a \neq 1$, то $a = g^l$, где $p-1 \nmid l$. Вычислим $\lambda(a)$. Имеем $\lambda(a) = \lambda(g)^l = e^{2\pi i (l/(p-1))} \neq 1$. Это завершает доказательство. □

Следствие. *Если $a \in F_p^*$ и $a \neq 1$, то $\sum_{\chi} \chi(a) = 0$, где суммирование проводится по всем характерам.*

Доказательство. Пусть $S = \sum_{\chi} \chi(a)$. Так как $a \neq 1$, то существует, согласно предложению 8.1.3, характер λ, для которого $\lambda(a) \neq 1$. Тогда

$$\lambda(a) S = \sum_{\chi} \lambda(a)\chi(a) = \sum_{\chi} \lambda\chi(a) = S.$$

Последнее равенство выполняется потому, что когда χ пробегает все характеры поля F_p, то и $\lambda\chi$ пробегает все эти характеры. Отсюда вытекает, что $(\lambda(a) - 1) S = 0$ и, следовательно, $S = 0$. □

Характеры полезны при изучении уравнений. Для иллюстрации этого утверждения рассмотрим уравнение $x^n = a$ для $a \in F_p^*$. В силу предложения 4.2.1 мы знаем, что решения существуют тогда и только тогда, когда $a^{(p-1)/d} = 1$, где $d = (n, p-1)$, и что если какое-то решение существует, то имеется точно d решений. Для простоты мы предположим, что n делит $p-1$. В этом случае $d = (n, p-1) = n$.

Мы выведем теперь критерий разрешимости уравнения $x^n = a$, используя характеры.

Предложение 8.1.4. *Если $a \in F_p^*$, $n \mid p-1$ и $x^n = a$ не разрешимо, то существует такой характер χ, что*
(a) $\chi^n = \varepsilon$;
(b) $\chi(a) \neq 1$.

Доказательство. Пусть g и λ такие же, как в предложении 8.1.3, и положим $\chi = \lambda^{(p-1)/n}$. Тогда $\chi(g) = \lambda^{(p-1)/n}(g) = \lambda(g)^{(p-1)/n} = e^{2\pi i/n}$. Далее, $a = g^l$ при некотором l, а так как $x^n = a$ не разрешимо, то $n \nmid l$. Имеем $\chi(a) = \chi(g)^l = e^{2\pi i(l/n)} \neq 1$. Наконец, $\chi^n = \lambda^{p-1} = \varepsilon$. □

Для $a \in F_p$ пусть $N(x^n = a)$ обозначает число решений уравнения $x^n = a$. Если $n \mid p-1$, то справедливо следующее

Предложение 8.1.5. $N(x^n = a) = \sum_{\chi^n = \varepsilon} \chi(a)$, *где сумма берется по всем характерам, порядок которых делит n.*

Доказательство. Мы утверждаем, прежде всего, что существует точно n характеров, порядок которых делит n. Так как значение $\chi(g)$ такого характера должно быть корнем степени n из единицы, то существует, самое большее, n таких характеров. В предложении 8.1.4 мы нашли характер χ, для которого $\chi(g) = e^{2\pi i/n}$. Отсюда следует, что $\varepsilon, \chi, \chi^2, \ldots, \chi^{n-1}$ суть n различных характеров, порядок которых делит n.

Для доказательства нашей формулы заметим, что $x^n = 0$ имеет одно решение, а именно $x = 0$. Далее, $\sum_{\chi^n = \varepsilon} \chi(0) = 1$, так как $\varepsilon(0) = 1$ и $\chi(0) = 0$ для $\chi \neq \varepsilon$.

Предположим теперь, что $a \neq 0$ и что $x^n = a$ разрешимо, т. е. существует такой элемент b, что $b^n = a$. Если $\chi^n = \varepsilon$, то $\chi(a) = \chi(b^n) = \chi(b)^n = \chi^n(b) = \varepsilon(b) = 1$. Таким образом, $\sum_{\chi^n = \varepsilon} \chi(a) = n$, а это и есть $N(x^n = a)$ в данном случае.

Наконец, предположим, что $a \neq 0$ и что $x^n = a$ неразрешимо. Мы должны показать, что $\sum_{\chi^n = \varepsilon} \chi(a) = 0$. Обозначим эту сумму через T. В силу предложения 8.1.4 существует такой характер ρ, что $\rho(a) \neq 1$ и $\rho^n = \varepsilon$. Простое вычисление показывает, что $\rho(a)\, T = T$ (используется очевидный факт, что характеры порядка, делящего n, образуют группу). Таким образом, $(\rho(a) - 1)\, T = 0$ и $T = 0$, что и требовалось. □

Рассмотрим частный случай, когда p нечетно и $n = 2$. Тогда предложение 8.1.5 утверждает, что $N(x^2 = a) = 1 + (a/p)$, где (a/p) — символ Лежандра. Это равенство нетрудно проверить и непосредственно.

Мы возвратимся к уравнениям над полем F_p в § 3.

§ 2. Суммы Гаусса

Квадратичные суммы Гаусса были введены в гл. 6. Следующее определение обобщает это понятие.

Определение. Пусть χ — некоторый характер поля F_p и $a \in F_p$. Положим

$$g_a(\chi) = \sum_t \chi(t)\,\zeta^{at},$$

где сумма берется по всем $t \in F_p$ и $\zeta = e^{2\pi i/p}$. Тогда $g_a(\chi)$ называется *суммой Гаусса* поля F_p, соответствующей характеру χ.

Предложение 8.2.1. *Если* $a \neq 0$ *и* $\chi \neq \varepsilon$, *то* $g_a(\chi) = \chi(a^{-1}) \cdot g_1(\chi)$. *Если* $a \neq 0$ *и* $\chi = \varepsilon$, *то* $g_a(\varepsilon) = 0$. *Если* $a = 0$ *и* $\chi \neq \varepsilon$, *то* $g_0(\chi) = 0$. *Если* $a = 0$ *и* $\chi = \varepsilon$, *то* $g_0(\varepsilon) = p$.

Доказательство. Предположим, что $a \neq \varepsilon$ и $\chi \neq \varepsilon$. Тогда

$$\chi(a)\,g_a(\chi) = \chi(a) \sum_t \chi(t)\,\zeta^{at} = \sum_t \chi(at)\,\zeta^{at} = g_1(\chi).$$

Это доказывает первое утверждение.

Если $a \neq 0$, то

$$g_a(\varepsilon) = \sum_t \varepsilon(t)\,\zeta^{at} = \sum_t \zeta^{at} = 0.$$

Мы здесь воспользовались леммой 1 из гл. 6.

Для завершения доказательства заметим, что

$$g_0(\chi) = \sum_t \chi(t)\,\zeta^{0t} = \sum_t \chi(t).$$

Если $\chi = \varepsilon$, то результат равен p; если $\chi \neq \varepsilon$, то результат равен нулю, согласно предложению 8.1.2. □

В дальнейшем мы будем обозначать $g_1(\chi)$ через $g(\chi)$. Мы хотим определить абсолютное значение для $g(\chi)$. Это очень просто сделать, следуя доказательству предложения 6.3.2.

Предложение 8.2.2. *Если* $\chi \neq \varepsilon$, *то* $|g(\chi)| = \sqrt{p}$.

Доказательство. Идея состоит в вычислении суммы $\sum_a g_a(\chi) \cdot \overline{g_a(\chi)}$ двумя способами.

Если $a \neq 0$, то, согласно предложению 8.2.1, $\overline{g_a(\chi)} = \overline{\chi(a^{-1})g(\chi)} = \chi(a)\,\overline{g(\chi)}$ и $g_a(\chi) = \chi(a^{-1})\,g(\chi)$. Таким образом,

$$g_a(\chi)\,\overline{g_a(\chi)} = \chi(a^{-1})\,\chi(a)\,g(\chi)\,\overline{g(\chi)} = |g(\chi)|^2.$$

Так как $g_0(\chi) = 0$, то наша сумма имеет значение $(p-1)\,|g(\chi)|^2$.

С другой стороны,

$$g_a(\chi)\,\overline{g_a(\chi)} = \sum_x \sum_y \chi(x)\,\overline{\chi(y)}\,\zeta^{ax-ay}.$$

Беря сумму обеих частей по a и используя следствие леммы 1 из гл. 6, получаем

$$\sum_a g_a(\chi)\,\overline{g_a(\chi)} = \sum_x \sum_y \chi(x)\,\overline{\chi}(y)\,\delta(x, y)\,p = (p-1)\,p.$$

Таким образом, $(p-1)\,|g(\chi)|^2 = (p-1)\,p$, откуда и следует доказываемый результат. □

Связь полученного результата с предложением 6.3.2 становится более ясной после следующего рассмотрения.

Как связаны между собой $\overline{g(\chi)}$ и $g(\bar{\chi})$ ($\bar{\chi}$ — характер, ставящий в соответствие a значение $\overline{\chi(a)}$, т. е. он совпадает с характером χ^{-1})? Имеем

$$\overline{g(\chi)} = \sum_t \overline{\chi(t)}\,\zeta^{-t} = \chi(-1)\sum_t \overline{\chi(-t)}\,\zeta^{-t} = \chi(-1)\,g(\bar{\chi}).$$

Мы воспользовались тем, что $\overline{\chi(-1)} = \chi(-1)$; это очевидно, ибо $\chi(-1) = \pm 1$. Следовательно, равенство $|g(\chi)|^2 = p$ может быть записано в виде $g(\chi)\,g(\bar{\chi}) = \chi(-1)\,p$. Если χ — символ Лежандра, то это соотношение есть в точности результат из предложения 6.3.2.

§ 3. Суммы Якоби

Рассмотрим уравнение $x^2 + y^2 = 1$ над полем F_p. Так как это поле конечно, наше уравнение имеет лишь конечное число решений. Пусть $N(x^2 + y^2 = 1)$ — это число. Мы хотим определить его явно.

Заметим, что

$$N(x^2 + y^2 = 1) = \sum_{a+b=1} N(x^2 = a)\,N(y^2 = b),$$

где сумма берется по всем парам $a,\ b \in F_p$ с $a + b = 1$. Так как $N(x^2 = a) = 1 + (a/p)$, то подставляя это значение, получаем, что

$$N(x^2 + y^2 = 1) = p + \sum_a \left(\frac{a}{p}\right) + \sum_b \left(\frac{b}{p}\right) + \sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Первые две суммы равны нулю, так что все сводится к вычислению последней суммы. Как мы вскоре убедимся, она равна $-(-1)^{(p-1)/2}$. Следовательно, $N(x^2 + y^2 = 1)$ равно $p - 1$, если $p \equiv 1$ (4) и $p + 1$ при $p \equiv 3$ (4). Читателю предлагается непосредственно проверить этот результат для нескольких первых простых чисел.

Продвигаясь далее, попытаемся вычислить $N(x^3 + y^3 = 1)$. Как и прежде,

$$N(x^3 + y^3 = 1) = \sum_{a+b=1} N(x^3 = a) N(y^3 = b).$$

Если $p \equiv 2$ (3), то $N(x^3 = a) = 1$ для всех a, так как $(3, p - 1) = 1$. Отсюда следует, что в этом случае $N(x^3 + y^3 = 1) = p$. Предположим теперь, что $p \equiv 1$ (3). Пусть $\chi \neq \varepsilon$ — некоторый характер порядка 3. Тогда χ^2 — характер порядка 3 и $\chi^2 \neq \varepsilon$. Следовательно, ε, χ и χ^2 — все характеры порядка 3, называемые поэтому *кубическими характерами*. Согласно предложению 8.1.5, $N(x^3 = a) = 1 + \chi(a) + \chi^2(a)$. Значит,

$$N(x^3 + y^3 = 1) = \sum_{a+b=1} \sum_{i=0}^{2} \chi^i(a) \sum_{j=0}^{2} \chi^j(b) =$$
$$= \sum_i \sum_j \left(\sum_{a+b=1} \chi^i(a) \chi^j(b) \right).$$

Внутренняя сумма подобна той, которая появилась при анализе $N(x^2 + y^2 = 1)$.

Определение. Пусть χ и λ — некоторые характеры поля F_p и

$$J(\chi, \lambda) = \sum_{a+b=1} \chi(a) \lambda(b).$$

$J(\chi, \lambda)$ называется *суммой Якоби*.

Чтобы завершить вычисление $N(x^2 + y^2 = 1)$ и $N(x^3 + y^3 = 1)$, нам следует получить информацию о значениях сумм Якоби. Следующая теорема не только доставляет эту информацию, но и показывает удивительную связь между суммами Якоби и Гаусса.

Теорема 1. *Пусть χ и λ — нетривиальные характеры. Тогда*

(a) $J(\varepsilon, \varepsilon) = p$;
(b) $J(\varepsilon, \chi) = 0$;
(c) $J(\chi, \chi^{-1}) = -\chi(-1)$;
(d) *если* $\chi\lambda \neq \varepsilon$, *то*

$$J(\chi, \lambda) = \frac{g(\chi) g(\lambda)}{g(\chi\lambda)}.$$

Доказательство. Пункт (a) очевиден; п. (b) — непосредственное следствие предложения 8.1.2.

Для доказательства (c) заметим, что

$$J(\chi, \chi^{-1}) = \sum_{a+b=1} \chi(a)\chi^{-1}(b) = \sum_{\substack{a+b=1 \\ b\neq 0}} \chi\left(\frac{a}{b}\right) = \sum_{a\neq 1} \chi\left(\frac{a}{1-a}\right).$$

Положим $a/(1-a) = c$. Если $c \neq -1$, то $a = c/(1+c)$. Отсюда следует, что в то время, как a пробегает поле F_p за исключением 1, c пробегает F_p, за исключением -1. Следовательно,

$$J(\chi, \chi^{-1}) = \sum_{c\neq -1} \chi(c) = -\chi(-1).$$

Для доказательства п. (d) заметим, что

$$g(\chi)g(\lambda) = \left(\sum_x \chi(x)\zeta^x\right)\left(\sum_y \lambda(y)\zeta^y\right) =$$

$$= \sum_{x,\,y} \chi(x)\lambda(y)\zeta^{x+y} = \sum_t \left(\sum_{x+y=t} \chi(x)\lambda(y)\right)\zeta^t. \qquad (1)$$

Если $t = 0$, то

$$\sum_{x+y=0} \chi(x)\lambda(y) = \sum_x \chi(x)\lambda(-x) = \lambda(-1)\sum_x \chi\lambda(x) = 0,$$

ибо $\chi\lambda \neq \varepsilon$ по предположению.

Если $t \neq 0$, определим x' и y' посредством формул $x = tx'$, $y = ty'$. Если $x + y = t$, то $x' + y' = 1$. Отсюда следует, что

$$\sum_{x+y=t} \chi(x)\lambda(y) = \sum_{x'+y'=1} \chi(tx')\lambda(ty') = \chi\lambda(t)J(\chi, \lambda).$$

Подставляя это в равенство (1), получаем

$$g(\chi)g(\lambda) = \sum_t \chi\lambda(t)J(\chi, \lambda)\zeta^t = J(\chi, \lambda)g(\chi\lambda). \qquad \square$$

Следствие. *Если* χ, λ *и* $\chi\lambda$ *не равны* ε, *то* $|J(\chi, \lambda)| = \sqrt{p}$.

Доказательство. Следует взять абсолютное значение обеих частей равенства в п. (d) и воспользоваться предложением 8.2.2. $\square$

Мы возвратимся теперь к анализу величин $N(x^2 + y^2 = 1)$ и $N(x^3 + y^3 = 1)$. В первом случае необходимо было вычислить сумму $\sum_{a+b=1} (a/p)(b/p)$. Применим случай (c) теоремы 1, который приводит к результату $-(-1)^{(p-1)/2}$, что и утверждалось ранее.

В случае величин $N(x^3 + y^3 = 1)$ мы должны вычислить суммы $\sum_{a+b=1} \chi^i(a)\chi^i(b)$, где χ — кубический характер.

Применение теоремы 1 приводит к равенству

$$N(x^3 + y^3 = 1) = p - \chi(-1) - \chi^2(-1) + J(\chi, \chi) + J(\chi^2, \chi^2).$$

Так как $-1 = (-1)^3$, то $\chi(-1) = \chi^3(-1) = 1$. Заметим также, что $\chi^2 = \chi^{-1} = \bar{\chi}$. Таким образом,

$$N(x^3 + y^3 = 1) = p - 2 + 2\mathrm{Re}\, J(\chi, \chi).$$

Этот результат не так приятен, как результат для $N(x^2 + y^2 = 1)$, поскольку мы не знаем явной формулы для $J(\chi, \chi)$. Тем не менее в силу следствия теоремы 1 $|J(\chi, \chi)| = \sqrt{p}$, так что мы получаем оценку

$$|N(x^3 + y^3 = 1) - p + 2| \leqslant 2\sqrt{p}.$$

Если обозначить через N_p число решений уравнения $x^3 + y^3 = 1$ в поле F_p, то эта оценка говорит, что N_p приблизительно равно $p - 2$ с «поправочным членом» $2\sqrt{p}$. Это показывает, что для больших простых чисел p всегда существует много решений.

Если $p \equiv 1$ (3), то всегда имеется по крайней мере шесть решений, ибо каждое из уравнений $x^3 = 1$ и $y^3 = 1$ имеет три решения и можно записать $1 + 0 = 1$ и $0 + 1 = 1$. Для $p = 7$ и $p = 13$ других решений не будет. Для $p = 19$ существуют другие решения, например $3^3 + 10^3 \equiv 1$ (19). Эти «нетривиальные» решения существуют для всех простых чисел $p \geqslant 19$, ибо из приведенной оценки следует, что $N_p \geqslant p - 2 - 2\sqrt{p} > 6$ для $p \geqslant 19$.

Используя символ Якоби, мы могли бы легко распространить наши рассуждения на уравнения вида $ax^n + by^n = 1$, но мы не будем сейчас углубляться в эту задачу.

Следствие теоремы 1 приводит к двум выводам, представляющим значительный интерес.

Предложение 8.3.1. *Если* $p \equiv 1$ (4), *то существуют такие целые числа* a *и* b, *что* $a^2 + b^2 = p$.

Если $p \equiv 1$ (3), *то существуют такие целые числа* a *и* b, *что* $a^2 - ab + b^2 = p$.

Доказательство. Если $p \equiv 1$ (4), то существует характер χ порядка 4 (если λ имеет порядок $p - 1$, пусть $\chi = \lambda^{(p-1)/4}$). Значения χ лежат в множестве $\{1, -1, i, -i\}$, где $i = \sqrt{-1}$. Таким образом, $J(\chi, \chi) = \sum_{s+t=1} \chi(s)\chi(t) \in \mathbf{Z}[i]$ (см. гл. 1, § 4). Отсюда следует, что $J(\chi, \chi) = a + bi$, где $a, b \in \mathbf{Z}$, а значит, $p = |J(\chi, \chi)|^2 = a^2 + b^2$.

Если $p \equiv 1$ (3), то существует характер χ порядка 3. Значения χ лежат в множестве $\{1, \omega, \omega^2\}$, где $\omega = e^{2\pi i/3} = (-1 + \sqrt{-3})/2$. Таким образом, $J(\chi, \chi) \in \mathbf{Z}[\omega]$. Как и выше, $J(\chi, \chi) = a + b\omega$, где $a, b \in \mathbf{Z}$ и $p = |J(\chi, \chi)|^2 = |a + b\omega|^2 = a^2 - ab + b^2$. □

Тот факт, что простые числа $p \equiv 1$ (4) могут быть записаны в виде суммы двух квадратов, был открыт Ферма. Нетрудно доказать, что если $a, b > 0$, a нечетно и b четно, то представление $p = a^2 + b^2$ единственно.

Если $p \equiv 1$ (3), представление $p = a^2 - ab + b^2$ не единственно, даже если предположить, что $a, b > 0$. Это видно из равенств

$$a^2 - ab + b^2 = (b - a)^2 - (b - a)\, b + b^2 = \\ = a^2 - a\,(a - b) + (a - b)^2.$$

Однако можно переформулировать утверждение так, что представление станет единственным. Если $p = a^2 - ab + b^2$, то

$$4p = (2a - b)^2 + 3b^2 = (2b - a)^2 + 3a^2 = \\ = (a + b)^2 + 3\,(a - b)^2.$$

Мы утверждаем, что 3 делит a, b или $a - b$. Предположим, что $3 \nmid a$ и $3 \nmid b$. Если $a \equiv 1$ (3) и $b \equiv 2$ (3) или $a \equiv 2$ (3) и $b \equiv 1$ (3), то $a^2 - ab + b^2 \equiv 0$ (3), а это означает, что $3 \mid p$ — противоречие. Следовательно, $3 \mid a - b$ и имеет место

Предложение 8.3.2. *Если $p \equiv 1$ (3), то существуют такие целые числа A и B, что $4p = A^2 + 27B^2$. В этом представлении числа $4p$ целые A и B определены однозначно (с точностью до знака).*

Доказательство. Доказательство однозначности мы относим в упражнения (см. упр. 13). □

Теорема 1 вместе с одним простым рассуждением приводит к еще одному интересному соотношению между суммами Гаусса и Якоби.

Предложение 8.3.3. *Предположим, что $p \equiv 1$ (n) и что χ — некоторый характер порядка n. Тогда*

$$g(\chi)^n = \chi(-1)\, pJ(\chi, \chi)\, J(\chi, \chi^2) \ldots J(\chi, \chi^{n-2}).$$

Доказательство. В силу п. (d) теоремы 1 имеем $g(\chi)^2 = J(\chi, \chi)\, g(\chi^2)$. Умножая обе части на $g(\chi)$, получаем $g(\chi)^3 = J(\chi, \chi)\, J(\chi, \chi^2)\, g(\chi^3)$. Продолжая таким же образом, приходим к равенству

$$g(\chi)^{n-1} = J(\chi, \chi)\, J(\chi, \chi^2) \ldots J(\chi, \chi^{n-2})\, g(\chi^{n-1}). \qquad (2)$$

Далее, $\chi^{n-1} = \chi^{-1} = \bar{\chi}$. Следовательно, как мы видели, $g(\chi)\, g(\chi^{n-1}) = g(\chi)\, g(\bar{\chi}) = \chi(-1)\, p$. Доказываемый результат получается теперь умножением обеих частей равенства (2) на $g(\chi)$. □

Следствие. *Если* χ *— кубический характер, то*

$$g(\chi)^3 = pJ(\chi, \chi).$$

Доказательство. Это просто частный случай предложения 8.3.3, надо лишь учесть, что $\chi(-1) = \chi((-1)^3) = 1$. □

С помощью этого следствия мы можем более полно проанализировать комплексное число $J(\chi, \chi)$, появившееся при вычислении $N(x^3 + y^3 = 1)$. Мы видели, что $J(\chi, \chi) = a + b\omega$, где a, $b \in \mathbf{Z}$ и $\omega = e^{2\pi i/3} = (-1 + \sqrt{-3})/2$.

Предложение 8.3.4. *Предположим, что* $p \equiv 1$ (3) *и что* χ *— кубический характер. Положим* $J(\chi, \chi) = a + b\omega$, *как и выше. Тогда*

(a) $b \equiv 0$ (3);

(b) $a \equiv -1$ (3).

Доказательство. Мы будем работать со сравнениями в кольце целых алгебраических чисел, как в гл. 6:

$$g(\chi)^3 = \Big(\sum_t \chi(t)\zeta^t\Big)^3 \equiv \sum_t \chi(t)^3 \zeta^{3t} \ (3).$$

Так как $\chi(0) = 0$ и $\chi(t)^3 = 1$ для $t \neq 0$, то $\sum\limits_t \chi(t)^3 \zeta^{3t} = \sum\limits_{t \neq 0} \zeta^{3t} = -1$. Следовательно,

$$g(\chi)^3 = pJ(\chi, \chi) \equiv a + b\omega \equiv -1 \ (3).$$

Подставляя $\bar{\chi}$ вместо χ и вспоминая, что $\overline{g(\chi)} = g(\bar{\chi})$, мы получаем

$$g(\bar{\chi})^3 = pJ(\bar{\chi}, \bar{\chi}) \equiv a + b\bar{\omega} \equiv -1 \ (3).$$

Вычитание дает $b(\omega - \bar{\omega}) \equiv 0$ (3), или $b\sqrt{-3} \equiv 0$ (3). Таким образом, $-3b^2 \equiv 0$ (9), откуда $3 \mid b$. Так как $3 \mid b$ и $a + b\omega \equiv -1$ (3), то должно быть справедливым сравнение $a \equiv -1$ (3), что и завершает доказательство. □

Следствие. *Пусть* $A = 2a - b$ *и* $B = b/3$. *Тогда* $A \equiv 1$ (3) *и*

$$4p = A^2 + 27B^2.$$

Доказательство. Так как $J(\chi, \chi) = a + b\omega$ и $|J(\chi, \chi)|^2 = p$, то $p = a^2 - ab + b^2$. Следовательно, $4p = (2a - b)^2 + 3b^2$ и $4p = A^2 + 27B^2$.

Согласно предложению 8.3.4, $3 \mid b$ и $a \equiv -1$ (3). Поэтому $A = 2a - b \equiv 1$ (3). □

Теперь мы можем доказать следующую красивую теорему, принадлежащую Гауссу.

Теорема 2. *Предположим, что* $p \equiv 1$ (3). *Тогда существуют такие целые числа* A *и* B, *что* $4p = A^2 + 27B^2$. *Если потребовать, чтобы* $A \equiv 1$ (3), *то* A *будет определено однозначно, и*

$$N(x^3 + y^3 = 1) = p - 2 + A.$$

Доказательство. Мы уже показали, что $N(x^3 + y^3 = 1) = p - 2 + 2\mathrm{Re}\, J(\chi, \chi)$. Так как $J(\chi, \chi) = a + b\omega$, как и выше, то $\mathrm{Re}\, J(\chi, \chi) = (2a - b)/2$. Следовательно, $2\mathrm{Re}\, J(\chi, \chi) = 2a - b = A \equiv 1$ (3). Доказательство однозначности предоставляется провести в качестве упражнения. □

Проиллюстрируем этот результат двумя примерами: $p = 61$ и $p = 67$.

Имеем $4 \cdot 61 = 1^2 + 27 \cdot 3^2$. Следовательно, число решений уравнения $x^3 + y^3 = 1$ в F_{61} равно $61 - 2 + 1 = 60$.

Далее, $4 \cdot 67 = 5^2 + 27 \cdot 3^2$. Мы должны быть здесь осторожными; так как $5 \not\equiv 1$ (3), то следует выбрать $A = -5$. Ответом, следовательно, будет $67 - 2 - 5 = 60$, что совпадает (случайно?) с числом решений в первом случае.

§ 4. Уравнение $x^n + y^n = 1$ в F_p

Мы будем предполагать, что $p \equiv 1$ (n). Исследуем число решений уравнения $x^n + y^n = 1$ в поле F_p. Метод § 3 непосредственно применим и здесь.

Имеем

$$N(x^n + y^n = 1) = \sum_{a+b=1} N(x^n = a)\, N(y^n = b).$$

Пусть χ — некоторый характер порядка n. Согласно предложению 8.1.5,

$$N(x^n = a) = \sum_{i=0}^{n-1} \chi^i(a).$$

Объединяя эти два результата, получаем

$$N(x^n + y^n = 1) = \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} J(\chi^j, \chi^i).$$

Для оценки этой суммы может быть использована теорема 1. Если $i = j = 0$, то $J(\chi^0, \chi^0) = J(\varepsilon, \varepsilon) = p$. Если $i + j = n$, то $\chi^i = (\chi^j)^{-1}$, так что $J(\chi^j, \chi^i) = -\chi^j(-1)$. Сумма этих членов равна $-\sum_{j=1}^{n-1} \chi^j(-1)$, причем $\sum_{j=0}^{n-1} \chi^j(-1)$ равна n, если -1 является n-й степенью, и нулю в противном случае. Таким образом, вклад

этих членов есть $1 - \delta_n(-1)\,n$, где $\delta_n(-1)$ имеет очевидное значение. Наконец, если $i = 0$ и $j \neq 0$ или $i \neq 0$ и $j = 0$, то $J(\chi^i, \chi^j) = 0$. Следовательно,

$$N(x^n + y^n = 1) = p + 1 - \delta_n(-1)\,n + \sum_{i,\ j} J(\chi^i, \chi^j).$$

Сумма берется по индексам i и j между 1 и $n-1$, таким, что $i + j \neq n$. Таких членов будет $(n-1)^2 - (n-1) = (n-1)(n-2)$, и все они имеют абсолютное значение $\sqrt{p}$. Таким образом, справедливо

Предложение 8.4.1.

$$|N(x^n + y^n = 1) + \delta_n(-1)\,n - (p+1)| \leqslant (n-1)(n-2)\sqrt{p}.$$

Член $\delta_n(-1)\,n$ будет позднее интерпретироваться как число точек «на бесконечности» на кривой $x^n + y^n = 1$.

Полученная оценка показывает, что для больших p существует много нетривиальных решений.

§ 5. Дальнейшие результаты о суммах Якоби

Теорему 1 можно обобщить в одном очень плодотворном направлении. Нам понадобится следующее определение.

Определение. Пусть $\chi_1, \chi_2, \ldots, \chi_l$ — характеры поля F_p. *Сумма Якоби* определяется по формуле

$$J(\chi_1, \chi_2 \ldots, \chi_l) = \sum_{t_1 + \cdots + t_l = 1} \chi_1(t_1)\,\chi_2(t_2) \cdots \chi_l(t_l).$$

Заметим, что при $l = 2$ это превращается в наше первое определение суммы Якоби.

Полезно определить другую сумму, которая останется безымянной:

$$J_0(\chi_1, \ldots, \chi_l) = \sum_{t_1 + \cdots + t_l = 0} \chi_1(t_1)\,\chi_2(t_2) \cdots \chi_l(t_l).$$

Предложение 8.5.1. (a) $J_0(\varepsilon, \varepsilon, \ldots, \varepsilon) = J(\varepsilon, \varepsilon, \ldots, \varepsilon) = p^{l-1}$.

(b) *Если некоторые, но не все, из* χ_i *тривиальны, то* $J_0(\chi_1, \chi_2, \ldots, \chi_l) = J(\chi_1, \chi_2, \ldots, \chi_l) = 0$.

(c) *Предположим, что* $\chi_l \neq \varepsilon$. *Тогда*

$$J_0(\chi_1, \chi_2, \ldots, \chi_l) = \begin{cases} 0, & \text{если } \chi_1\chi_2 \ldots \chi_l \neq \varepsilon, \\ \chi_l(-1)(p-1)\,J(\chi_1, \chi_2, \ldots, \chi_{l-1}) & \text{в противном случае.} \end{cases}$$

Доказательство. Если $t_1, t_2, \ldots, t_{l-1}$ выбраны (произвольным образом) в F_p, то t_l однозначно определяется условием $t_1 + t_2 + \ldots + t_{l-1} + t_l = 0$. Следовательно, $J_0(\varepsilon, \varepsilon, \ldots, \varepsilon) = p^{l-1}$. Аналогично определяется $J(\varepsilon, \varepsilon, \ldots, \varepsilon)$.

Для доказательства п. (b) предположим, что $\chi_1, \chi_2, \ldots, \chi_s$ нетривиальны и что $\chi_{s+1} = \chi_{s+2} = \ldots = \chi_l = \varepsilon$. Тогда

$$\sum_{t_1+\cdots+t_l=0} \chi_1(t_1)\chi_2(t_2)\ldots\chi_l(t_l) = \sum_{t_1, t_2, \ldots, t_{l-1}} \chi_1(t_1)\chi_2(t_2)\ldots\chi_s(t_s) =$$

$$= p^{l-s-1}\Big(\sum_{t_1}\chi_1(t_1)\Big)\Big(\sum_{t_2}\chi_2(t_2)\Big)\ldots\Big(\sum_{t_s}\chi_s(t_s)\Big) = 0.$$

Мы воспользовались предложением 8.1.2. Значит, $J_0(\chi_1, \chi_2, \ldots, \chi_l) = 0$. Аналогичные рассуждения надо провести для $J(\chi_1, \ldots, \chi_l)$.

Для доказательства п. (c) заметим, что

$$J_0(\chi_1, \chi_2, \ldots, \chi_l) = \sum_s \Big(\sum_{t_1+\cdots+t_{l-1}=-s} \chi_1(t_1)\ldots\chi_{l-1}(t_{l-1})\Big)\chi_l(s).$$

Так как $\chi_l \neq \varepsilon$, то $\chi_l(0) = 0$, так что можно считать, что в предыдущей сумме $s \neq 0$. Если $s \neq 0$, то определим t_i' равенством $t_i = -st_i'$. Тогда

$$\sum_{t_1+\cdots+t_{l-1}=-s} \chi_1(t_1)\ldots\chi_{l-1}(t_{l-1}) =$$

$$= \chi_1\chi_2\ldots\chi_{l-1}(-s) \sum_{t_1'+\cdots+t_{l-1}'=1} \chi_1(t_1')\ldots\chi_{l-1}(t_{l-1}') =$$

$$= \chi_1\chi_2\ldots\chi_{l-1}(-s)\, J(\chi_1, \ldots, \chi_{l-1}).$$

Объединяя полученные результаты, приходим к равенству

$$J_0(\chi_1, \chi_2, \ldots, \chi_l) = \chi_1\chi_2\ldots\chi_{l-1}(-1)\, J(\chi_1, \ldots, \chi_{l-1}) \sum_{s\neq 0} \chi_1\chi_2\ldots\chi_l(s).$$

Отсюда следует основной результат, так как последняя сумма равна нулю, если $\chi_1\chi_2\ldots\chi_l \neq \varepsilon$, и $p-1$, если $\chi_1\chi_2\ldots\chi_l = \varepsilon$. □

Пункты (a) и (b) предложения 8.5.1 обобщают пп. (a) и (b) теоремы 1. Пункт (d) теоремы 1 можно обобщить следующим образом.

Теорема 3. *Предположим, что характеры $\chi_1, \chi_2, \ldots, \chi_r$ нетривиальны и что характер $\chi_1\chi_2\ldots\chi_r$ также нетривиален. Тогда*

$$g(\chi_1)g(\chi_2)\ldots g(\chi_r) = J(\chi_1, \chi_2, \ldots, \chi_r)\, g(\chi_1\chi_2\ldots\chi_r).$$

Доказательство. Пусть функция ψ: $F_p \to \mathbf{C}$ определена равенством $\psi(t) = \zeta^t$. Тогда $\psi(t_1 + t_2) = \psi(t_1)\psi(t_2)$ и $g(\chi) = \sum \chi(t)\psi(t)$. Функция ψ вводится для удобства записи. Имеем

$$g(\chi_1)g(\chi_2)\cdots g(\chi_r) = \Big(\sum_{t_1}\chi_1(t_1)\psi(t_1)\Big)\cdots\Big(\sum_{t_r}\chi_r(t_r)\psi(t_r)\Big) =$$

$$= \sum_s \Big(\sum_{t_1+t_2+\cdots+t_r=s}\chi_1(t_1)\chi_2(t_2)\cdots\chi_r(t_r)\Big)\psi(s).$$

Если $s = 0$, то по п. (c) предложения 8.5.1 и из условия $\chi_1 \ldots \chi_r \neq \varepsilon$ получаем

$$\sum_{t_1+\cdots+t_r=0}\chi_1(t_1)\cdots\chi_r(t_r) = 0.$$

Если $s \neq 0$, то подстановка $t_i = st_i'$ показывает, что

$$\sum_{t_1+\cdots+t_r=s}\chi_1(t_1)\cdots\chi_r(t_r) = \chi_1\chi_2\cdots\chi_r(s)J(\chi_1, \chi_2, \ldots, \chi_r).$$

Собирая эти замечания вместе, приходим к равенствам

$$g(\chi_1)\cdots g(\chi_r) = J(\chi_1, \chi_2, \ldots, \chi_r)\sum_{s\neq 0}\chi_1\chi_2\cdots\chi_r(s)\psi(s) =$$

$$= J(\chi_1, \chi_2, \ldots, \chi_r)g(\chi_1\chi_2\cdots\chi_r). \qquad \square$$

Следствие 1. *Предположим, что характеры* $\chi_1, \chi_2, \ldots, \chi_r$ *нетривиальны, а характер* $\chi_1\chi_2\ldots\chi_r$ *тривиален. Тогда*

$$g(\chi_1)g(\chi_2)\cdots g(\chi_r) = \chi_r(-1)pJ(\chi_1, \chi_2, \ldots, \chi_{r-1}).$$

Доказательство. Имеем $g(\chi_1)g(\chi_2)\ldots g(\chi_{r-1}) = J(\chi_1, \ldots, \chi_{r-1})g(\chi_1\chi_2\ldots\chi_{r-1})$ по теореме 3. Умножим обе части этого равенства на $g(\chi_r)$. Так как $\chi_1\chi_2\ldots\chi_{r-1} = \chi_r^{-1}$, то

$$g(\chi_1\cdots\chi_{r-1})g(\chi_r) = g(\chi_r^{-1})g(\chi_r) = \chi_r(-1)p. \qquad \square$$

Следствие 2. *В условиях следствия* 1

$$J(\chi_1, \ldots, \chi_r) = -\chi_r(-1)J(\chi_1, \chi_2, \ldots, \chi_{r-1}).$$

[*Если* $r = 2$, *то полагаем* $J(\chi_1) = 1$.]

Доказательство. Если $r = 2$, то это утверждение есть п. (c) теоремы 1.

Предположим, что $r > 2$. Используя в доказательстве теоремы 3 предположение о том, что $\chi_1\chi_2\ldots\chi_r = \varepsilon$, получаем

$$g(\chi_1)g(\chi_2)\cdots g(\chi_r) = J_0(\chi_1, \chi_2, \ldots, \chi_r) + J(\chi_1, \ldots, \chi_r)\sum_{s\neq 0}\psi(s).$$

Так как $\sum_s \psi(s) = 0$, то сумма в предыдущем соотношении равна -1. Согласно п. (c) предложения 8.5.1, $J_0(\chi_1, \ldots, \chi_r) = \chi_r(-1)(p-1) J(\chi_1, \ldots, \chi_{r-1})$. Согласно следствию 1,

$$g(\chi_1) \cdots g(\chi_r) = \chi_r(-1)\, pJ(\chi_1, \chi_2, \ldots, \chi_{r-1}).$$

Объединяя эти результаты вместе, завершаем доказательство следствия. □

Теорема 4. *Предположим, что характеры* $\chi_1, \chi_2, \ldots, \chi_r$ *нетривиальны.*

(a) *Если* $\chi_1\chi_2 \ldots \chi_r \neq \varepsilon$, *то*

$$|J(\chi_1, \chi_2, \ldots, \chi_r)| = p^{(r-1)/2}.$$

(b) *Если* $\chi_1\chi_2 \ldots \chi_r = \varepsilon$, *то*

$$|J_0(\chi_1, \chi_2, \ldots, \chi_r)| = (p-1)\, p^{(r/2)-1}$$

и

$$|J(\chi_1, \chi_2, \ldots, \chi_r)| = p^{(r/2)-1}.$$

Доказательство. Если χ нетривиален, то $|g(\chi)| = \sqrt{p}$. Пункт (a) следует непосредственно из теоремы 3.

Пункт (b) аналогичным образом вытекает из п. (c) предложения 8.5.1 и из следствия 2 теоремы 3. □

§ 6. Применения

Ранее в этой главе мы исследовали число решений уравнения $x^2 + y^2 = 1$ в поле F_p. Тот же самый вопрос естественно поставить об уравнении $x_1^2 + x_2^2 + \ldots + x_r^2 = 1$. Ответ может быть получен без труда, если воспользоваться результатами § 5.

Пусть $\chi \neq$ характер порядка 2 ($\chi(a) = (a/p)$ в наших прежних обозначениях). Тогда $N(x^2 = a) = 1 + \chi(a)$. Следовательно,

$$N(x_1^2 + \cdots + x_r^2 = 1) = \sum N(x_1^2 = a_1)\, N(x_2^2 = a_2) \ldots N(x_r^2 = a_r),$$

где сумма берется по всем r-наборам $(a_1, \ldots, a_r)$ с $a_1 + a_2 + \ldots + a_r = 1$. Произведя умножение и воспользовавшись предложением 8.5.1, получаем

$$N(x_1^2 + \cdots + x_r^2 = 1) = p^{r-1} + J(\chi, \chi, \ldots, \chi).$$

Если r нечетно, то $\chi^r = \chi$, а если четно, то $\chi^r = \varepsilon$.

Предположим, что r нечетно. Тогда применима теорема 3 и $J(\chi, \ldots, \chi) = g(\chi)^{r-1}$. Так как $g(\chi)^2 = \chi(-1)\, p$, отсюда следует, что $J(\chi, \ldots, \chi) = \chi(-1)^{(r-1)/2} p^{(r-1)/2}$.

Если r четно, мы, воспользовавшись следствием 2 теоремы 3, находим, что $J(\chi, \chi, \ldots, \chi) = -\chi(-1)^{r/2} p^{(r-2)/2}$. Наконец, вспомним, что $\chi(-1) = (-1)^{(p-1)/2}$. Таким образом, имеет место

Предложение 8.6.1. *Если r нечетно, то*

$$N\left(x_1^2+x_2^2+\cdots+x_r^2=1\right)=p^{r-1}+(-1)^{((r-1)/2)((p-1)/2)}p^{(r-1)/2}.$$

Если r четно, то

$$N\left(x_1^2+x_2^2+\cdots+x_r^2=1\right)=p^{r-1}-(-1)^{(r/2)((p-1)/2)}p^{(r/2)-1}.$$

Наиболее общее уравнение, к которому могут быть применены изложенные методы, имеет вид

$$a_1x_1^{l_1}+a_2x_2^{l_2}+\cdots+a_rx_r^{l_r}=b,$$

где $a_1, \ldots, a_r, b \in F_p^{\times}$ и $l_1, l_2, \ldots, l_r$ — положительные целые числа. Мы возвратимся к этой теме в § 7. Теперь же мы воспользуемся суммами Якоби для получения еще одного доказательства квадратичного закона взаимности.

Пусть q — некоторое нечетное простое число, отличное от p, и χ — характер порядка 2 на F_p. Тогда, согласно следствию 1 теоремы 3,

$$g(\chi)^{q+1}=(-1)^{(p-1)/2}pJ(\chi, \chi, \cdots, \chi),$$

где в сумме Якоби имеется q компонент.

Так как $q+1$ четно, то

$$g(\chi)^{q+1}=\left(g(\chi)^2\right)^{(q+1)/2}=(-1)^{((p-1)/2)((q+1)/2)}p^{(q+1)/2}.$$

Подставляя это значение в предыдущую формулу, получаем

$$(-1)^{((p-1)/2)((q-1)/2)}p^{(q-1)/2}=J(\chi, \chi, \ldots, \chi).$$

Далее, $J(\chi, \chi, \ldots, \chi)=\sum\chi(t_1)\chi(t_2)\ldots\chi(t_q)$, где сумма берется по всем $(t_1, t_2, \ldots, t_q)$, таким, что $t_1+t_2+\ldots+t_q=1$. Если $t=t_1=t_2=\ldots=t_q$, то $t=1/q$ и соответствующий член в сумме имеет значение $\chi(1/q)^q=\chi(q)^{-q}=\chi(q)$. Если не все t_i равны, то имеется q разных q-наборов, получаемых из $(t_1, t_2, \ldots, t_q)$ циклической перестановкой. Все соответствующие члены суммы имеют одинаковое значение. Следовательно,

$$(-1)^{((p-1)/2)((q-1)/2)}p^{(q-1)/2}\equiv\chi(q)\ (q).$$

Так как $\chi(q)=(q/p)$ и $p^{(q-1)/2}\equiv(p/q)\ (q)$, то

$$(-1)^{((p-1)/2)((q-1)/2)}\left(\frac{p}{q}\right)\equiv\left(\frac{q}{p}\right)\ (q),$$

а значит,

$$(-1)^{((p-1)/2)((q-1)/2)}\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right).$$

§ 7. Общая теорема

Все уравнения, рассмотренные нами до сих пор, являются частными случаями уравнения

$$a_1 x_1^{l_1} + a_2 x_2^{l_2} + \cdots + a_r x_r^{l_r} = b, \tag{3}$$

где $a_1, a_2, \ldots, a_r \in F_p^*$ и $b \in F_p$. Пусть N — число решений этого уравнения. Наша цель — получить формулу для N и оценку для него. Для этого будут использоваться те же методы, которые уже были развиты в предыдущих параграфах.

Для начала мы имеем равенство

$$N = \sum N\left(x_1^{l_1} = u_1\right) N\left(x_2^{l_2} = u_2\right) \ldots N\left(x_r^{l_r} = u_r\right), \tag{4}$$

где сумма берется по всем таким r-наборам $(u_1, u_2, \ldots, u_r)$, что $\sum_{i=1}^{r} a_i u_i = b$.

Мы предположим, что $l_1, l_2, \ldots, l_r$ являются делителями числа $p - 1$, хотя в этом и нет необходимости (см. упражнения). Пусть χ_i пробегает характеры порядка l_i. Тогда

$$N\left(x_i^{l_i} = u_i\right) = \sum_{\chi_i} \chi_i(u_i).$$

Подставляя это в равенство (4), получаем

$$N = \sum_{\chi_1,\ \chi_2,\ \ldots,\ \chi_r} \sum_{\sum a_i u_i = b} \chi_1(u_1)\chi_2(u_2)\ldots\chi_r(u_r). \tag{5}$$

Внутренняя сумма тесно связана с суммами Якоби, рассмотренными нами.

Случаи $b = 0$ и $b \neq 0$ необходимо рассмотреть отдельно.

Если $b = 0$, то положим $t_i = a_i u_i$. Тогда внутренняя сумма превращается в

$$\chi_1(a_1^{-1})\chi_2(a_2^{-1})\ldots\chi_r(a_r^{-1}) J_0(\chi_1, \chi_2, \ldots, \chi_r).$$

Если $b \neq 0$, то положим $t_i = b^{-1} a_i u_i$. Внутренняя сумма превращается в

$$\chi_1\chi_2\ldots\chi_r(b)\chi_1(a_1^{-1})\ldots\chi_r(a_r^{-1}) J(\chi_1, \chi_2, \ldots, \chi_r).$$

В обоих случаях, если $\chi_1 = \chi_2 = \ldots = \chi_r = \varepsilon$, то выписанный член имеет значение p^{r-1}, так как $J_0(\varepsilon, \ldots, \varepsilon) = J(\varepsilon, \varepsilon, \ldots, \varepsilon) = p^{r-1}$. Если некоторые, но не все, χ_i равны ε, то этот член равен нулю. В первом случае его значение равно нулю, если $\chi_1\chi_2\ldots\chi_r \neq \varepsilon$. Все это следует из предложения 8.5.1.

Объединяя это с теоремой 4, получаем такой результат:

Теорема 5. *Если* $b = 0$, *то*

$$N = p^{r-1} + \sum \chi_1(a_1^{-1})\chi_2(a_2^{-1}) \dots \chi_r(a_r^{-1}) J_0(\chi_1, \chi_2, \dots, \chi_r).$$

Сумма берется по всем r-наборам характеров $\chi_1, \chi_2, \dots, \chi_r$, *таким, что* $\chi_i^{l_i} = \varepsilon$, $\chi_i \neq \varepsilon$ *для* $i = 1, \dots, r$ *и* $\chi_1\chi_2 \dots \chi_r = \varepsilon$. *Если* M — *число таких r-наборов, то*

$$|N - p^{r-1}| \leqslant M(p-1)p^{(r/2)-1}.$$

Если $b \neq 0$, *то*

$$N = p^{r-1} + \sum \chi_1\chi_2 \dots \chi_r(b)\chi_1(a_1^{-1}) \dots \chi_r(a_r^{-1}) J(\chi_1, \chi_2, \dots, \chi_r).$$

Суммирование ведется по всем r-наборам характеров $\chi_1, \dots, \chi_r$, *таким, что* $\chi_i^{l_i} = \varepsilon$ *и* $\chi_i \neq \varepsilon$ *для* $i = 1, \dots, r$. *Если* M_0 — *число таких r-наборов с* $\chi_1\chi_2 \dots \chi_r = \varepsilon$ *и* M_1 — *число таких наборов с* $\chi_1\chi_2 \dots \chi_r \neq \varepsilon$, *то*

$$|N - p^{r-1}| \leqslant M_0 p^{(r/2)-1} + M_1 p^{(r-1)/2}.$$

Стоит обратить внимание на одно непосредственное следствие теоремы 5. Для $a_1, a_2, \dots, a_r$ и $b \in \mathbf{Z}$ рассмотрим сравнение

$$a_1x_1^{l_1} + a_2x_2^{l_2} + \dots + a_rx_r^{l_r} \equiv b \ (p).$$

Если p достаточно велико, это сравнение имеет много решений. В действительности число решений стремится к бесконечности с возрастанием p.

Замечания

Эта глава была написана под воздействием знаменитой статьи А. Вейля [80]. Основная связь между суммами Гаусса, называемыми также резольвентами Лагранжа, и суммами Якоби была известна Гауссу [34] (не опубликовано), Якоби [47], Эйзенштейну [27] и Коши. Полные доказательства фундаментальных соотношений, приводимых в предложении 8.3.3 и теореме 1, были опубликованы Эйзенштейном в его статье «Beiträge zur Kreistheilung» («К вопросу о делении круга») в 1844 г. Эйзенштейн ввел также обобщение суммы Якоби (§ 5) для получения доказательства биквадратичного закона взаимности (см. гл. 9).

Помимо применения в доказательстве гипотезы Вейля—Римана для некоторых гиперповерхностей над конечными полями (см. гл. 11) обобщенная сумма Якоби имеет важное значение в теории круговых полей и разностных множеств (difference sets). В качестве введения в этот круг вопросов см. [74]. См. также трудное, но важное продолжение [81] работы [80].

Материал о суммах Гаусса и Якоби разбросан по всей книге Хассе [41]. В последней главе он дает систематическое изложе-

ние вопроса, причем в дополнение ко многим интересным результатам показывает, как оба типа сумм естественно возникают в теории круговых полей. Большая часть теории, изложенной в этой главе, почерпнута из статьи Дэвенпорта и Хассе [23]. Последняя статья заслуживает самого пристального изучения, но она, к сожалению, рассчитана на повышенный уровень и, по-видимому, недоступна для начинающего. Несколько легче более поздние статьи [82] и [83]. Можно обратиться также к классическому труду [5].

Не так давно Берндт и Эванс изучили суммы Гаусса и Якоби, а также другие классические суммы, соответствующие характерам порядка 6, 8, 12, 24. С их интересными результатами и обширной библиографией читатель может ознакомиться в [92] и [95]. См. также [177].

Теорема 2 доказана Гауссом в § 358 «Disquisitiones Arithmeticae». На самом деле он не сформулировал эту теорему явно. Она получилась как побочный результат при исследовании другого вопроса. Что он в действительности сделал — это использовал ее для нахождения алгебраического уравнения, которому удовлетворяют некоторые суммы Гаусса. Мы пошли в обратном направлении, использовав теорию гауссовых сумм для получения нашей теоремы. Другие результаты этого типа были получены Гауссом в его первом мемуаре о биквадратичной взаимности [34]. Дальнейшие исторические замечания на эту тему см. во введении к статье [80].

Оценки, приведенные в теореме 5, получены в первой главе книги [9]. В ней используется несколько иной метод, который мы намечаем в общих чертах в упражнениях. В частном случае квадратичных форм, т. е. когда все l равны 2, этот результат восходит по крайней мере к Диксону [25].

Техника вычисления решений с помощью характеров естественно связана с проблемой нахождения последовательности целых чисел заданной длины, имеющих заданные k-степенные характеры по модулю p. Эта проблема до некоторой степени рассмотрена у Хассе [41]. В интересной и элементарной статье [21] показано, что число последовательностей четырех следующих друг за другом квадратичных вычетов между 1 и p удовлетворяет неравенству $|R - p/8| < Kp^{3/4}$, где K — не зависящая от p постоянная. Если воспользоваться результатами Вейля, то можно получить лучшие оценки. Статья [36] посвящена той же теме.

Наше последнее замечание касается теоремы 5. Она была доказана первоначально Вейлем и независимо (и почти одновременно) Хуа и Вандивером (Proc. Nat. Acad. Sci. U. S. A., 1949, v. 35, p. 94—99). С небольшими упрощениями и дополнениями мы, по существу, следовали изложению Вейля.

Упражнения

1. Пусть p — простое число и $d = (m, p-1)$. Доказать, что $N(x^m = a) = \sum \chi(a)$, где сумма берется по всем χ, таким, что $\chi^d = \varepsilon$.

2. В обозначениях упр. 1 показать, что $N(x^m = a) = N(x^d = a)$, и сделать вывод о том, что если $d_i = (m_i, p-1)$, то уравнения $\sum_i a_i x_i^{m_i} = b$ и $\sum_i a_i x_i^{d_i} = b$ имеют одинаковое число решений.

3. Пусть χ — нетривиальный мультипликативный характер поля F_p и ρ — характер порядка 2. Показать, что $\sum_t \chi(1-t^2) = J(\chi, \rho)$. [*Указание.* Вычислить $J(\chi, \rho)$, используя соотношение $N(x^2 = a) = 1 + \rho(a)$.]

4. Показать, что если $k \in F_p$, $k \neq 0$, то $\sum_t \chi(t(k-t)) = \chi(k^2/2^2) J(\chi, \rho)$.

5. Показать, что если $\chi^2 \neq \varepsilon$, то $g(\chi)^2 = \chi(2)^{-2} J(\chi, \rho)\, g(\chi^2)$. [*Указание.* Явно записать $g(\chi)^2$ и воспользоваться упр. 4.]

6 (продолжение). Показать, что $J(\chi, \chi) = \chi(2)^{-2} J(\chi, \rho)$.

7. Предположим, что $p \equiv 1$ (4) и что χ — характер порядка 4. Тогда $\chi^2 = \rho$ и $J(\chi, \chi) = \chi(-1) J(\chi, \rho)$. [*Указание.* Вычислить $g(\chi)^4$ двумя способами.]

8. Обобщить упр. 3 следующим образом. Предположим, что p — некоторое простое число; тогда $\sum_t \chi(1-t^m) = \sum_\lambda J(\chi, \lambda)$, где λ пробегает все такие характеры, что $\lambda^m = \varepsilon$. Получить отсюда, что $\left| \sum_t \chi(1-t^m) \right| \leqslant (m-1)\, p^{1/2}$.

9. Предположим, что $p \equiv 1$ (3) и что χ — характер порядка 3. Доказать (используя упр. 5), что $g(\chi)^3 = p\pi$, где $\pi = \chi(2) J(\chi, \rho)$.

10 (продолжение). Показать, что $\chi\rho$ — характер порядка 6 и что $g(\chi\rho)^6 = (-1)^{(p-1)/2} p\bar{\pi}^3$.

11. Воспользоваться теоремой Гаусса для нахождения числа решений уравнения $x^3 + y^3 = 1$ в F_p для $p = 13$, 19, 37 и 97.

12. Мы видели, что если $p \equiv 1$ (4), то $p = a^2 + b^2$, где $a, b \in \mathbf{Z}$. Предполагая, что a и b положительны, a нечетно и b четно, показать, что a и b однозначно определены. [*Указание.* Воспользоваться тем фактом, что в $\mathbf{Z}[i]$ имеет место однозначность разложения на простые множители и что если $p = a^2 + b^2$, то $a + bi$ — простой элемент в $\mathbf{Z}[i]$.]

13. Мы видели, что если $p \equiv 1$ (3), то $4p = A^2 + 27B^2$, где $A, B \in \mathbf{Z}$. Потребовав, чтобы $A \equiv 1$ (3), показать, что A определено однозначно. [*Указание.* Использовать тот факт, что в $\mathbf{Z}[\omega]$ имеет место однозначность разложения на простые множители. Это доказательство несколько сложнее, чем в упр. 12.]

14. Предположим, что $p \equiv 1$ (n) и что χ — характер порядка n. Показать, что $g(\chi)^n \in \mathbf{Z}[\zeta]$, где $\zeta = e^{2\pi i/n}$.

15. Предположим, что $p \equiv 1$ (6), и пусть χ и ρ — характеры порядков 3 и 2 соответственно. Показать, что число решений уравнения $y^2 = x^3 + D$ в F_p равно $p + \pi + \bar{\pi}$, где $\pi = \chi\rho(D) J(\chi, \rho)$. Показать, что если $\chi(2) = 1$, то число решений уравнения $y^2 = x^3 + 1$ равно $p + A$, где $4p = A^2 + 27B^2$ и $A \equiv 1$ (3). Проверить этот результат прямым вычислением при $p = 31$.

16. Предположим, что $p \equiv 1$ (4) и что χ — характер порядка 4. Пусть N — число решений уравнения $x^4 + y^4 = 1$ в F_p. Показать, что $N = p + 1 - \delta_4(-1)\, 4 + 2\,\mathrm{Re}\, J(\chi, \chi) + 4\,\mathrm{Re}\, J(\chi, \rho)$.

17 (продолжение). Согласно упр. 7, $J(\chi, \chi) = \chi(-1) J(\chi, \rho)$. Пусть $\pi = -J(\chi, \rho)$. Показать, что

(a) $N = p - 3 - 6\,\mathrm{Re}\,\pi$, если $p \equiv 1$ (8);

(b) $N = p + 1 - 2\,\mathrm{Re}\,\pi$, если $p \equiv 5$ (8).

18 (продолжение). Пусть $\pi = a + bi$. Можно показать (см. гл. 11 § 5), что a нечетно, b четно и $a \equiv 1$ (4), если $4 \mid b$, и $a \equiv -1$ (4), если $4 \nmid b$. Пусть $p = A^2 + B^2$, и зафиксируем A требованием $A \equiv 1$ (4). Показать тогда, что

(a) $N = p - 3 - 6A$, если $p \equiv 1$ (8);
(b) $N = p + 1 + 2A$, если $p \equiv 5$ (8).

19. Найти формулу для числа решений уравнения $x_1^2 + x_2^2 + \ldots + x_r^2 = 0$ в F_p.

20. Обобщить предложение 8.6.1, найдя явную формулу для числа решений уравнения $a_1x_1^2 + a_2x_2^2 + \ldots + a_rx_r^2 = 1$ в F_p.

21. Предположим, что $p \equiv 1$ (d), $\zeta = e^{2\pi i/p}$, и рассмотрим $\sum_x \zeta^{ax^d}$. Показать, что $\sum_x \zeta^{ax^d} = \sum_r m(r)\,\zeta^{ar}$, где $m(r) = N(x^d = r)$.

22 (продолжение). Доказать, что $\sum_x \zeta^{ax^d} = \sum_\chi g_a(\chi)$, где сумма берется по всем χ, для которых $\chi^d = \varepsilon$, $\chi \neq \varepsilon$. Предположить, что $p \nmid a$.

23. Пусть $f(x_1, x_2, \ldots, x_n) \in F_p[x_1, x_2, \ldots, x_n]$. Пусть N — число нулей многочлена f в F_p. Показать, что

$$N = p^{n-1} + p^{-1} \sum_{a \neq 0} \left(\sum_{x_1, \ldots, x_n} \zeta^{af(x_1, \ldots, x_n)} \right).$$

24 (продолжение). Пусть $f(x_1, x_2, \ldots, x_n) = a_1x_1^{m_1} + a_2x_2^{m_2} + \ldots + a_nx_n^{m_n}$. Пусть $d_i = (m_i, p - 1)$. Показать, что

$$N = p^{n-1} + p^{-1} \sum_{a \neq 0} \prod_{i=1}^{n} \sum_{\chi_i} g_{aa_i}(\chi_i),$$

где χ_i пробегает все характеры, для которых $\chi_i^{d_i} = \varepsilon$ и $\chi_i \neq \varepsilon$.

25. Получить из упр. 24, что

$$\left| N - p^{n-1} \right| \leqslant (p-1)(d_1 - 1) \ldots (d_n - 1)\, p^{(n/2)-1}.$$

26. Пусть p — простое число, $p \equiv 1$ (4), χ — мультипликативный характер порядка 4 поля F_p и ρ — символ Лежандра. Положим $J(\chi, \rho) = a + bi$. Показать, что

(a) $N(y^2 + x^4 = 1) = p - 1 + 2a$;

(b) $N(y^2 = 1 - x^4) = p + \sum \rho(1 - x^4)$;

(c) $2a \equiv -(-1)^{(p-1)/4} \binom{2m}{m}$ (p), где $m = (p-1)/4$;

(d) проверить (c) для $p = 13, 17, 29$.

27. Пусть $p \equiv 1$ (3), χ — характер порядка 3, ρ — символ Лежандра. Показать, что

(a) $N(y^2 = 1 - x^3) = p + \sum \rho(1 - x^3)$;

(b) $N(y^2 + x^3 = 1) = p + 2\mathrm{Re}\, J(\chi, \rho)$;

(c) $2a - b \equiv -\binom{(p-1)/2}{(p-1)/3}$ (p), где $J(\chi, \rho) = a + b\omega$.

28. Пусть $p \equiv 3\ (4)$ и χ — квадратичный характер, определенный на $\mathbf{Z}/p\mathbf{Z}$. Показать, что

(a) $\sum_{x=1}^{p-1} x\chi(x) = 2\sum_{x=1}^{(p-1)/2} x\chi(x) - p\sum_{x=1}^{(p-1)/2} \chi(x)$;

(b) $\sum_{x=1}^{p-1} x\chi(x) = 4\chi(2)\sum_{x=1}^{(p-1)/2} x\chi(x) - p\chi(2)\sum_{x=1}^{(p-1)/2} \chi(x)$;

(c) если $p \equiv 3\ (8)$, то $\sum_{x=1}^{p-1} x\chi(x)/p = \frac{1}{3}\sum_{x=1}^{(p-1)/2} \chi(x)$;

(d) если $p \equiv 7\ (8)$, то $\sum_{x=1}^{p-1} x\chi(x)/p = \sum_{x=1}^{(p-1)/2} \chi(x)$.

Глава 9

КУБИЧЕСКИЙ И БИКВАДРАТИЧНЫЙ ЗАКОНЫ ВЗАИМНОСТИ

В гл. 5 мы видели, что квадратичный закон взаимности дает ответ на такой вопрос: для каких простых чисел p разрешимо сравнение $x^2 \equiv a \ (p)$? Здесь a — некоторое фиксированное число. Если тот же самый вопрос поставить для сравнений $x^n \equiv a \ (p)$, где n — фиксированное положительное целое число, то мы вступим в область высших законов взаимности. При $n = 3$ и 4 мы говорим о кубическом и биквадратичном законах взаимности.

Во введении к двум своим знаменитым статьям «Theorie der biquadratischen Reste I, II» («*Теория биквадратичных вычетов* I, II») [34] *Гаусс пишет, что теория квадратичных вычетов приведена в состояние такого совершенства, что и желать больше нечего. А с другой стороны, «теория кубических и биквадратичных вычетов гораздо труднее». Он смог рассмотреть лишь некоторые частные случаи, доказательства для которых оказались столь трудными, что вскоре он пришел к выводу о том, что «...принципы арифметики, разработанные до сих пор, совершенно недостаточны для обоснования новой теории, что эта теория требует с необходимостью, чтобы область высшей арифметики была расширена до бесконечности...». На современном языке он призывает к созданию теории алгебраических чисел. В качестве первого шага, имея в виду изучение биквадратичных вычетов, он детально исследует арифметику кольца* $\mathbf{Z}[i]$, *которое мы теперь называем кольцом гауссовых целых чисел.*

Любопытно, что, хотя Гаусс открыл биквадратичный закон взаимности, он его полностью не доказал. Первые полные опубликованные доказательства кубического и биквадратичного законов взаимности принадлежат Эйзенштейну.

В этой главе мы сформулируем и докажем кубический и биквадратичный законы взаимности. Мы дадим два доказательства кубического закона взаимности. Первое принадлежит Эйзенштейну и во всех отношениях близко к доказательству квадратичного закона взаимности из гл. 6. *Второе доказательство использует суммы Якоби и аналогично доказательству квадратичного закона взаимности из гл.* 8, § 6. *Наше доказательство биквадратичного закона взаимности также принадлежит Эйзенштейну.*

В § 9 устанавливается рациональный закон взаимности для биквадратичных вычетов. Этот элегантный результат, полученный Бурдэ в 1969 г., решает следующую задачу. Если $p \equiv 1$ (4) и $q \equiv 1$ (4) — простые числа и p есть четвертая степень по модулю q, то каковы необходимые и достаточные условия для того, чтобы q было четвертой степенью по модулю p?

В § 11 с помощью сумм Якоби будет получен критерий Гаусса возможности построения правильного многоугольника.

Глава кончается кратким обсуждением проблемы Куммера относительно распределения кубических сумм Гаусса.

§ 1. Кольцо Z [ω]

Пусть $\omega = (-1 + \sqrt{-3})/2$. Кольцо $\mathbf{Z}[\omega]$ было определено и обсуждалось в гл. 1, § 4. Его элементами являются комплексные числа вида $a + b\omega$, $a, b \in \mathbf{Z}$. Если $\alpha = a + b\omega \in \mathbf{Z}[\omega]$, то определим норму элемента α, $N\alpha$, формулой $N\alpha = \alpha\bar{\alpha} = a^2 - ab + b^2$. Здесь $\bar{\alpha}$ означает комплексно-сопряженный к α. В гл. 1 использовалось обозначение $\lambda(\alpha)$ вместо $N\alpha$. Изменение делается лишь для согласования со стандартным обозначением. Для удобства записи мы положим также $D = \mathbf{Z}[\omega]$.

Как мы доказали ранее, D — область с однозначным разложением на простые множители. Наша первая задача — описать единицы и простые элементы в D.

Предложение 9.1.1. *$\alpha \in D$ является единицей тогда и только тогда, когда $N\alpha = 1$. Единицы в D суть $1, -1, \omega, -\omega, \omega^2$ и $-\omega^2$.*

Доказательство. Если $N\alpha = 1$, то $\alpha\bar{\alpha} = 1$; это означает, что α — единица, ибо $\bar{\alpha} \in D$.

Если α — единица, то существует такое $\beta \in D$, что $\alpha\beta = 1$. В таком случае $N\alpha N\beta = 1$. Так как $N\alpha$ и $N\beta$ — положительные целые числа, это означает, что $N\alpha = 1$.

Предположим теперь, что $\alpha = a + b\omega$ — единица. Тогда $1 = a^2 - ab + b^2$, или $4 = (2a - b)^2 + 3b^2$. Имеются две возможности:

(a) $2a - b = \pm 1$, $b = \pm 1$;

(b) $2a - b = \pm 2$, $b = 0$.

Решая эти шесть пар уравнений, получаем $1, -1, \omega, -\omega, -1 - \omega$ и $1 + \omega$. Так как $\omega^2 + \omega + 1 = 0$, последние два элемента совпадают с ω^2 и $-\omega^2$. Предложение доказано. □

Для исследования простых элементов в D важно представлять себе, что числа, простые в $\mathbf{Z}$, не обязательно будут простыми элементами в D. Например, $7 = (3 + \omega)(2 - \omega)$. По этой причине мы будем говорить о простых числах в $\mathbf{Z}$ как о рациональ-

ных простых числах, а о простых элементах кольца D — как о простых числах.

Предложение 9.1.2. *Если π — простое число в D, то существует такое простое рациональное число p, что $N\pi = p$ или $N\pi = p^2$. В первом случае π не ассоциировано ни с каким простым рациональным числом; во втором случае π ассоциировано с p.*

Доказательство. Имеем $N\pi = n > 1$, или $\pi\bar{\pi} = n$. Целое число n представляется в виде произведения рациональных простых чисел. Таким образом, $\pi \mid p$ для некоторого рационального простого числа p. Если $p = \pi\gamma$, $\gamma \in D$, то $N\pi N\gamma = Np = p^2$. Таким образом, либо $N\pi = p^2$ и $N\gamma = 1$, либо $N\pi = p$. В первом случае γ — единица и потому π ассоциировано с p. Во втором случае, если $\pi = uq$, u — единица и q — рациональное простое число, то $p = N\pi = NuNq = q^2$, что невозможно. Следовательно, π не ассоциировано ни с каким рациональным простым числом. □

Предложение 9.1.3. *Если $\pi \in D$ — такое число, что $N\pi = p$, p — рациональное простое число, то π — простое число в D.*

Доказательство. Если бы π не было простым числом в D, то мы могли бы записать $\pi = \rho\gamma$, где $N\rho$, $N\gamma > 1$. В таком случае $p = N\pi = N\rho\, N\gamma$, что невозможно, ибо p — простое число в $\mathbf{Z}$. Следовательно, π — простое число в D. □

Следующий результат классифицирует простые числа в D.

Предложение 9.1.4. *Предположим, что p и q — рациональные простые числа. Если $q \equiv 2$ (3), то q — простое число в D. Если $p \equiv 1$ (3), то $p = \pi\bar{\pi}$, где π — простое число в D. Наконец, $3 = -\omega^2(1-\omega)^2$ и $1 - \omega$ — простое число в D.*

Доказательство. Предположим, что p — непростое число в D. Тогда $p = \pi\gamma$, где $N\pi > 1$, $N\gamma > 1$. Отсюда следует, что $p^2 = N\pi N\gamma$ и $N\pi = p$. Пусть $\pi = a + b\omega$. Тогда $p = a^2 - ab + b^2$, или $4p = (2a-b)^2 + 3b^2$, откуда получаем, что $p \equiv (2a-b)^2$ (3). Если $3 \nmid p$, то $p \equiv 1$ (3), так как 1 — единственный ненулевой квадрат по модулю 3. Отсюда сразу же следует, что если $q \equiv 2$ (3), то оно будет простым числом в D.

Предположим теперь, что $p \equiv 1$ (3). По квадратичному закону взаимности имеем

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{3}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)(-1)^{((p-1)/2)\,((3-1)/2)} =$$

$$= \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

Следовательно, существует такое $a \in \mathbf{Z}$, что $a^2 \equiv -3\ (p)$, или $pb = a^2 + 3$ для некоторого $b \in \mathbf{Z}$. Таким образом, p делит $(a + \sqrt{-3})(a - \sqrt{-3}) = (a + 1 + 2\omega)(a - 1 - 2\omega)$. Если бы p было простым числом в D, то оно делило бы один из сомножителей, чего быть не может, ибо $p \neq 2$ и $2/p \notin \mathbf{Z}$. Таким образом, $p = \pi\gamma$, где π и γ не являются единицами. Беря нормы, видим, что $p^2 = N\pi N\gamma$ и $p = N\pi = \pi\bar{\pi}$.

Последний случай разбирается следующим образом. Из равенства $x^3 - 1 = (x - 1)(x - \omega)(x - \omega^2)$ вытекает, что $x^2 + x + 1 = (x - \omega)(x - \omega^2)$. Полагая $x = 1$, получаем $3 = (1 - \omega)(1 - \omega^2) = (1 + \omega)(1 - \omega)^2 = -\omega^2(1 - \omega)^2$. Беря нормы, приходим к равенству $9 = N(1 - \omega)^2$, а потому $3 = N(1 - \omega)$. Следовательно, $1 - \omega$ — простое число в D. □

Относительно дальнейших обозначений сделаем следующее замечание: q будет положительным рациональным простым числом, сравнимым с 2 по модулю 3, а π — простым комплексным числом, норма $N\pi = p$ которого есть рациональное простое число, сравнимое с 1 по модулю 3. Иногда π будет обозначать произвольное простое число в D. Из контекста будет ясно, что имеется в виду.

§ 2. Кольца классов вычетов

Как и в случаях кольца $\mathbf{Z}$ и кольца всех целых алгебраических чисел, понятие сравнимости оказывается в высшей степени полезным в D. Если $\alpha, \beta, \gamma \in D$ и $\gamma \neq 0$ — не единица, то мы говорим, что $\alpha \equiv \beta\ (\gamma)$, если γ делит $\alpha - \beta$. Как и для $\mathbf{Z}$, классы элементов по модулю γ можно превратить в кольцо $D/\gamma D$, называемое кольцом классов вычетов по модулю γ.

Предложение 9.2.1. *Пусть $\pi \in D$ — простое число. Тогда $D/\pi D$ есть поле, состоящее из $N\pi$ элементов.*

Доказательство. Мы покажем сначала, что $D/\pi D$ — поле. Пусть $\alpha \in D$ таково, что $\alpha \not\equiv 0\ (\pi)$. Согласно следствию 1 предложения 1.3.2, существуют элементы $\beta, \gamma \in D$, для которых $\beta\alpha + \gamma\pi = 1$. Таким образом, $\beta\alpha \equiv 1\ (\pi)$, откуда следует, что класс вычетов элемента α является единицей в $D/\pi D$. Чтобы показать, что $D/\pi D$ имеет $N\pi$ элементов, мы должны рассмотреть отдельно случаи из предложения 9.1.4.

Предположим, что $\pi = q$ — рациональное простое число, сравнимое с 2 по модулю 3. Мы утверждаем, что $\{a + b\omega \mid 0 \leqslant a < q \text{ и } 0 \leqslant b < q\}$ — полное множество представителей классов вычетов. Из этого будет следовать, что $D/\pi D$ имеет $q^2 = Nq$ элементов. Пусть $\mu = m + n\omega \in D$. Тогда $m = qs + a$ и $n = qt + b$, где $s, t, a, b \in \mathbf{Z}$ и $0 \leqslant a, b < q$. Ясно, что $\mu \equiv a +$

$+ b\omega$ (q). Далее, предположим, что $a + b\omega \equiv a' + b'\omega$ (q), где $0 \leqslant a, b, a', b' < q$. Тогда $((a - a')/q) + ((b - b')/q)\,\omega \in D$, откуда следует, что $(a - a')/q$ и $(b - b')/q$ лежат в $\mathbf{Z}$. Это возможно лишь при $a = a'$ и $b = b'$.

Предположим теперь, что $p \equiv 1$ (3) — рациональное простое число и $\pi\bar{\pi} = N\pi = p$. Мы утверждаем, что $\{0, 1, \ldots, p - 1\}$ — полное множество представителей классов вычетов. Из этого будет следовать, что $D/\pi D$ имеет $p = N\pi$ элементов. Пусть $\pi = a + b\omega$. Так как $p = a^2 - ab + b^2$, то $p \nmid b$. Пусть $\mu = m + n\omega$. Существует такое целое число c, что $cb \equiv n$ (p). Тогда $\mu - c\pi \equiv m - ca$ (p), так что $\mu \equiv m - ca$ (π). Каждый элемент из D сравним с некоторым целым рациональным числом по модулю π. Если $l \in \mathbf{Z}$, то $l = sp + r$, где $s, r \in \mathbf{Z}$ и $0 \leqslant r < p$. Таким образом, $l \equiv r$ (p) и, тем более, $l \equiv r$ (π). Мы показали, что каждый элемент из D сравним с каким-либо элементом из $\{0, 1, 2, \ldots, p - 1\}$ по модулю π. Если $r \equiv r'$ (π) с $r, r' \in \mathbf{Z}$ и $0 \leqslant r, r' < p$, то $r - r' = \pi\gamma$ и $(r - r')^2 = pN\gamma$, откуда следует, что $p \mid r - r'$. Таким образом, $r = r'$, и данный случай разобран.

Случай простого числа $1 - \omega$ предлагается рассмотреть в качестве упражнения. □

§ 3. Характер кубического вычета

Пусть π — простое число. Тогда мультипликативная группа поля $D/\pi D$ имеет порядок $N\pi - 1$. Мы получаем, таким образом, аналог малой теоремы Ферма.

Предложение 9.3.1. *Если* $\pi \nmid \alpha$, *то*

$$\alpha^{N\pi - 1} \equiv 1 \ (\pi).$$

Если норма числа π отлична от 3, то классы вычетов чисел 1, ω и ω^2 различны в $D/\pi D$. Чтобы убедиться в этом, предположим, например, что $\omega \equiv 1$ (π). Тогда $\pi \mid 1 - \omega$, а так как $1 - \omega$ — простое число, то π и $1 - \omega$ ассоциированы. Таким образом, $N\pi = N(1 - \omega) = 3$ — противоречие. Другие случаи разбираются тем же способом.

Так как $\{1, \omega, \omega^2\}$ есть циклическая группа порядка 3, то 3 делит порядок группы $(D/\pi D)^*$, т. е. $3 \mid N\pi - 1$. В этом можно убедиться и другим способом, используя предложение 9.1.3. Если $\pi = q$, q — рациональное простое число, то $N\pi = q^2 \equiv 1$ (3). Если π таково, что $N\pi = p$, то $p \equiv 1$ (3).

Предложение 9.3.2. *Предположим, что* π — *простое число, для которого* $N\pi \neq 3$, *и что* $\pi \nmid \alpha$. *Тогда существует единственное целое число* $m = 0$, 1 *или* 2, *для которого* $\alpha^{(N\pi - 1)/3} \equiv \omega^m$ (π).

Доказательство. Как мы знаем, π делит $\alpha^{N\pi-1} - 1$. Далее,

$$\alpha^{N\pi-1} - 1 = (\alpha^{(N\pi-1)/3} - 1)(\alpha^{(N\pi-1)/3} - \omega)(\alpha^{(N\pi-1)/3} - \omega^2).$$

Так как π — простое число, оно должно делить один из трех сомножителей справа. Согласно предшествующему замечанию, оно может делить только один сомножитель, ибо если бы оно делило два, то оно делило бы их разность. Предложение доказано. □

На основе этого результата можно дать следующее определение.

Определение. Если $N\pi \neq 3$, то *характер* $(\alpha/\pi)_3$ *кубического вычета числа* α *по модулю* π задается так:
(a) $(\alpha/\pi)_3 = 0$ при $\pi \mid \alpha$;
(b) $\alpha^{(N\pi-1)/3} \equiv (\alpha/\pi)_3 \ (\pi)$, где $(\alpha/\pi)_3$ равно 1, ω или ω^2.

Этот характер играет в теории кубических вычетов ту же роль, что и символ Лежандра — в теории квадратичных вычетов.

Предложение 9.3.3. (a) $(\alpha/\pi)_3 = 1$ *тогда и только тогда, когда* $x^3 \equiv \alpha \ (\pi)$ *разрешимо, т. е. тогда и только тогда, когда* α — *кубический вычет.*
(b) $\alpha^{(N\pi-1)/3} \equiv (\alpha/\pi)_3 \ (\pi)$.
(c) $(\alpha\beta/\pi)_3 = (\alpha/\pi)_3 (\beta/\pi)_3$.
(d) *Если* $\alpha \equiv \beta \ (\pi)$, *то* $(\alpha/\pi)_3 = (\beta/\pi)_3$.

Доказательство Пункт (a) — это частный случай предложения 7.1.2. Следует положить в этом предложении $F = D/\pi D$, $q = N\pi$ и $n = 3$.

Пункт (b) совпадает с определением.

Пункт (c): $(\alpha\beta/\pi)_3 \equiv (\alpha\beta)^{(N\pi-1)/3} \equiv \alpha^{(N\pi-1)/3}\beta^{(N\pi-1)/3} \equiv (\alpha/\pi)_3 (\beta/\pi)_3 \ (\pi)$. Отсюда следует доказываемый результат.

Пункт (d): если $\alpha \equiv \beta \ (\pi)$, то $(\alpha/\pi)_3 \equiv \alpha^{(N\pi-1)/3} \equiv \beta^{(N\pi-1)/3} \equiv (\beta/\pi)_3 \ (\pi)$, так что $(\alpha/\pi)_3 = (\beta/\pi)_3$. □

Поскольку в этой главе мы будем иметь дело лишь с характером кубического вычета, будет удобно использовать обозначение $\chi_\pi(\alpha) = (\alpha/\pi)_3$.

Полезно изучить поведение характеров при комплексном сопряжении.

Предложение 9.3.4. (a) $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$;
(b) $\overline{\chi_\pi(\alpha)} = \chi_{\bar\pi}(\bar\alpha)$.

Доказательство. (a) $\chi_\pi(\alpha)$ по определению равно 1, ω или ω^2, и каждое из этих чисел в квадрате равно своему сопряженному.

(b) Имеем

$$\alpha^{(N\pi-1)/3} \equiv \chi_\pi(\alpha)\ (\pi),$$

откуда вытекает, что

$$\bar{\alpha}^{(N\pi-1)/3} \equiv \overline{\chi_\pi(\alpha)}\ (\bar{\pi}).$$

Так как $N\bar{\pi} = N\pi$, полученное сравнение показывает, что $\chi_{\bar{\pi}}(\bar{\alpha}) \equiv \overline{\chi_\pi(\alpha)}\ (\bar{\pi})$, а следовательно, $\chi_{\bar{\pi}}(\bar{\alpha}) = \overline{\chi_\pi(\alpha)}$. □

Следствие. $\chi_q(\bar{\alpha}) = \chi_q(\alpha^2)$ *и* $\chi_q(n) = 1$, *если* n — *рациональное целое число, взаимно простое с* q.

Доказательство. Так как $\bar{q} = q$, то $\chi_q(\bar{\alpha}) = \chi_{\bar{q}}(\bar{\alpha}) = \overline{\chi_q(\alpha)} = \chi_q(\alpha^2)$, что дает первое соотношение.

Поскольку $\bar{n} = n$, то $\chi_q(n) = \overline{\chi_q(n)} = \chi_q(n)^2$. Так как $\chi_q(n) \neq 0$, отсюда следует, что $\chi_q(n) = 1$. □

В следствии утверждается, что n есть кубический вычет по модулю q. Таким образом, если $q_1 \neq q_2$ — два простых числа, сравнимых с 2 по модулю 3, то (тривиальным образом) $\chi_{q_1}(q_2) = \chi_{q_2}(q_1)$. Это частный случай кубического закона взаимности. Для формулировки общего закона нужно ввести понятие примарного простого числа.

Определение. Если π — некоторое простое число в D, то мы говорим, что π *примарно*, если $\pi \equiv 2$ (3).

Если $\pi = q$ рационально, то ничего нового не получается. Если же $\pi = a + b\omega$ — комплексное простое число, то это определение эквивалентно условиям $a \equiv 2$ (3) и $b \equiv 0$ (3).

Понятие примарности нам нужно для того, чтобы избавиться от неопределенности, вызываемой тем фактом, что каждый ненулевой элемент в D имеет шесть ассоциированных с ним.

Предложение 9.3.5. *Предположим, что* $N\pi = p \equiv 1$ (3). *Среди чисел, ассоциированных с* π, *имеется точно одно примарное число.*

Доказательство. Запишем $\pi = a + b\omega$. Ассоциированными для π будут π, $\omega\pi$, $\omega^2\pi$, $-\pi$, $-\omega\pi$, $-\omega^2\pi$. Через a и b эти элементы могут быть выражены так:

(a) $a + b\omega$.
(b) $-b + (a - b)\,\omega$.
(c) $(b - a) - a\omega$.
(d) $-a - b\omega$.
(e) $b + (b - a)\,\omega$.
(f) $(a - b) + a\omega$.

Так как $p = a^2 - ab + b^2$, то оба числа a и b не могут делиться на 3. Взглянув на выражения (a) и (b), убеждаемся в возможности предположить, что $3 \nmid a$. Рассматривая (a) и (d), приходим к выводу, что можно также предположить, что $a \equiv 2$ (3). При этом условии равенство $p = a^2 - ab + b^2$ приводит к сравнению $1 \equiv 4 - 2b + b^2$ (3), или $b(b-2) \equiv 0$ (3). Если $3 \mid b$, то $a + b\omega$ примарно. Если $b \equiv 2$ (3), то $b + (b-a)\omega$ примарно.

Для получения единственности предположим, что $a + b\omega$ примарно. Рассматривая класс вычетов первого члена в (b)—(e), убеждаемся в том, что ни одно из этих чисел не примарно. Не будет примарным и число из (f), так как коэффициент a при ω не делится на 3. □

Например, $3 + \omega$ — простое число, ибо $N(3+\omega) = 7$, и $-\omega^2(3+\omega) = 2 + 3\omega$ — примарное простое число, ассоциированное с ним.

Теперь может быть сформулирована

Теорема 1 (кубический закон взаимности). *Пусть* π_1 *и* π_2 — *примарные простые числа,* $N\pi_1$, $N\pi_2 \neq 3$ *и* $N\pi_1 \neq N\pi_2$. *Тогда*

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1).$$

Доказательство будет приведено в § 4, а сначала мы сделаем несколько замечаний.

(a) Следует рассмотреть три случая. А именно: оба числа π_1 и π_2 рациональны, π_1 рационально и π_2 комплексно, оба числа π_1 и π_2 комплексны. Первый случай, как мы видели, тривиален.

(b) Характер кубического вычета для единиц можно получить следующим образом. Так как $-1 = (-1)^3$, то $\chi_\pi(-1) = 1$ для всех простых чисел π.

Если $N\pi \neq 3$, то из предложения 9.3.3, п. (b), следует, что $\chi_\pi(\omega) = \omega^{(N\pi-1)/3}$. Таким образом, $\chi_\pi(\omega) = 1$, ω или ω^2 в зависимости от того, будет $N\pi \equiv 1$, 4 или 7 по модулю 9.

(c) Рассмотрение простого числа $1 - \omega$ представляет особые трудности. Если $N\pi \neq 3$ то мы хотели бы вычислить $\chi_\pi(1-\omega)$. Это сделано Эйзенштейном в [29] с помощью довольно тонких соображений. Элегантное доказательство, принадлежащее Вильямсу, приведено в упражнениях.

Теорема 1′ (дополнение к кубическому закону взаимности). *Предположим, что* $N\pi \neq 3$. *Если* $\pi = q$ *рационально, то запишем* $q = 3m - 1$. *Если* $\pi = a + b\omega$ — *примарное комплексное простое число, запишем* $a = 3m - 1$. *Тогда*

$$\chi_\pi(1-\omega) = \omega^{2m}.$$

Мы дадим доказательство для случая рационального простого числа q. Так как $(1-\omega)^2 = -3\omega$, то

$$\chi_q(1-\omega)^2 = \chi_q(-3)\chi_q(\omega).$$

Согласно следствию предложения 9.3.4, $\chi_q(-3) = 1$. По замечанию (b) $\chi_q(\omega) = \omega^{(Nq-1)/3} = \omega^{(q^2-1)/3}$. Таким образом, $\chi_q(1-\omega)^2 = \omega^{(q^2-1)/3}$. Возводя обе части этого равенства в квадрат, получаем

$$\chi_q(1-\omega) = \omega^{(2/3)(q^2-1)}.$$

Далее, $q^2 - 1 = 9m^2 - 6m$, так что $(2/3)(q^2-1) \equiv -4m \ (3) \equiv 2m \ (3)$, откуда и следует доказываемый результат.

§ 4. Доказательство кубического закона взаимности

Пусть π — такое комплексное простое число, что $N\pi = p \equiv 1 \ (3)$. Так как $D/\pi D$ — конечное поле характеристики p, оно содержит экземпляр поля $\mathbf{Z}/p\mathbf{Z}$. Оба поля $D/\pi D$ и $\mathbf{Z}/p\mathbf{Z}$ имеют по p элементов. Поэтому их можно отождествить. Более явно отождествление задается отображением класса вычетов числа n в $\mathbf{Z}/p\mathbf{Z}$ в соответствующий класс в $D/\pi D$.

Это отождествление дает возможность рассматривать χ_π как кубический характер на $\mathbf{Z}/p\mathbf{Z}$ в смысле гл. 8 [см. предложение 9.3.3, п. (c) и (d)]. Следовательно, можно работать с суммами Гаусса $g_\alpha(\chi_\pi)$ и суммой Якоби $J(\chi_\pi, \chi_\pi)$.

Если χ — произвольный кубический характер, то мы доказали (см. следствие предложения 8.3.3 и предложение 8.3.4), что

(a) $g(\chi)^3 = pJ(\chi, \chi)$;

(b) если $J(\chi, \chi) = a + b\omega$, то $a \equiv -1 \ (3)$ и $b \equiv 0 \ (3)$.

Так как $J(\chi, \chi)\overline{J(\chi, \chi)} = p$, второе утверждение означает, что $J(\chi, \chi)$ — примарное простое число в D с нормой p.

Нам понадобится следующая лемма. Предположим, что π примарно.

Лемма 1. $J(\chi_\pi, \chi_\pi) = \pi$.

Доказательство. Пусть $J(\chi_\pi, \chi_\pi) = \pi'$. Так как $\pi\bar{\pi} = p = \pi'\bar{\pi}'$, то $\pi \mid \pi'$ или $\pi \mid \bar{\pi}'$. Так как все привлеченные простые числа примарны, то либо $\pi = \pi'$, либо $\pi = \bar{\pi}'$. Мы хотим исключить вторую возможность.

Из определений получаем

$$J(\chi_\pi, \chi_\pi) = \sum_x \chi_\pi(x)\chi_\pi(1-x) \equiv \sum_x x^{(p-1)/3}(1-x)^{(p-1)/3} \ (\pi),$$

где сумма берется по всем элементам из $\mathbf{Z}/p\mathbf{Z}$. Многочлен $x^{(p-1)/3}(1-x)^{(p-1)/3}$ имеет степень $(2/3)(p-1) < p-1$. Из упр. 11 гл. 4 следует, что $\sum_x x^{(p-1)/3}(1-x)^{(p-1)/3} \equiv 0\ (p)$. Это показывает, что $J(\chi_\pi, \chi_\pi) \equiv 0\ (\pi)$, т. е. $\pi \mid \pi'$, а значит, $\pi = \pi'$. □

Следствие. $g(\chi_\pi)^3 = p\pi$.

Теперь мы можем доказать кубический закон взаимности. Рассмотрим сначала случай, когда $\pi_1 = q \equiv 2\ (3)$ и $\pi_2 = \pi$, причем $N\pi = p$.

Возведем обе части равенства $g(\chi_\pi)^3 = p\pi$ в степень $(q^2-1)/3$. В результате имеем $g(\chi_\pi)^{q^2-1} = (p\pi)^{(q^2-1)/3}$. Взяв сравнение по модулю q, получим

$$g(\chi_\pi)^{q^2-1} \equiv \chi_q(p\pi)\ (q).$$

Так как $\chi_q(p) = 1$, это дает

$$g(\chi_\pi)^{q^2} \equiv \chi_q(\pi)\, g(\chi_\pi)\ (q). \tag{1}$$

Проанализируем теперь левую часть:

$$g(\chi_\pi)^{q^2} = \Big(\sum \chi_\pi(t)\zeta^t\Big)^{q^2} \equiv \sum \chi_\pi(t)^{q^2}\zeta^{q^2 t}\ (q).$$

Так как $q^2 \equiv 1\ (3)$ и $\chi_\pi(t)$ — корень степени 3 из единицы, то

$$g(\chi_\pi)^{q^2} \equiv g_{q^2}(\chi_\pi)\ (q). \tag{2}$$

Согласно предложению 8.2.1, $g_{q^2}(\chi_\pi) = \chi_\pi(q^{-2})\, g(\chi_\pi) = \chi_\pi(q)\, g(\chi_\pi)$. Таким образом, объединяя сравнения (1) и (2), получаем

$$\chi_\pi(q)\, g(\chi_\pi) \equiv \chi_q(\pi)\, g(\chi_\pi)\ (q).$$

Умножим обе части этого сравнения на $\overline{g(\chi_\pi)}$. Так как $g(\chi_\pi)\,\overline{g(\chi_\pi)} = p$, то

$$\chi_\pi(q)\, p \equiv \chi_q(\pi)\, p\ (q),$$

или

$$\chi_\pi(q) \equiv \chi_q(\pi)\ (q),$$

откуда получаем

$$\chi_\pi(q) = \chi_q(\pi).$$

Остается рассмотреть случай двух комплексных простых чисел π_1 и π_2, для которых $N\pi_1 = p_1 \equiv 1\ (3)$ и $N\pi_2 = p_2 \equiv 1\ (3)$. Этот случай рассматривается по существу так же, но он немного сложнее.

Пусть $\gamma_1 = \bar{\pi}_1$ и $\gamma_2 = \bar{\pi}_2$. Тогда γ_1 и γ_2 примарны и $p_1 = \pi_1\gamma_1$ и $p_2 = \pi_2\gamma_2$.

Начав с равенства $g(\chi_{\gamma_1})^3 = p_1\gamma_1$, возводим его в степень $(N\pi_2 - 1)/3 = (p_2 - 1)/3$ и переходим к сравнению по модулю π_2. Тем же способом, что и выше, получаем соотношение

$$\chi_{\gamma_1}(p_2^2) = \chi_{\pi_2}(p_1\gamma_1). \tag{3}$$

Аналогично, начав с равенства $g(\chi_{\pi_2})^3 = p_2\pi_2$, возводим его в степень $(p_1 - 1)/3$ и переходим к сравнению по модулю π_1. В результате получим

$$\chi_{\pi_2}(p_1^2) = \chi_{\pi_1}(p_2\pi_2). \tag{4}$$

Нам понадобится также соотношение $\chi_{\gamma_1}(p_2^2) = \chi_{\pi_1}(p_2)$, которое получается из предложения 9.3.4, так как $\gamma_1 = \bar{\pi}_1$ и $\bar{p}_2 = p_2$. Далее последовательно получаем

$$\begin{aligned}\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\gamma_1) &= \chi_{\pi_1}(\pi_2)\chi_{\gamma_1}(p_2^2) \text{ (по равенству (3))} = \\ &= \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2) = \chi_{\pi_1}(p_2\pi_2) \text{ (по замечанию выше)} = \\ &= \chi_{\pi_2}(p_1^2) = \chi_{\pi_2}(p_1\pi_1\gamma_1) \text{ (по равенству (4))} = \\ &= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\gamma_1).\end{aligned}$$

Приравнивая первый и последний члены и сокращая на $\chi_{\pi_2}(p_1\gamma_1)$, приходим к нужному результату:

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1).$$

§ 5. Другое доказательство кубического закона взаимности

Мы приведем доказательство кубического закона взаимности с использованием сумм Якоби. Это доказательство несколько короче и более изящно, чем приведенное в § 4. Следует, однако, заметить, что при этом используется больше предварительных сведений.

Рассмотрим случай $\pi_1 = q$, $\pi_2 = \pi$. Пусть $\chi_\pi = \chi$, и рассмотрим сумму Якоби $J(\chi, \chi, \ldots, \chi)$ с q членами. Так как $3 \mid q + 1$, то, согласно следствию 1 теоремы 3 из гл. 8,

$$g(\chi)^{q+1} = pJ(\chi, \chi, \ldots, \chi). \tag{5}$$

Так как $g(\chi)^3 = p\pi$, то

$$g(\chi)^{q+1} = (p\pi)^{(q+1)/3}. \tag{6}$$

Далее, напомним, что

$$J(\chi, \chi, \ldots, \chi) = \sum \chi(x_1)\chi(x_2)\ldots\chi(x_q),$$

где сумма берется по всем $x_1, x_2, \ldots, x_q \in \mathbf{Z}/p\mathbf{Z}$ с $x_1 + x_2 + \ldots + x_q = 1$. Рассмотрим член, для которого $x_1 = x_2 = \ldots = x_q$.

Тогда $qx_1 \equiv 1$ и $\chi(q)\,\chi(x_1) = 1$. Возводя обе части полученного равенства в степень q и вспоминая, что $q \equiv 2$ (3), получаем $\chi(q)^2\,\chi(x_1)^q = 1$, так что $\chi(x_1)^q = \chi(q)$. Таким образом, «диагональный» член в $J(\chi, \chi, \ldots, \chi)$ принимает значение $\chi(q)$. Если же не все x_i равны, то имеется q разных q-наборов, получаемых из $(x_1, \ldots, x_q)$ циклической перестановкой. Соответствующие члены в $J(\chi, \chi, \ldots, \chi)$ все имеют одинаковое значение. Таким образом,

$$J(\chi, \chi, \ldots, \chi) \equiv \chi(q)\ (q). \tag{7}$$

Объединяя равенства (5), (6) и (7), получаем

$$(p\pi)^{(q+1)/3} \equiv p\chi(q)\ (q),$$

или

$$p^{(q-2)/3}\pi^{(q+1)/3} \equiv \chi(q)\ (q).$$

Возводя обе части этого сравнения в степень $q-1$ (напомним, что $q-1 \equiv 1$ (3)), получим

$$p^{((q-2)/3)\,(q-1)}\pi^{(q^2-1)/3} \equiv \chi(q)^{(q-1)} \equiv \chi(q)\ (q).$$

Так как $p^{((q-2)/3)\,(q-1)} \equiv 1\ (q)$ по теореме Ферма и $\pi^{(q^2-1)/3} \equiv \chi_q(\pi)\ (q)$, то

$$\chi_q(\pi) \equiv \chi_\pi(q)\ (q)$$

и

$$\chi_q(\pi) = \chi_\pi(q).$$

Рассмотрим теперь случай двух примарных комплексных простых чисел π_1 и π_2. Пусть $\gamma_1 = \bar{\pi}_1$, $\gamma_2 = \bar{\pi}_2$, $p_1 = \pi_1\gamma_1$ и $p_2 = \pi_2\gamma_2$. Тогда $p_1,\ p_2 \equiv 1$ (3). По теореме 3 гл. 8

$$g(\chi_{\gamma_1})^{p_2} = J(\chi_{\gamma_1}, \ldots, \chi_{\gamma_1})\, g(\chi_{\gamma_1}^{p_2}).$$

В этой сумме Якоби p_2 членов. Так как $p_2 \equiv 1$ (3), то $\chi_{\gamma_1}^{p_2} = \chi_{\gamma_1}$. Таким образом,

$$[g(\chi_{\gamma_1})^3]^{(p_2-1)/3} = J(\chi_{\gamma_1}, \ldots, \chi_{\gamma_1}). \tag{8}$$

Выделяя диагональный член в сумме Якоби (как мы уже делали несколько раз до сих пор), получаем, что

$$J(\chi_{\gamma_1}, \ldots, \chi_{\gamma_1}) \equiv \chi_{\gamma_1}(p_2^{-1})\ (p_2) \equiv \chi_{\gamma_1}(p_2^2)\,(p_2).$$

Используя это и тот факт, что $g(\chi_{\gamma_1})^3 = p_1\gamma_1$, из равенства (8) получаем сравнение

$$\chi_{\pi_2}(p_1\gamma_1) \equiv \chi_{\gamma_1}(p_2^2)\ (\pi_2),$$

а следовательно,

$$\chi_{\pi_2}(p_1\gamma_1) = \chi_{\gamma_1}(p_2^2). \tag{9}$$

Аналогично доказывается, что

$$\chi_{\pi_1}(p_2\pi_2) = \chi_{\pi_2}(p_1^2). \tag{10}$$

Равенства (9) и (10) суть основные соотношения. Далее рассуждения проводятся точно так же, как в § 4, вплоть до искомого соотношения $\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$.

§ 6. Характер кубического вычета числа 2

Кубический закон взаимности можно использовать для развития теории кубических вычетов таким же образом, как квадратичный закон взаимности для получения результатов § 2 гл. 5. Мы откажемся от построения общей теории ради обсуждения поучительного частного случая, а именно нахождения всех простых чисел π в кольце D, для которых 2 является кубическим вычетом.

Для начала заметим, что $x^3 \equiv 2\ (\pi)$ разрешимо тогда и только тогда, когда $x^3 \equiv 2\ (\pi')$ разрешимо для всех π', ассоциированных с π. Следовательно, можно предполагать, что π примарно. Если $\pi = q$ — рациональное простое число, то $\chi_q(2) = 1$, так что 2 будет кубическим вычетом для всех таких простых чисел. Мы будем далее предполагать, что $\pi = a + b\omega$ — примарное комплексное простое число. По кубическому закону взаимности $\chi_\pi(2) = \chi_2(\pi)$. Норма для 2 равна $2^2 = 4$. Следовательно,

$$\pi = \pi^{(4-1)/3} \equiv \chi_2(\pi)\ (2).$$

Отсюда вытекает, что $\chi_\pi(2) = 1$ в том и только том случае, когда $\pi \equiv 1\ (2)$. Мы доказали

Предложение 9.6.1. *$x^3 \equiv 2\ (\pi)$ разрешимо тогда и только тогда, когда $\pi \equiv 1\ (2)$, т. е. тогда и только тогда, когда $a \equiv 1\ (2)$ и $b \equiv 0\ (2)$.*

Это предложение можно сформулировать по-другому. Пусть $\pi = a + b\omega$ — примарное комплексное простое число и $p = N\pi = a^2 - ab + b^2$. Тогда $4p = (2a - b)^2 + 3b^2$. Если положить $A = 2a - b$ и $B = b/3$, то $4p = A^2 + 27B^2$. Согласно предложению 8.3.2, целые числа A и B определены однозначно с точностью до знака.

Предложение 9.6.2. *Если $p \equiv 1\ (3)$, то $x^3 \equiv 2\ (p)$ разрешимо в том и только том случае, когда существуют такие целые числа C и D, что $p = C^2 + 27D^2$.*

Доказательство. Если сравнение $x^3 \equiv 2\ (p)$ разрешимо, то разрешимо и сравнение $x^3 \equiv 2\ (\pi)$, а следовательно, $\pi \equiv 1\ (2)$ по предложению 9.6.1. Мы имеем

$$4p = A^2 + 27B^2, \text{ где } A = 2a - b,\ B = b/3.$$

Так как b четно, то четны B и A. Пусть $D = B/2$ и $C = A/2$. Тогда $p = C^2 + 27D^2$.

Обратно, предположим, что $p = C^2 + 27D^2$. Тогда $4p = (2C)^2 + 27(2D)^2$. Из однозначности получаем, что $B = \pm 2D$, т. е. B четно, а следовательно, четным будет и b. Отсюда следует, что $\pi = a + b\omega \equiv 1$ (2) и $x^3 \equiv 2$ (π) разрешимо. Так как $D/\pi D$ содержит $p = N\pi$ элементов, то существует такое целое число h, что $h^3 \equiv 2$ (π). Теперь нетрудно показать, что $h^3 \equiv 2$ (p). Если $\pi \mid h^3 - 2$, то $\bar{\pi} \mid h^3 - 2$ и $\pi\bar{\pi} = p \mid (h^3 - 2)^2$. Следовательно, $p \mid h^3 - 2$, и предложение доказано. □

В качестве примера рассмотрим $p = 7$. Тогда $x^3 \equiv 2$ (7) неразрешимо, так как очевидно, что не существует целых чисел C и D, для которых $7 = C^2 + 27D^2$.

С другой стороны, $p = 31 = 2^2 + 27 \cdot 1^2$. Следовательно, $x^3 \equiv 2$ (31) разрешимо. Действительно, $4^3 \equiv 2$ (31).

§ 7. Биквадратичный закон взаимности: предварительные сведения

В своем втором мемуаре (1832 г.) о биквадратичных вычетах Гаусс сформулировал (без доказательства) биквадратичный закон взаимности. Он писал, что доказательство этого закона является одной из тайн высшей арифметики. Детали доказательства должны были быть опубликованы в третьем мемуаре, который, к сожалению, не появился в печати.

Позже (1844 г.) несколько доказательств с использованием сумм Якоби и Гаусса опубликовал Эйзенштейн. Основная идея та же самая, что и в кубическом случае, хотя детали доказательств более громоздки. Использование сумм Гаусса для доказательства законов взаимности восходит к самому Гауссу, который существенно использовал их в своем шестом доказательстве квадратичного закона взаимности.

На протяжении следующих трех параграфов D обозначает кольцо $\mathbf{Z}[i]$ целых гауссовых чисел. Если $\alpha \in D$, то $(\alpha) = \alpha D$ есть главный идеал, порожденный α. Под простым числом будет всегда иметься в виду положительное простое число в $\mathbf{Z}$. Напомним, что D — евклидово кольцо (гл. 1). Следовательно, если π неразложим и $\pi \mid \alpha\beta$, то либо $\pi \mid \alpha$, либо $\pi \mid \beta$. Если $N(\alpha) = \alpha\bar{\alpha}$ — норма числа α, то, согласно упр. 32 гл. 1, $N(\alpha) = 1$ тогда и только тогда, когда α — единица. Отсюда следует, что единицами в D будут ± 1, $\pm i$.

Лемма 1. *Если π неразложим, то существует такое простое число $p \in \mathbf{Z}$, что $\pi \mid p$.*

Доказательство. $N(\pi) = \pi\bar{\pi} = n = p_1 \dots p_s$, p_i — простые числа, $p_i \in \mathbf{Z}$. Тогда $\pi \mid p_i$ при некотором i. □

Следовательно, все неразложимые числа находятся разложением в D всех чисел, простых в $\mathbf{Z}$. Будет полезна следующая лемма.

Лемма 2. *Если $\alpha \in D$ и $N(\alpha)$ — простое число, то α неразложимо.*

Доказательство. Если $\alpha = \mu\lambda$, то $N(\alpha) = N(\mu)\,N(\lambda)$. Так как $N(\alpha)$ — простое число, отсюда следует, что $N(\mu) = 1$ или $N(\lambda) = 1$. Значит, одно из чисел μ или λ будет единицей.

Лемма 3. *Число $1 + i$ неразложимо и $2 = -i(1 + i)^2$ — разложение на простые множители числа 2 в D.*

Доказательство. $N(1 + i) = 2$, и поэтому первое утверждение следует из леммы 2. Второе утверждение проверяется прямым вычислением. □

Лемма 4. *Если $q \equiv 3\ (4)$ — простое число в $\mathbf{Z}$, то q неразложимо в D.*

Доказательство. Если бы q было разложимо в D, то $q = \alpha\beta$, причем $N(\alpha) > 1$ и $N(\beta) > 1$. Переходя к нормам, получим $q^2 = N(\alpha)\,N(\beta)$. Отсюда следует, что $q = N(\alpha)$. Если $\alpha = a + bi$, где $a, b \in \mathbf{Z}$, то $q = a^2 + b^2$. Получается противоречие, ибо сумма двух квадратов в $\mathbf{Z}$ сравнима с 0 или 1 по модулю 4, а q сравнимо с 3 по модулю 4.

Лемма 5. *Если p — простое число, $p \equiv 1\ (4)$, то существует такое неразложимое число π, что $p = \pi\bar{\pi}$. Кроме того, $(\pi) \neq (\bar{\pi})$.*

Доказательство. Первое утверждение совпадает с п. (а) предложения 8.3.1. Другое доказательство, не использующее сумм Якоби, следующее. Так как $p \equiv 1\ (4)$, то, согласно предложению 5.1.2, существует целое число a с $a^2 \equiv -1\ (p)$. Следовательно, $p \mid a^2 + 1 = (a + i)(a - i)$. Если бы p было неразложимым, то $p \mid a + i$, что невозможно. Таким образом, $p = \alpha\beta$, $N(\alpha) > 1$, $N(\beta) > 1$. Взятие нормы приводит к заключению, что $p = N(\alpha)$. Так как $N(\alpha)$ — простое число, из леммы 2 следует, что α неразложим. Утверждение о том, что $(\alpha) \neq (\bar{\alpha})$, предлагается проверить в качестве упражнения. □

Это завершает описание неразложимых чисел в кольце D.

Определение. Число $\alpha \in D$, не являющееся единицей (в дальнейшем мы будем называть такие элементы неединицами), называется *примарным*, если $\alpha \equiv 1$ $((1+i)^3)$.

Лемма 6. *Неединица α примарна тогда и только тогда, когда* $a \equiv 1$ (4), $b \equiv 0$ (4) *или* $a \equiv 3$ (4), $b \equiv 2$ (4).

Доказательство. Так как $(1+i)^3 = 2i(1+i)$, то $a+bi$ примарно в том и только том случае, когда

$$\frac{a-1+bi}{2+2i} = \frac{a+b-1}{4} + \frac{b-a+1}{4}, \quad i \in D.$$

Это эквивалентно справедливости сравнений $a+b \equiv 1$ (4), $a-b \equiv 1$ (4). Отсюда легко получается доказываемый результат. □

Заметим, что любая неединица $\alpha \equiv 1$ (4) в D примарна. Кроме того, если α примарно, то $(1+i) \nmid \alpha$. Если q — вещественное простое число в $\mathbf{Z}$, $q \equiv 3$ (4), то $-q$ примарно и неразложимо. Относительно неразложимых чисел, возникающих из простых чисел $p \equiv 1$ (4), имеет место следующий важный результат.

Лемма 7. *Пусть $\alpha \in D$ — неединица, $(1+i) \nmid \alpha$. Тогда существует единственная единица u, для которой $u\alpha$ примарно.*

Доказательство. Существует единица ε, для которой $\varepsilon\alpha = a+bi$, где a нечетно и b четно. Умножая, если нужно, это равенство на -1, из леммы 6 выводим, что α имеет примарное ассоциированное число. Если u_1 и u_2 — такие единицы, что $u_1\alpha$ и $u_2\alpha$ примарны, то из $(1+i) \nmid \alpha$ следует, что $u_1 \equiv u_2$ $((1+i)^3)$. Рассмотрение всех случаев показывает, что $u_1 = u_2$. □

Лемма 8. *Примарный элемент может быть записан в виде произведения примарных неразложимых элементов.*

Доказательство. Пусть $\alpha \in D$ примарно. Тогда существуют такие рациональные простые числа $q_i \equiv 3$ (4), примарные неразложимые π_i, $N(\pi_i) \equiv 1$ (4), и единица u, что $\alpha = u\pi_1 \ldots \pi_t(-q_1)\ldots(-q_s)$. Приведение по модулю $(1+i)^3$ показывает, что $1 \equiv u$ $((1+i)^3)$. Это означает, что $u = 1$. □

§ 8. Символ вычета степени 4 [1])

Рассмотрим некоторый неразложимый элемент π в D.

[1]) В дальнейшем используются также выражения «символ биквадратичного вычета», «характер биквадратичного вычета», «характер вычета степени 4». — *Прим. ред.*

Предложение 9.8.1. *Кольцо классов вычетов $D/\pi D$ является полем, состоящим из $N(\pi)$ элементов.*

Доказательство. Оно проводится точно так же, как в предложении 9.2.1, с заменой классификации неразложимых элементов в $\mathbf{Z}[\omega]$ на соответствующую классификацию в $D = \mathbf{Z}[i]$. □

Следствие. *Если* $\pi \nmid \alpha$, *то* $\alpha^{N(\pi)-1} \equiv 1 \ (\pi)$.

Предложение 9.8.2. *Если* $\pi \nmid \alpha$, $(\pi) \neq (1+i)$, *то существует единственное целое число* j, $0 \leqslant j \leqslant 3$, *для которого*

$$\alpha^{(N(\pi)-1)/4} \equiv i^j \ (\pi).$$

Доказательство. Нетрудно убедиться в том, что классы вычетов чисел $1, -1, i, -i$ различны. Они являются корнями сравнения $x^4 \equiv 1 \ (\pi)$. Но класс вычетов элемента $\alpha^{(N(\pi)-1)/4}$ тоже является решением сравнения $x^4 \equiv 1 \ (\pi)$ согласно предыдущему следствию. Отсюда и вытекает доказываемый результат.

Определение. Если π неразложим, $N(\pi) \neq 2$, то *характер биквадратичного вычета* элемента α для $\pi \nmid \alpha$ определяется посредством формулы $\chi_\pi(\alpha) = i^j$, где j берется из предложения 9.8.2. Если $\pi \mid \alpha$, то $\chi_\pi(\alpha) = 0$.

Предложение 9.8.3. (a) *Если* $\pi \nmid \alpha$, *то*

$\chi_\pi(\alpha) = 1 \Leftrightarrow$ *сравнение* $x^4 \equiv \alpha \ (\pi)$ *имеет решение в* D;

(b) $\chi_\pi(\alpha\beta) = \chi_\pi(\alpha)\chi_\pi(\beta)$;

(c) $\overline{\chi_\pi(\alpha)} = \chi_{\bar\pi}(\bar\alpha)$;

(d) *если число* π *примарно и неразложимо, то* $\chi_\pi(-1) = (-1)^{(a-1)/2}$, *где* $\pi = a + bi$;

(e) *если* $\alpha \equiv \beta \ (\pi)$, *то* $\chi_\pi(\alpha) = \chi_\pi(\beta)$;

(f) $\chi_\pi(\alpha) = \chi_\lambda(\alpha)$, *если* $(\pi) = (\lambda)$.

Доказательство. Пункт (a) следует из предложения 7.1.2. Пункты (b), (c), (e) и (f) следуют непосредственно из определения. Пункт (d) вытекает из леммы 6 (см. упр. 38). □

Предложение 9.8.4. *Пусть* q — *простое число,* $q \equiv 3 \ (4)$. *Тогда* $\chi_q(a) = 1$ *для* $a \in \mathbf{Z}$, $q \nmid a$.

Доказательство. $N(q) = q^2$. Следовательно,

$$\chi_q(a) \equiv a^{(q^2-1)/4} \ (q) = \left(a^{q-1}\right)^{(q+1)/4} \equiv 1 \ (q),$$

согласно малой теореме Ферма. □

Характер биквадратичного вычета обобщается следующим образом.

Определение. Пусть $\alpha \in D$ — такая неединица, что $(1+i) \nmid \alpha$, и $\beta \in D$. Запишем $\alpha = \prod_i \lambda_i$, где λ_i неразложимы. Если $(\alpha, \beta) = 1$, определим $\chi_\alpha(\beta)$ формулой

$$\chi_\alpha(\beta) = \prod_i \chi_{\lambda_i}(\beta).$$

Согласно предложению 9.8.3 (f), это определение корректно. Из п. (e) этого предложения следует, что если $\beta \equiv \gamma\ (\alpha)$, то $\chi_\alpha(\beta) = \chi_\alpha(\gamma)$.

Предложение 9.8.5. *Пусть* $\alpha \in \mathbf{Z}$, $\alpha \neq 0$, *и* $a \in \mathbf{Z}$ *нечетно и не равно* ± 1. *Если* $(a, \alpha) = 1$, *то*

$$\chi_\alpha(\alpha) = 1.$$

Доказательство. Можно считать, что $a > 0$. Запишем $a = \prod p_i \prod q_i$, где p_i, q_i — простые числа, $p_i \equiv 1\ (4)$, $q_i \equiv 3\ (4)$. В силу предложения 9.8.4 нам следует проверить лишь, что $\chi_{p_i}(\alpha) = 1$. Если $p_i = \pi\bar{\pi}$, где π неразложимо, то $\chi_{p_i}(\alpha) = \chi_\pi(\alpha)\,\chi_{\bar{\pi}}(\alpha) = \chi_\pi(\alpha)\,\overline{\chi_\pi(\alpha)} = 1$ в силу предложения 9.8.3 (c).

Предложение 9.8.6. *Если* $n \neq 1$ — *целое число,* $n \equiv 1\ (4)$, *то* $\chi_n(i) = (-1)^{(n-1)/4}$.

Доказательство. Заметим, что n может быть отрицательным. Если n — положительное простое число $p \equiv 1\ (4)$, то, записывая $p = \pi\bar{\pi}$, получаем

$$\chi_p(i) = \chi_\pi(i)\,\chi_{\bar{\pi}}(i) = \left(i^{(p-1)/4}\right)^2 = (-1)^{(p-1)/4}.$$

Если, с другой стороны, $n = -q$, причем q — простое число, $q \equiv 3\ (4)$, то $\chi_{-q}(i) = i^{(q^2-1)/4} = \left(i^{q-1}\right)^{(q+1)/4} = (-1)^{(-q-1)/4}$. Если $n \equiv 1\ (4)$ произвольно, то можно записать

$$n = p_1 \ldots p_t(-q_1) \ldots (-q_s),\ p_i \equiv 1\ (4),\ q_i \equiv 3\ (4).$$

Тогда наш результат следует из упр. 44.

§ 9. Биквадратичный закон взаимности

Общий биквадратичный закон взаимности может быть сформулирован следующим образом. Пусть λ и π — взаимно простые примарные элементы в D. Тогда имеет место

Теорема 2. $\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{((N(\lambda)-1)/4)((N(\pi)-1)/4)}$.

Если λ и π примарны и $\lambda = c + di$, $\mu = a + bi$, нетрудно убедиться в том, что числа $((a-1)/2)((c-1)/2)$ и $((N(\pi)-1)/4)((N(\lambda)-1)/4)$ имеют одинаковую четность, так что можно написать

$$\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{((a-1)/2)((c-1)/2)}.$$

Другими словами, если хотя бы одно из π и λ сравнимо с 1 по модулю 4, то π и λ соответствует один и тот же биквадратичный характер. Если же они оба сравнимы с $3 + 2i$ (см. лемму 6), то π и λ имеют «противоположные» характеры в том смысле что $\chi_\pi(\lambda) = -\chi_\lambda(\pi)$.

Рассмотрим примарное неразложимое число π с $N(\pi) = p \equiv 1\ (4)$, и пусть χ_π — соответствующий характер вычета степени 4. Тогда χ_π можно рассматривать как мультипликативный характер конечного поля $D/\pi D = F$. Напомним, что F — конечное поле из p элементов, состоящее из классов вычетов чисел $0, 1, \ldots, p-1$. Если $\zeta = e^{2\pi i/p}$, то пусть $g(\chi_\pi) = \sum_{i \in F} \chi_\pi(i)\,\zeta^i$ — сумма Гаусса, соответствующая χ_π. Если $\psi = \chi_\pi^2$, то ψ — нетривиальный характер порядка 2 на F и, следовательно, совпадает с символом Лежандра.

Предложение 9.9.1. $J(\chi_\pi, \chi_\pi) = \chi_\pi(-1)\,J(\chi_\pi, \psi)$.

Доказательство. В силу теоремы 1 из гл. 8 $J(\chi_\pi, \chi_\pi) = g(\chi_\pi)^2/g(\psi)$. Таким образом,

$$J(\chi_\pi, \chi_\pi)^2 = \frac{g(\chi_\pi)^4}{g(\psi)^2} = \chi_\pi(-1)\,J(\chi_\pi, \chi_\pi)\,J(\chi_\pi, \psi),$$

если воспользоваться предложениями 6.3.2 и 8.3.3. Это и дает доказываемый результат. □

Предложение 9.9.2. $g(\chi_\pi)^4 = pJ(\chi_\pi, \chi_\pi)^2$.

Доказательство непосредственно следует из предложений 9.9.1 и 8.3.3. □

Предложение 9.9.3. *Число* $-\chi_\pi(-1)J(\chi_\pi, \chi_\pi)$ *примарно.*

Доказательство. Очевидно, что

$$J(\chi_\pi, \chi_\pi) = 2\sum_{t=2}^{(p-1)/2} \chi_\pi(t)\,\chi_\pi(1-t) + \chi_\rho\left(\frac{p+1}{2}\right)^2.$$

Но любая единица в D сравнима с 1 по модулю $1+i$. Кроме того, $p \equiv 1\ (2+2i)$. Наконец, $\chi_\pi((p+1)/2)^2 = (\chi_\pi(2^{-1}))^2 = \chi_\pi(2)^{-2} = \chi_\pi(2)^2 = \chi_\pi(-i(1+i)^2)^2 = \chi_\pi(-i)^2 = \chi_\pi(-1)$. Таким образом,

$$J(\chi_\pi, \chi_\pi) \equiv 2\left(\frac{p-3}{2}\right) + \chi_\pi(-1)(2+2i) \equiv -2 + \chi_\pi(-1)(2+2i).$$

Следовательно,

$$-\chi_\pi(-1)J(\chi_\pi, \chi_\pi) \equiv 2\chi_\pi(-1) - 1\ (2+2i) \equiv 1\ (2+2i),$$

так как $\chi_\pi(-1) = \pm 1$. □

В следующем предложении вычисляется примарный элемент $-\chi_\pi(-1)\,J(\chi_\pi, \chi_\pi)$.

Предложение 9.9.4. $-\chi_\pi(-1)\,J(\chi_\pi, \chi_\pi) = \pi$.

Доказательство. В силу леммы 7 из § 7 достаточно показать, что левая и правая части отличаются на единицу. Но $J(\chi_\pi, \chi_\pi) \equiv \sum_{t=1}^{p-1} t^{(p-1)/4}(1-t)^{(p-1)/4}\ (\pi)$. В силу упр. 11 из гл. 4 отсюда следует, что $J(\chi_\pi, \chi_\pi) \equiv 0\ (\pi)$. Согласно следствию теоремы 1 из гл. 8, $N(J(\chi_\pi, \chi_\pi)) = p$. Таким образом, элемент $J(\chi_\pi, \chi_\pi)$ неразложим и предложение доказано. □

Объединяя предложение 9.9.4 с предложением 9.9.2, получаем разложение на множители для $g(\chi)^4$ в D.

Предложение 9.9.5. $g(\chi_\pi)^4 = \pi^3\bar{\pi}$.

Мы докажем теперь два частных случая биквадратичного закона взаимности. Общее утверждение будет их формальным, хотя и утомительным следствием.

Предложение 9.9.6. *Пусть $q > 0$ — вещественное неразложимое число в D. Тогда*

$$\chi_\pi(-q) = \chi_q(\pi).$$

Доказательство. Так как $q \equiv 3\ (4)$, то

$$g(\chi_\pi)^q \equiv \sum_{j=1}^{p-1} \chi_\pi(j)^q \zeta^{qj}\ (q) \equiv \sum \chi_\pi^3(j)\,\zeta^{qj}\ (q) \equiv \chi_\pi(q)\,g(\bar{\chi}_\pi)\ (q).$$

Следовательно,

$$(g(\chi_\pi)^4)^{(q+1)/4} = g(\chi_\pi)^{q+1} \equiv \chi_\pi(q)\,g(\chi_\pi)\,g(\bar{\chi}_\pi)\ (q).$$

В силу замечания, следующего за предложением 8.2.2, и того факта, что $\bar{\pi} \equiv \pi^q\ (q)$ (см. упр. 45), из предложения 9.9.5 получаем

$$\pi^{[(p+3)\,(q+1)]/4} \equiv \chi_\pi(-1)\,\chi_\pi(q)\,\pi^{q+1}\ (q),$$

или

$$\pi^{(q^2-1)/4} \equiv \chi_\pi(-q)\ (q).$$

Но $\pi^{(q^2-1)/4} \equiv \chi_q(\pi)\ (q)$. Таким образом,

$$\chi_q(\pi) \equiv \chi_\pi(-q)\ (q),$$

откуда, ввиду того что обе части являются единицами, следует, что

$$\chi_q(\pi) = \chi_\pi(-q).$$

Это завершает доказательство. □

Заметим, что число $-q$ *примарно* и неразложимо, а $(N(q) - 1)/4 = (q^2 - 1)/4$ четно. Следовательно, предложение 9.9.6 в самом деле есть частный случай биквадратичного закона взаимности.

Предложение 9.9.7. *Пусть q — простое число с $q \equiv 1$ (4). Тогда $\chi_\pi(q) = \chi_q(\pi)$.*

Доказательство. Так как $q \equiv 1$ (4), то

$$g(\chi_\pi)^q \equiv \sum \chi_\pi(j)^q \zeta^{qj}\ (q) \equiv \sum \chi_\pi(j)\,\zeta^{qj}\ (q) \equiv \bar{\chi}_\pi(q)\,g(\chi_\pi)\ (q),$$

а следовательно,

$$g(\chi_\pi)^{q+3} \equiv \bar{\chi}_\pi(q)\,g(\chi_\pi)^4\ (q).$$

Ввиду предложения 9.9.5 это приводит к

$$(\pi^3\bar{\pi})^{(q+3)/4} \equiv \bar{\chi}_\pi(q)\,\pi^3\bar{\pi}\ (q).$$

Обе части этого сравнения принадлежат D и $(q, \pi) = (q, \bar{\pi}) = 1$. Таким образом, можно произвести деление и получить

$$(\pi^3)^{(q-1)/4}\bar{\pi}^{(q-1)/4} \equiv \bar{\chi}_\pi(q)\ (q).$$

Если $q = \lambda\bar{\lambda}$, где λ неразложим в D, то полученное сравнение означает, что

$$\chi_\lambda(\pi^3)\,\chi_\lambda(\bar{\pi}) \equiv \bar{\chi}_\pi(q)\ (\lambda).$$

Как и в предыдущем случае, делаем вывод о том, что

$$\chi_\lambda(\pi^3)\,\chi_\lambda(\bar{\pi}) = \bar{\chi}_\pi(q).$$

Это можно записать в виде

$$\overline{\chi_\lambda(\pi)}\,\chi_\lambda(\bar{\pi}) = \bar{\chi}_\pi(q),$$

или

$$\chi_{\bar{\lambda}}(\bar{\pi})\,\chi_\lambda(\bar{\pi}) = \bar{\chi}_\pi(q),$$

что по определению дает

$$\chi_q(\bar{\pi}) = \bar{\chi}_\pi(q).$$

Переход к сопряженным завершает доказательство.

Читателю следует обратить внимание на то, что в определении 9.9.7 q разложимо и что правая часть есть обобщенный символ биквадратичного вычета.

Следующее предложение является формальным упражнением, использующим лемму 8 из § 7 и предложения 9.8.6, 9.9.6 и 9.9.7.

Предложение 9.9.8. *Пусть a вещественно и $a \equiv 1$ (4), a λ примарно, $(\lambda, a) = 1$. Тогда $\chi_a(\lambda) = \chi_\lambda(a)$.*

Предположим теперь, что $\pi = a + bi$ и $\lambda = c + di$ примарны и взаимно просты. Мы не предполагаем, что $N(\pi) \neq N(\lambda)$ или что они неразложимы.

Предложение 9.9.9. *Если $(a, b) = 1$, $(c, d) = 1$, то*

$$\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{((a-1)/2)((c-1)/2)}.$$

Доказательство. Так как $(\pi, \lambda) = 1$, то из предположений следует, что $(a, \pi) = (b, \pi) = (c, \lambda) = (d, \lambda) = 1$. Соотношение $c\pi \equiv ac + bd$ (λ) означает, что $(ac + bd, \lambda) = (ac + bd, \pi) = 1$. Кроме того,

$$\chi_\lambda(c)\,\chi_\lambda(\pi) = \chi_\lambda(ac + bd). \tag{1}$$

Аналогично

$$\chi_\pi(a)\,\chi_\pi(\lambda) = \chi_\pi(ac + bd). \tag{2}$$

Беря сопряженное к (2) и умножая на (1), получаем соотношение

$$\chi_\lambda(c)\,\chi_{\bar{\pi}}(a)\,\chi_\lambda(\pi)\,\overline{\chi_\pi(\lambda)} = \chi_{\lambda\bar{\pi}}(ac + bd).$$

Таким образом, мы показали (следует использовать предложение 9.8.3 (c)), что

$$\chi_\lambda(\pi)\,\overline{\chi_\pi(\lambda)} = \chi_{\bar{\lambda}}(c)\,\chi_\pi(a)\,\chi_{\lambda\bar{\pi}}(ac + bd). \tag{3}$$

Предположим, что c, a и $ac + bd$ — неединицы. Три члена в правой части равенства (3) легко вычисляются. Для нечетного числа n положим $\varepsilon(n) = (-1)^{(n-1)/2}$. Тогда $\varepsilon(n)\,n \equiv 1$ (4) и $\varepsilon(ac + bd) = \varepsilon(a)\,\varepsilon(c)$, так как $bd \equiv 0$ (4). Записывая равенство $\chi_\alpha(x) =$

$= \chi_\alpha(\varepsilon(x))\,\chi_\alpha(\varepsilon(x)\,x)$ для каждого члена из правой части соотношения (3), получаем, если заметить, что $\chi_\alpha(\varepsilon(x))\quad\overline{\chi_\alpha(\varepsilon(x))}$, и воспользоваться предложениями 9.9.8 и 9.8.3 (b), равенство

$$\chi_\lambda(\pi)\,\overline{\chi_\pi(\lambda)}\quad\chi_c(\bar{\lambda})\,\chi_a(\pi)\,\chi_{ac+bd}(\lambda\bar{\pi}). \tag{4}$$

Что касается последних трех членов, то мы вычисляем их, используя предложение 9.8.6:

$$\chi_c(\bar{\lambda}) = \chi_c(c - di) \quad \chi_c(-di) = \chi_c(i),$$
$$\chi_a(\pi) \quad \chi_a(a + bi) = \chi_a(bi) = \chi_a(i),$$
$$\chi_{ac+bd}(\bar{\pi}\lambda) \quad \chi_{ac+bd}((ad \quad bc)\,i) = \chi_{ac+bd}(i).$$

Таким образом,

$$\chi_\lambda(\pi)\,\overline{\chi_\pi(\lambda)} = \chi_{(ac+bd)\,ac}(i) =$$
$$= (-1)^{((ac+bd)\,ac-1)/4} \text{ (предложение 9.8.6)} =$$
$$= (-1)^{((a-1)/2)\,((c-1)/2)}. \tag{5}$$

Последнее равенство — простое упражнение с использованием леммы 6 из § 7. Мы оставляем читателю несложную задачу рассмотреть ситуацию, когда одно из чисел a, c или $ac + bd$ является единицей (т. е. ± 1). □

Общий биквадратичный закон взаимности легко следует из предложения 9.9.9. Действительно, запишем $\pi = m\,(a + bi)$, $\lambda = n\,(c + di)$, $(\pi, \lambda) = 1$, где $m \equiv n \equiv 1$ (4), $(a, b) = 1$, $(c, d) = 1$. В силу предложения 9.9.7 $\chi_\pi(n) = \chi_n(\pi)$ и $\chi_\lambda(m) = \chi_m(\lambda)$. Кроме того, $\chi_m(n) = \chi_n(m) = 1$, в силу предложения 9.8.5. Тогда, так как числа $a + bi$ и $c + di$ примарны,

$$\chi_\lambda(\pi) = \chi_\lambda(m)\,\chi_\lambda(a + bi) =$$
$$= \chi_m(\lambda)\,\chi_n(a + bi)\,\chi_{c+di}(a + bi) =$$
$$= \chi_m(\lambda)\,\chi_{a+bi}(n)\,\chi_{a+bi}(c + di)\,(-1)^{((a-1)/2)\,((c-1)/2)} =$$
$$= \chi_\pi(\lambda)\,(-1)^{((a-1)/2)\,((c-1)/2)} =$$
$$= \chi_\pi(\lambda)\,(-1)^{((N(\pi)-1)/4)\,((N(\lambda)-1)/4)},$$

где в последнем равенстве мы воспользовались тем, что $m \equiv n \equiv 1$ (4). Это завершает доказательство, памятник изобретательности и настойчивости! □

§ 10. Рациональный биквадратичный закон взаимности

В этом параграфе всюду p и q обозначают различные простые числа, сравнимые с 1 по модулю 4. В таком случае мультиплика-

тивная группа $(\mathbf{Z}/p\mathbf{Z})^*$ имеет единственную подгруппу порядка) $(p-1)/4$, состоящую из вычетов четвертых степеней целых чисел. Рассмотрим характер биквадратичного вычета χ_π, определенный с помощью неразложимого числа π, делящего p в $\mathbf{Z}[i]$. В силу предложения 9.8.3 $\chi_\pi(q) = 1$ тогда и только тогда, когда $x^4 \equiv q\ (\pi)$ имеет решение $x \in \mathbf{Z}[i]$.

Лемма 1. *$\chi_\pi(q) = 1$ тогда и только тогда, когда $x^4 \equiv q\ (p)$ имеет решение $x \in \mathbf{Z}$.*

Доказательство. В силу предложения 9.8.1 целые числа 0, 1, 2, ..., $p-1$ образуют полную систему вычетов для классов вычетов в $\mathbf{Z}[i]$ по модулю π. Таким образом, $\chi_\pi(q) = 1$ тогда и только тогда, когда $x^4 \equiv q\ (\pi)$ имеет решение $x \in \mathbf{Z}$. Отсюда следует, что $x^4 \equiv q\ (\bar{\pi})$. Но $(\pi, \bar{\pi}) = 1$. Поэтому $p = \pi\bar{\pi} \mid x^4 - q$. □

Пусть ψ_p обозначает квадратичный характер (см. гл. 8 § 1).

Лемма 2. *Если $\psi_p(q) = 1$, то $\chi_\pi(q) = \pm 1$.*

Доказательство. Поскольку $q^{(p-1)/2} \equiv 1\ (p)$, то $\chi_\pi^2(q) \equiv \left(q^{(p-1)/4}\right)^2\ (\pi) \equiv q^{(p-1)/2}\ (\pi) \equiv 1\ (\pi)$. Следовательно, $\chi_\pi^2(q) = 1$. □

Таким образом, предполагая, что q — квадрат по модулю p, получаем, что $\chi_\pi(q)$ равно 1 или -1 в зависимости от того, будет или нет q четвертой степенью по модулю p. По квадратичному закону взаимности $\psi_q(p) = +1$. Заметим, что значение $\chi_\pi(q)$ зависит лишь от p и q, а не от выбора неразложимого π. Вопреки тому что можно ожидать, связь между двумя целыми числами $\chi_\pi(q)$ и $\chi_\lambda(p)$, где λ — неразложимое число, делящее q, не является простым следствием биквадратичного закона взаимности. В 1969 г. Бурдэ [102] открыл следующий замечательный закон взаимности. Так как p и q сравнимы с 1 по модулю 4, мы можем записать $p = a^2 + b^2$, $q = c^2 + d^2$, где $a \equiv c \equiv 1\ (2)$ и $b \equiv d \equiv 0\ (2)$. Всюду далее мы предполагаем, что $\psi_q(p) = 1$.

Теорема 3. $\chi_\pi(q)\,\chi_\lambda(p) = (-1)^{(q-1)/4}\psi_q(ad - bc)$.

Излагаемое ниже изящное доказательство принадлежит Вильямсу [244]. В нем не предполагается, что биквадратичный закон взаимности установлен, однако используется значение квадратичной суммы Гаусса (гл. 6, § 4). Следующее предложение представляет интерес и само по себе. (См. комментарии в конце § 12.)

Предложение 9.10.1. *Пусть* π — *примарное неразложимое число, делящее* p. *Тогда*

$$g(\chi_\pi)^2 = -(-1)^{(p-1)/4} \cdot p\pi,$$

где $\sqrt{p}$ *обозначает положительный квадратный корень.*

Доказательство. В силу предложения 9.9.4 и теоремы 1 из гл. 8

$$J(\chi_\pi, \chi_\pi) = -\chi_\pi(-1)\pi = \frac{g(\chi_\pi)^2}{g(\psi_p)}.$$

Наше предложение следует из теоремы 1 гл. 6 и того факта, что $\chi_\pi(-1) = (-1)^{(p-1)/4}$. □

Предложение 9.10.2. *Если* π — *примарное неразложимое число, делящее* p, *то* $\chi_\lambda(p)\chi_\pi(q) \equiv \pi^{(q-1)/2}(q)$.

Доказательство. В кольце всех целых алгебраических чисел

$$g(\chi_\pi)^q = \Big(\sum \chi_\pi(j)\zeta^j\Big)^q \equiv \sum \chi_\pi(j)\zeta^{qj}(q) \equiv$$
$$\equiv \chi_\pi(q^{-1})\, g(\chi_\pi)(q) \equiv \chi_\pi(q)\, g(\chi_\pi)(q).$$

Последнее сравнение получается потому, что

$$\chi_\pi(q^{-1}) = \chi_\pi^3(q) = \chi_\pi^2(q)\chi_\pi(q) = \chi_\pi(q).$$

Значит, умножение на $g(\chi_\pi)^3$ дает

$$g(\chi_\pi)^4 (g(\chi_\pi))^{q-1} \equiv \chi_\pi(q)\, g(\chi_\pi)^4 (q).$$

Два члена в левой части принадлежат $\mathbf{Z}[i]$, согласно предложению 8.3.3; а в силу предложения 8.2.2 $N(g(\chi_\pi)^4) = p^4$. Поэтому можно произвести сокращение на $g(\chi_\pi)^4$ и получить

$$g(\chi_\pi)^{q-1} \equiv \chi_\pi(q)(q).$$

Использование предложения 9.10.1 приводит к соотношениям

$$(g(\chi_\pi)^2)^{(q-1)/2} = p^{(q-1)/4}\pi^{(q-1)/2} \equiv \chi_\pi(q)(q).$$

Но $p^{(q-1)/4} \equiv \chi_\lambda(p)(\lambda)$. Так как обе части этого сравнения вещественны, то, беря сопряженные и используя равенство $(\lambda, \bar{\lambda}) = 1$, убеждаемся, что это сравнение выполняется по модулю q. Это завершает доказательство. □

В следующем предложении π не предполагается примарным. Запишем $\pi = a + bi$ и $\lambda = c + di$.

Предложение 9.10.3. $\pi^{(q-1)/2} \equiv \psi_q(d)\psi_q(ad - bc)(q)$.

Доказательство. Так как $d\pi \equiv ad - bc\ (\lambda)$, то

$$(d\pi)^{(q-1)/2} \equiv (ad - bc)^{(q-1)/2}\ (\lambda).$$

Таким образом,

$$\psi_q(d)\,\pi^{(q-1)/2} \equiv \psi_q(ad - bc)\ (\lambda).$$

Аналогично сравнение $d\pi \equiv (ad + bc)\ (\bar{\lambda})$ означает, что

$$\psi_q(d)\,\pi^{(q-1)/2} \equiv \psi_q(ad + bc)\ (\bar{\lambda}).$$

Доказательство получается теперь из следующей леммы. □

Лемма 3. $\psi_q(ad - bc) = \psi_q(ad + bc)$.

Доказательство. Так как $c^2 \equiv -d^2\ (q)$, то

$$\psi_q(ad - bc)\,\psi_q(ad + bc) = \psi_q(a^2d^2 - b^2c^2) = \psi_q(d^2p) = \psi_q(p) = 1.$$ □

Заметим, кроме того, что, так как $\psi_q(-1) = 1$, в качестве следствия доказанной леммы имеем $\psi_q(ad - bc) = \psi_q(-ad + bc) = \psi_q(-ad - bc)$. Таким образом, без потери общности в формулировке теоремы 3 можно предположить, что число π примарно. При этом предположении из предложений 9.10.2 и 9.10.3 получаем, что

$$\chi_\pi(q)\,\chi_\lambda(p) = \psi_q(d)\,\psi_q(ad - bc).$$

Доказательство теоремы 3 завершается следующей леммой.

Лемма 4. *Если* $q = c^2 + d^2$, $c > 0$, $c \equiv 1\ (2)$, *то* $\psi_q(d) = (-1)^{(q-1)/4}$.

Доказательство. Пусть ψ_c обозначает символ Якоби. Тогда в силу предложения 5.2.2 имеем $\psi_q(c) = \psi_c(q) = \psi_c(d^2) = 1$. (Ср. упр. 26 из гл. 5.) Но из $c^2 \equiv -d^2\ (q)$ следует, что $c^{(q-1)/2} \equiv (-1)^{(q-1)/4}\,d^{(q-1)/2}\ (q)$. Таким образом, $\psi_q(c) = 1 = (-1)^{(q-1)/4}\,\psi_q(d)$. □

§ 11. Построение правильных многоугольников

30 марта 1796 г. Гаусс, которому тогда еще не исполнилось 19 лет, начал вести дневник, в котором он сообщал о своих открытиях. Первая его запись такова: «Principia quibus innitur sectio circuli, ac divisibilitas eiusdem geometrica in septemdecim partes, etc.» («Принципы, на которых основывается деление круга, а именно геометрическое деление на 17 частей и т. д. ...»). В более общем виде в своих «Disquisitiones Arithmeticae», § 365, Гаусс доказал, используя «круговые периоды», что если p — простое

число вида $2^n + 1$, то правильный многоугольник с p сторонами может быть построен с помощью линейки и циркуля.

В этом параграфе мы даем короткое доказательство этого результата, используя суммы Гаусса и Якоби.

Вообще возможность построения комплексных чисел в нашей ситуации означает, что они могут быть получены из $\mathbf{Q}$ конечной последовательностью рациональных операций и операций взятия квадратных корней. Более точно:

Определение. Комплексное число $\alpha \in \mathbf{C}$ *может быть построено*, если существуют такие подполя $\mathbf{Q} = K_0 \subset K_1 \subset \ldots \subset K_n$ в $\mathbf{C}$, что $\alpha \in K_n$ и $K_i = K_{i-1}(\sqrt{\alpha_i})$ для некоторого $\alpha_i \in K_{i-1}$, $i = 1, \ldots, n$.

Здесь $K(\sqrt{\beta})$ обозначает поле всех комплексных чисел $a + b\sqrt{\beta}$, $a, b \in K$ (см. упр. 6 из гл. 6). Легко видеть, что α может быть построено тогда и только тогда, когда вещественная и мнимая части числа α могут быть построены. Кроме того, если α может быть построено, то может быть построено и число $\sqrt{\alpha}$. Пусть, как обычно, $\zeta_t = e^{2\pi i/t}$.

Лемма 1. *ζ_{2^n} может быть построено*, $n = 1, 2, \ldots$.

Доказательство. Так как $(\zeta_{2^n})^2 = \zeta_{2^{n-1}}$, этот результат получается по индукции (ζ_2, конечно, может быть построено).

Лемма 2.

$$\sum_{\chi} \chi(t) = \begin{cases} 1, & \text{если } t = 0, \\ p - 1, & \text{если } t = 1, \\ 0, & \text{если } t \neq 0, 1, \end{cases}$$

где сумма берется по всем характерам группы F_p^*.

Доказательство. Если $\chi = \varepsilon$ — тривиальный характер, то $\varepsilon(0) = 1$. Поэтому результат верен для $t = 0$. Он верен также для $t = 1$, в силу предложения 8.1.3, а оставшийся случай есть следствие предложения 8.1.3. □

Напомним, что простое число Ферма есть простое число вида $2^n + 1$.

Теорема 4. *Если p — простое число Ферма, то ζ_p может быть построено.*

Доказательство. Если $g(\chi) = \sum_{t=0}^{p-1} \chi(t)\,\zeta_p^t$ — сумма Гаусса, соответствующая χ, то

$$\sum_{\chi} g(\chi) = \sum_{t=0}^{p-1} \Big(\sum_{\chi} \chi(t)\Big)\,\zeta_p^t = 1 + (p-1)\,\zeta_p.$$

Таким образом, $\zeta_p = (p-1)^{-1}\Big(-1 + \sum_{\chi} g(\chi)\Big)$, а потому ζ_p может быть построено, если может быть построено каждое $g(\chi)$.

Но $p - 1 = 2^n$. Так как характеры образуют группу порядка $p - 1$, мы видим, что порядок χ есть 2^m для некоторого m. Воспользовавшись предложением 8.3.3, получаем тогда $g(\chi)^{2^m} = \chi(-1)\,pJ(\chi, \chi)\,J(\chi, \chi^2)\ldots J(\chi, \chi^l)$, где $l = 2^m - 2$. Но $J(\chi, \chi^i) \in \mathbf{Z}[\zeta_{2^n}]$, так что по лемме 1 $g(\chi)^{2^m}$ может быть построено. Отсюда следует, что $g(\chi)$ может быть построено и доказательство окончено. □

§ 12. Кубические суммы Гаусса и проблема Куммера

Если p — простое число, сравнимое с 1 по модулю 4, то простое рассуждение из предложения 6.3.2 показывало, что $g(\chi)^2 = p$, где

$$g(\chi) = \sum_{t=1}^{p-1} \Big(\frac{t}{p}\Big)\,\zeta_p^t = \sum_{t=0}^{p-1} \zeta_p^{t^2} = \sum_{t=0}^{p-1} \cos\frac{2\pi t^2}{p}$$

— классическая квадратичная сумма Гаусса. Таким образом, мы без особого труда показали, что $g(\chi)$ является одним из вещественных корней уравнения $x^2 - p = 0$. Используя более сложные рассуждения, мы показали в § 6 гл. 6, что на самом деле $g(\chi)$ всегда будет бóльшим корнем, т. е. $g(\chi) = \sqrt{p}$.

В случае кубических сумм Гаусса обсуждаемый вопрос более тонок. Пусть p — простое число, сравнимое с 1 по модулю 3, и рассмотрим $\sum_{t=0}^{p-1} \cos(2\pi t^3/p) = G$. Запишем $p = \pi\bar{\pi}$, где π — комплексное примарное простое число в $\mathbf{Z}[\omega]$, и пусть χ_π — кубический характер, соответствующий π, как это определено в § 3.

Лемма 1. $G = g(\chi_\pi) + \overline{g(\chi_\pi)}$.

Доказательство. Если $\zeta = e^{2\pi i/p}$, то, так как G вещественно и $-1 = (-1)^3$,

$$G = \sum_{t=0}^{p-1} \zeta^{t^3} = \sum_{t=0}^{p-1} \zeta^t (1 + \chi_\pi(t) + \chi_\pi(t^2)) = g(\chi_\pi) + g(\chi_\pi^2) =$$

$$= g(\chi_\pi) + g(\bar{\chi}_\pi) = g(\chi_\pi) + \chi_\pi(-1)\,\overline{g(\chi_\pi)} = g(\chi_\pi) + \overline{g(\chi_\pi)}. \quad \square$$

Заметим, что в приведенном выше доказательстве χ может быть любым характером порядка 3. Однако в следующей лемме выбор χ_π существен. Запишем $\pi = a + b\omega$.

Лемма 2. *G является вещественным корнем уравнения* $x^3 - 3px - (2a - b)\,p = 0$.

Доказательство. В силу леммы 1, заменяя χ_π на χ, получаем

$$G^3 = g(\chi)^3 + \overline{g(\chi)^3} + 3g(\chi)\,\overline{g(\chi)}\,(g(\chi) + \overline{g(\chi)}) =$$
$$= p\pi + p\bar{\pi} + 3pG = 3pG + p(2a - b).$$

На втором шаге мы воспользовались следствием леммы 1 из § 4. $\square$

Следствие. *G является корнем уравнения* $x^3 - 3px - Ap = 0$, *где* $4p = A^2 + 27B^2$, $A \equiv 1\ (3)$.

Доказательство. Это утверждение есть простое следствие предложения 8.3.4. $\square$

Таким образом, G одновременно является вещественной частью $g(\chi_\pi)$ и корнем многочлена $x^3 - 3px - Ap$. Так же как и выше, убеждаемся в том, что другими корнями будут $2\mathrm{Re}\,(\omega g(\chi_\pi))$ и $2\mathrm{Re}\,(\omega^2 g(\chi_\pi))$. Используя тот факт, что $|g(\chi_\pi)| = p^{1/2}$, нетрудно получить, что каждый интервал $(-2\sqrt{p},\ -\sqrt{p})$, $(-\sqrt{p},\ \sqrt{p})$ и $(\sqrt{p},\ 2\sqrt{p})$ содержит точно один корень (см. упр. 43). По следствию леммы 1 из § 4 значение $g(\chi_\pi)$ определено с точностью до 1, ω или ω^2. Не сумев найти выражения для этого корня из 1 для p общего вида, Куммер предложил произвести статистическое изучение распределения тех простых чисел, для которых G, скажем, равно наибольшему корню многочлена $x^3 - 3px - Ap$. Он обнаружил, например, что среди простых чисел <500 G лежит в интервале $(\sqrt{p},\ 2\sqrt{p})$ для 24 простых чисел. Интервал $(-2\sqrt{p},\ -\sqrt{p})$ отвечает 7 простым числам, а средний интервал — 14 простым числам. (См. [164], т. 1, с. 50, 296, 353.) Полагая $I_1 = (-2\sqrt{p},\ -\sqrt{p})$, $I_2 = (-\sqrt{p},\ \sqrt{p})$, $I_3 = (\sqrt{p},\ 2\sqrt{p})$ и обозначая через $N_j(B)$ число простых чисел $\leqslant B$, для которых G

лежит в I_j, он заметил, что отношение $N_1(500) : N_2(500) : N_3(500)$ приближенно равно $1 : 2 : 3$.

Однако в 1953 г. фон Нейман и Гольдштейн, рассматривая все простые числа ($\equiv 1$ (3)), меньшие 9973, пришли к приближенному отношению $2 : 3 : 4$ [197]. В их вычислениях $N_1(10^4) = 138$, $N_2(10^4) = 201$, $N_3(10^4) = 272$. Они писали: «Эти результаты, по-видимому, указывают на значительное отклонение от предполагаемой плотности и на тенденцию к случайности». Эмма Хемер расширила вычисления до первых 1000 простых чисел p, $p \equiv 1$ (3), и получила приближенное отношение $3 : 4 : 5$ [176]. Таким образом, возникает подозрение, что значения G располагаются по трем интервалам асимптотически равномерно. Что это действительно так, установили в 1978 г. Хис-Браун и Паттерсон в статье [147] [1]).

Упомянем, что Касселс [108] высказал гипотезу по поводу точного выражения для $g(\chi_\pi)$ через эллиптические функции. Эта гипотеза была доказана Мэттьюзом [186]. Он же нашел явное элементарное выражение для биквадратичной суммы Гаусса. Результат Мэттьюза формулируется следующим образом. Пусть p — простое число, $p \equiv 1$ (4); запишем $p = \pi\bar{\pi}$, π примарно, $\pi = a + bi$. Определим $\beta = \pm i$ посредством сравнения $((p - 1)/2)! \equiv \beta(\pi)$. Если $g(\chi_\pi)$ — биквадратичная сумма Гаусса, соответствующая χ_π, то в силу предложения 9.10.1 $g(\chi_\pi)^2 = -(-1)^{(p-1)/4}\pi\sqrt{\bar{p}}$. Таким образом, $g(\chi_\pi) = \varepsilon\sqrt{-(-1)^{(p-1)/4}\pi\sqrt{\bar{p}}}$, где квадратный корень имеет положительную вещественную часть. Мэттьюз доказал, что $\varepsilon = -\beta\chi_\pi(2i)(2 \mid b \mid/a)$, где $(2 \mid b \mid/a)$ — символ Якоби. См. также [182] и [93].

Замечания

По поводу ранней истории кубического и биквадратичного законов взаимности заметим, что Эйлер в 1748—1750 гг. выдвигал в качестве гипотезы предложение 9.6.2 относительно характера кубического вычета числа 2, а также аналогичные результаты для целых чисел 3, 5 и 7. Он также высказал гипотезу о том, что 2 — четвертая степень по модулю p, $p \equiv 1$ (4), тогда и только тогда, когда $p = a^2 + 64b^2$ (упр. 6 гл. 5), и сформулировал аналогичные результаты для простых чисел 3 и 5. Все эти гипотезы Эйлера относительно частных случаев закона взаимности оказались верными — замечательный пример его «индуктивного» чутья. Произвольный характер биквадратичного вычета числа 2 (упр. 37) был получен Гауссом в его первом мемуаре о биквадратичных

[1]) Обзор этих и других результатов по проблеме Куммера см. в [9*]. — *Прим. ред.*

вычетах (1828 г.), в то время как общий биквадратичный закон взаимности был сформулирован в его втором мемуаре на ту же самую тему (1832 г.). Дальнейшие комментарии по истории этих результатов см. в статье [116].

В 1846 г. Гаусс писал Александру фон Гумбольдту, что такой математический талант, как у Эйзенштейна, природа дарует немногим в каждом столетии. К 1844 г., когда ему исполнился 21 год, Эйзенштейн опубликовал в совокупности 25 статей в журнале Крелля. В них содержатся как доказательства кубического и биквадратичного законов взаимности из этой главы, так и доказательства квадратичного закона взаимности из гл. 6 (см. [28], [130], [131]). Теперь доступно полное собрание сочинений этого выдающегося ученого, умершего в возрасте 29 лет. Насыщенное информацией превосходное описание жизни и исследований Эйзенштейна имеется в обзоре А. Вейля этого собрания сочинений [239]. Стоит познакомиться также с замечательной статьей Вейля [238]. В одной из следующих глав мы докажем обобщение этих законов взаимности, знаменитый закон взаимности Эйзенштейна. Обсуждение других доказательств Эйзенштейна биквадратичного закона взаимности содержится в [72]. Что касается кубического закона взаимности, то Якоби утверждал, что приводил его доказательство в своих лекциях в 1837 г., однако первое опубликованное доказательство 1844 г. безусловно принадлежит Эйзенштейну. Споры о приоритете были довольно ожесточенными.

О фактическом построении 17-угольника см. [40], с. 61. Теория деления круга излагается Гауссом в разд. VII его «Disquisitiones Arithmeticae» [136]. В § 335 он упоминает, что разработанную технику можно перенести на другие трансцендентные функции, например трансцендентные функции, связанные с $\int dx/\sqrt{1-x^4}$, интегралом, выражающим длину лемнискаты. В своем дневнике от 21 марта 1797 г. Гаусс записал, что ему удалось разделить дугу лемнискаты на пять равных частей. В 1827 г. Абель смог показать, что, как и в случае круга, дуга лемнискаты может быть разделена на p равных частей с помощью циркуля и линейки, если p — простое число Ферма. Рассмотрение доказательства Абеля с современной точки зрения имеется в [212].

В последнее время возродился интерес к рациональным законам взаимности. Заинтересованному читателю следует обратиться к обзорной статье [175], а также к статье [181].

Упражнения

1. Показать, что если $\alpha \in \mathbf{Z}[\omega]$, то α сравнимо с 0, 1 или -1 по модулю $1-\omega$.

2. Положим $D = \mathbf{Z}[\omega]$ и $\lambda = 1 - \omega$. Показать, что если $\mu \in D$, то можно записать $\mu = (-1)^a \omega^b \lambda^c \pi_1^{a_1} \pi_2^{a_2} \dots \pi_t^{a_t}$, где a, b, c и a_i — неотрицательные целые числа и π_i — примарные простые числа.

3. Пусть γ — примарное простое число. Как мы видели в упр. 2, чтобы вычислить $\chi_\gamma(\mu)$, достаточно вычислить $\chi_\gamma(-1)$, $\chi_\gamma(\omega)$, $\chi_\gamma(\lambda)$ и $\chi_\gamma(\pi)$, где π — примарное простое число. Так как $-1 = (-1)^3$, то $\chi_\gamma(-1) = 1$. Рассмотрим теперь $\chi_\gamma(\omega)$. Пусть $\gamma = a + b\omega$, и положим $a = 3m - 1$ и $b = 3n$. Показать, что $\chi_\gamma(\omega) = \omega^{m+n}$.

4 (продолжение). Показать, что $\chi_\gamma(\omega) = 1$, ω или ω^2 в зависимости от того, сравнимо γ с 8, 2 или 5 по модулю 3λ. В частности, если q — рациональное простое число, $q \equiv 2$ (3), то $\chi_q(\omega) = 1$, ω или ω^2 в зависимости от того, будет $q \equiv 8$, 2 или 5 (9). [*Указание.* $\gamma = a + b\omega = -1 + 3(m + n\omega)$, так что $\gamma \equiv -1 + 3(m + n)$ (3λ).]

5. В основном тексте мы сформулировали результат Эйзенштейна о том, что $\chi_\gamma(\lambda) = \omega^{2m}$. Показать, что $\chi_\gamma(3) = \omega^{2n}$.

6. Доказать, что

(a) $\chi_\gamma(\lambda) = 1$ для $\gamma \equiv 8$, $8 + 3\omega$, $8 + 6\omega$ (9);

(b) $\chi_\gamma(\lambda) = \omega$ для $\gamma \equiv 5$, $5 + 3\omega$, $5 + 6\omega$ (9);

(c) $\chi_\gamma(\lambda) = \omega^2$ для $\gamma \equiv 2$, $2 + 3\omega$, $2 + 6\omega$ (9).

7. Найти примарные простые числа, ассоциированные с $1 - 2\omega$, $-7 - 3\omega$ и $3 - \omega$.

8. *Разложить следующие числа на простые множители в* D: 7, 21, 45, 22 и 143.

9. Показать, что $\tilde{\alpha}$, класс вычетов числа α, является кубом в поле $D/\pi D$ тогда и только тогда, когда $\alpha^{(N\pi-1)/3} \equiv 1$ (π). Вывести отсюда, что в $D/\pi D$ существует $(N\pi - 1)/3$ кубов.

10. Каково разложение на простые множители многочлена $x^{24} - 1$ в $D/5D$?

11. Сколько кубов имеется в $D/5D$?

12. Показать, что $\omega\lambda$ имеет порядок 8 в $D/5D$ и что $\omega^2\lambda$ имеет порядок 24. [*Указание. Сначала показать, что* $(\omega\lambda)^2$ *имеет порядок* 4.]

13. Показать, что π — куб в $D/5D$ тогда и только тогда, когда $\pi \equiv 1$, 2, 3, 4, $1 + 2\omega$, $2 + 4\omega$, $3 + \omega$ или $4 + 3\omega$ (5).

14. Для каких простых $\pi \in D$ разрешимо сравнение $x^3 \equiv 5$ (π)?

15. Предположим, что $p \equiv 1$ (3) и что $p = \pi\bar{\pi}$, где π — примарное простое число в D. Показать, что сравнение $x^3 \equiv a$ (p) разрешимо в $\mathbf{Z}$ в том и только том случае, когда $\chi_\pi(a) = 1$. Предполагается, что $a \in \mathbf{Z}$.

16. Разрешимо ли сравнение $x^3 \equiv 2 - 3\omega$ (11)? Так как $D/11D$ имеет 121 элемент, ответить на этот вопрос прямым вычислением затруднительно. Дополнить детали следующего доказательства того, что оно неразрешимо. Имеем $\chi_\pi(2 - 3\omega) = \chi_{2-3\omega}$ (11), так что наше сравнение обладает решением тогда *и только тогда, когда* $x^3 \equiv 11$ $(2 - 3\omega)$ *разрешимо. Это сравнение разрешимо* в том и только том случае, когда $x^3 \equiv 11$ (7) разрешимо в $\mathbf{Z}$. Но $x^3 \equiv a$ (7) *разрешимо в* $\mathbf{Z}$ *тогда и только тогда, когда* $a \equiv 1$ *или* 6 (7).

17. Элемент $\gamma \in D$ называется *примарным*, если $\gamma \equiv 2$ (3). Показать, что если γ и ρ примарны, то $-\gamma\rho$ примарен. Если γ примарен, то показать, что $\gamma = \pm\gamma_1\gamma_2 \dots \gamma_t$, где γ_i суть (не обязательно разные) примарные простые числа.

18 (продолжение). Если $\gamma = \pm\gamma_1\gamma_2 \dots \gamma_t$ — примарное разложение примарного элемента γ, положим $\chi_\gamma(\alpha) = \chi_{\gamma_1}(\alpha)\chi_{\gamma_2}(\alpha) \dots \chi_{\gamma_t}(\alpha)$. Доказать, что $\chi_\gamma(\alpha) = \chi_\gamma(\beta)$, если $\alpha \equiv \beta$ (γ), и $\chi_\gamma(\alpha\beta) = \chi_\gamma(\alpha)\chi_\gamma(\beta)$. Показать, что если ρ примарно, то $\chi_\rho(\alpha)\chi_\gamma(\alpha) = \chi_{-\rho\gamma}(\alpha)$.

19. Предположим, что $\gamma = A + B\omega$ примарно и что $A = 3M - 1$ и $B = 3N$. Доказать, что $\chi_\gamma(\omega) = \omega^{M+N}$ и $\chi_\gamma(\lambda) = \omega^{2M}$.

20. Показать, что если γ и ρ примарны, то $\chi_\gamma(\rho) = \chi_\rho(\gamma)$.

21. Показать, что если γ примарно, то существует бесконечно много примарных простых чисел π, для которых сравнение $x^3 \equiv \gamma\ (\pi)$ неразрешимо. Показать также, что существует бесконечно много примарных простых чисел π, для которых $x^3 \equiv \omega\ (\pi)$ неразрешимо, и доказать аналогичное утверждение для $x^3 \equiv \lambda\ (\pi)$. [*Указание.* Доказательство аналогично доказательству теоремы 3 из гл. 5.]

22 (продолжение). Показать в общем виде, что если $\gamma \in D$ и $x^3 \equiv \gamma\ (\pi)$ разрешимо для всех примарных простых π, кроме конечного числа, то γ — куб в D.

23. Предположим, что $p \equiv 1\ (3)$. Используя упр. 5, показать, что $x^3 \equiv 3\ (p)$ разрешимо в $\mathbf{Z}$ в том и только том случае, когда p вида $4p = C^2 + 243B^2$.

Следующие три упражнения дают изящное доказательство Вильямса дополнения к кубическому закону взаимности для комплексного случая [245]. Читатель имеет возможность обращаться к указаниям в конце книги.

24. Пусть $\pi = a + b\omega$ — комплексный примарный элемент в $D = \mathbf{Z}[\omega]$. Положим $a = 3m - 1$, $b = 3n$, $p = N(\pi)$.

(a) $(p - 1)/3 \equiv -2m + n\ (3)$;

(b) $(a^2 - 1)/3 \equiv m\ (3)$;

(c) $\chi_\pi(a) = \omega^m$;

(d) $\chi_\pi(a + b) = \omega^{2n}\chi_\pi(1 - \omega)$.

25. Показать, что $\chi_{a+b}(\pi)$ может быть вычислено следующим образом

(a) $\chi_{a+b}(\pi) = \chi_{a+b}(1 - \omega)$;

(b) $\chi_{a+b}(\pi) = \omega^{2(m+n)}$.

26. Объединить предыдущие два упражнения для получения того, что $\chi_\pi(1 - \omega) = \omega^{2m}$.

Следующие четыре упражнения взяты из [186].

27. Пусть $\pi = a + bi$ примарно и неразложимо в $\mathbf{Z}[i]$, $b \neq 0$. Показать, что

(a) $a \equiv (-1)^{(p-1)/4}\ (4)$, $p = N(\pi)$;

(b) $b \equiv 2(-1)^{(p-1)/4}\ (4)$.

28. В обозначениях упр. 27 показать, что $\chi_\pi(\bar{\pi}) = \chi_\pi(2)\chi_\pi(a)$.

29. Согласно упр. 27, $a(-1)^{(p-1)/4}$ примарно. Воспользовавшись биквадратичным законом взаимности, показать, что $\chi_\pi(a(-1)^{(p-1)/4}) = (-1)^{(a^2-1)/8}$.

30. Используя предыдущие два упражнения, показать, что $\chi_\pi(\bar{\pi}) = \chi_\pi(-2)(-1)^{(a^2-1)/8}$.

31. Пусть p — простое число, $p \equiv 1\ (4)$. Показать, что $p = a^2 + b^2$, где a и b однозначно определены условиями $a \equiv 1\ (4)$, $b \equiv -((p - 1)/2)!\ a\ (p)$.

Следующие пять упражнений взяты из [130], § 9.

32. Пусть p — простое число, $p \equiv 1\ (4)$ и $p = \pi\bar{\pi}$, $\pi \in \mathbf{Z}[i]$. Показать, что $\chi_p(1 + i) = i^{(p-1)/4}$.

33. Пусть q — положительное простое число, $q \equiv 3\ (4)$. Показать, что $\chi_q(1 + i) = i^{(p+1)/4}$. [*Указание.* $(1 + i)^{q-1} \equiv -i\ (q)$.]

34. Пусть $\pi = a + bi$ примарно и неразложимо, $(a, b) = 1$. Показать, что
(a) если $\pi \equiv 1$ (4), то $\chi_\pi(a) = i^{(a-1)/2}$;
(b) если $\pi \equiv 3 + 2i$ (4), то $\chi_\pi(a) = -i^{(-a-1)/2}$.

35. Показать, что если $\pi = a + bi$ такое же, как в упр. 34, то $\chi_\pi(a)\,\chi_\pi(a+b) = i^{(3(a+b-1))/4}$. [*Указание.* $a(1+i) = a + b + i(a + bi)$. Обобщить упр. 32 и 33 на любое целое число $\equiv 1$ (4) и воспользоваться предложением 9.9.8. Заметим, что $a + b \equiv 1$ (4).]

36. Избавиться от ограничения $(a, b) = 1$ в упр. 34.

37. Объединяя упр. 32—35, показать, что $\chi_\pi(1+i) = i^{(a-b-b^2-1)/4}$. Показать, что из этого результата следует упр. 26 гл. 5 («характер биквадратичного вычета числа 2»).

38. Доказать п. (d) предложения 9.8.3.

39. Пусть $p \equiv 1$ (6) и запишем $4p = A^2 + 27B^2$, $A \equiv 1$ (3). Положим $m = (p-1)/6$. Показать, что $\binom{3m}{m} \equiv -A\ (p) \Leftrightarrow 2 \mid B$.

40. Пусть $p \equiv 1$ (6), и положим $p = \pi\bar{\pi}$, где π примарно. Записав $\pi = a + b\omega$,
(a) показать, что если $\chi_\pi(2) = \omega$, то $2b - a \equiv -\binom{3m}{m}\ (p)$;
(b) показать, что если $\chi_\pi(2) = \omega^2$, то $a + b \equiv \binom{3m}{m}\ (p)$;
(c) при $\chi_\pi(2) = \omega$ положим $A = 2a - b$, $B = b/3$; показать, что $(A - 9B)/2 \equiv \binom{3m}{m}\ (p)$;
(d) при $\chi_\pi(2) = \omega^2$ положим $A = 2a - b$ и $B = -b/3$; показать, что $(A - 9B)/2 \equiv \binom{3m}{m}\ (p)$;
(e) показать, что «нормализация» B в (c) и (d) эквивалентна сравнению $A \equiv B$ (4).
[Напомним, что $\chi_\pi(2) = \pi$ (2) по кубическому закону взаимности.]

41. Пусть $p \equiv 1$ (6), $4p = A^2 + 27B^2$, $A \equiv 1$ (3), A и B нечетны. Положим $\pi = a + b\omega$, $2a - b = A$, $b = 3B$. Пусть χ_π — характер кубического вычета.
(a) Показать, что если $\chi_\pi(2) = \omega$, то $N(x^3 + 2y^3 = 1) = p + 1 + 2b - a \equiv 0$ (2).
(b) Показать, что если $\chi_\pi(2) = \omega^2$, то $N(x^3 + 2y^3 = 1) = p + 1 - a - b \equiv 0$ (2).
(c) Показать, что если $A \equiv B$ (4), то, предполагая, что $\chi_\pi(2) \neq 1$, имеем $\chi_\pi(2) = \omega$.
(d) Если $\chi_\pi(2) \neq 1$, $A \equiv B$ (4), то $2^{(p-1)/3} \equiv (-A - 3B)/6B \equiv (A + 9B)/(A - 9B)$ (π).
(Это обобщение критерия Эйлера принадлежит Лемеру [174]. См. также [243].)

42. В обозначениях из § 12 показать, что минимальный многочлен для $g(\chi_\pi)$ равен $x^3 - 3px - Ap$.

43. Найти локальные минимум и максимум многочлена $x^3 - 3px - Ap$ и показать, что каждый из интервалов $(-2\sqrt{p}, -\sqrt{p})$, $(-\sqrt{p}, \sqrt{p})$, $(\sqrt{p}, 2\sqrt{p})$ содержит точно одно из значений $2\,\mathrm{Re}\,(\omega^k g(\chi_\pi))$, $k = 0, 1, 2$.

44. Пусть $n \in \mathbf{Z}$, $n = s_1 \ldots s_t$, $n \equiv 1$ (4), $s_i \equiv 1$ (4), $i = 1, \ldots, t$. Показать, что $(n-1)/4 \equiv \sum_{i=1}^{t} (s_i - 1)/4$ (4).

45. Пусть $\pi = a + bi \in \mathbf{Z}[i]$ и $q \equiv 3$ (4) — рациональное простое число. Показать, что $\pi^q \equiv \bar{\pi}$ (q).

Глава 10

УРАВНЕНИЯ НАД КОНЕЧНЫМИ ПОЛЯМИ

В этой главе мы изложим новую точку зрения. Диофантовы задачи над конечными полями будут рассматриваться на языке элементарной алгебраической геометрии. Будут определены понятия аффинного пространства, проективного пространства и бесконечно удаленных точек.

После того как будут введены эти понятия, мы докажем очень общую теорему Шевалле о том, что многочлен от нескольких переменных без свободного члена над конечным полем всегда имеет нетривиальные нули, если число переменных превосходит его степень.

Затем мы обратимся к проблеме обобщения результатов гл. 8 на произвольные конечные поля. Оказывается, что это относительно просто сделать. Эти более общие результаты представляют интерес сами по себе, а также играют важную роль при рассмотрении дзета-функций, которое начинается в гл. 11.

§ 1. Аффинное пространство, проективное пространство и многочлены

Пусть F — некоторое поле и $A^n(F)$ — множество n-наборов $(a_1, a_2, \ldots, a_n)$ с $a_i \in F$. Его можно рассматривать как векторное пространство при обычном способе определения сложения и умножения на скаляры. Мы же будем иметь дело с $A^n(F)$ как множеством и будем называть его n-мерным аффинным пространством над F. Как обычно, точка $(0, 0, \ldots, 0)$ называется *началом координат*. Для краткости мы будем обозначать иногда точку $(a_1, a_2, \ldots, a_n)$ одной буквой a.

n-мерное проективное пространство над F, $P^n(F)$, — несколько более сложное понятие. Мы рассматриваем сначала $A^{n+1}(F)$, обозначая его точки через $(a_0, a_1, \ldots, a_n)$. На множестве $A^{n+1}(F) - \{(0, 0, \ldots, 0)\}$ ($(n+1)$-мерном аффинном пространстве с выброшенным началом координат) мы определяем отношение эквивалентности. Точка $(a_0, a_1, \ldots, a_n)$ *эквивалентна* точке $(b_0, b_1, \ldots, b_n)$, если существует такой элемент $\gamma \in F^*$, что $a_0 = \gamma b_0$, $a_1 = \gamma b_1$, $\ldots$, $a_n = \gamma b_n$. Нетрудно убедиться в том, что это отношение эквивалентности. Классы эквивалентности называются *точками* пространства $P^n(F)$. Если точка $a \in A^{n+1}(F)$ от-

лична от начала координат, то $[a]$ обозначает класс эквивалентности, содержащий a, причем a называется представителем класса $[a]$. Геометрически точки пространства $P^n(F)$ находятся во взаимно однозначном соответствии с прямыми в $A^{n+1}(F)$, проходящими через начало координат.

Если F — конечное поле из q элементов, то очевидно, что $A^n(F)$ содержит q^n элементов. $P^n(F)$ состоит из $q^n + q^{n-1} + \ldots + q + 1$ элементов. Чтобы убедиться в этом, заметим, что $A^{n+1}(F) - \{(0, 0, \ldots, 0)\}$ имеет $q^{n+1} - 1$ элементов. Так как группа F^* состоит из $q - 1$ элементов, то каждый класс эквивалентности содержит $q - 1$ элементов. Таким образом, $P^n(F)$ имеет $(q^{n+1} - 1)/(q - 1) = q^n + q^{n-1} + \ldots + q + 1$ элементов.

Вообще говоря, $P^n(F)$ содержит больше точек, чем $A^n(F)$. Непосредственно убедиться в этом можно следующим образом. Если $[x] \in P^n(F)$ и $x_0 \neq 0$, то положим

$$\varphi([x]) = (x_1/x_0, x_2/x_0, \ldots, x_n/x_0) \in A^n(F).$$

Как нетрудно убедиться, это отображение не зависит от выбора представителя x.

Лемма 1. *Пусть $\bar{H}$ — множество классов $[x] \in P^n(F)$ с $x_0 = 0$. Тогда φ отображает $P^n(F) - \bar{H}$ в $A^n(F)$, и это отображение взаимно однозначно и сюръективно. (Если S и T — множества, то $S - T$ — это множество элементов из S, не принадлежащих T.)*

Доказательство. Если $\varphi([x]) = \varphi([y])$, то $x_i/x_0 = y_i/y_0$ для $i = 0, 1, \ldots, n$. Пусть $\gamma = y_0/x_0$. Тогда $\gamma x_i = y_i$ для $i = 0, 1, \ldots, n$, так что $[x] = [y]$.

Если $v = (v_1, v_2, \ldots, v_n) \in A^n(F)$, то положим $w = (1, v_1, v_2, \ldots, v_n)$. Тогда $\varphi([w]) = v$. □

Множество $\bar{H}$ называется *бесконечно удаленной гиперплоскостью*. Нетрудно убедиться в том, что $\bar{H}$ обладает структурой пространства $P^{n-1}(F)$. Таким образом, $P^n(F)$ состоит из двух кусков, один есть копия пространства $A^n(F)$, и его точки называются *конечными*, а другой — копия пространства $P^{n-1}(F)$, и его точки называются *бесконечно удаленными*.

Заметим, что $P^0(F)$ состоит просто из одной точки. Таким образом, $P^1(F)$ имеет лишь одну бесконечно удаленную точку. Аналогично, $P^2(F)$ имеет бесконечно удаленную (проективную) прямую и т. д.

Теперь, когда определены аффинные и проективные пространства, мы привлечем многочлены для получения множеств, называемых гиперповерхностями.

Пусть $F[x_1, x_2, \ldots, x_n]$ — кольцо многочленов от n переменных над полем F. Если $f \in F[x_1, \ldots, x_n]$, то

$$f(x) = \sum_{(i_1, i_2, \ldots, i_n)} a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},$$

где сумма берется по всем наборам неотрицательных целых чисел $(i_1, i_2, \ldots, i_n)$, для которых $a_{i_1 i_2 \ldots i_n} \neq 0$. Многочлен вида $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ называется *одночленом*. По определению его общая степень равна $i_1 + i_2 + \ldots + i_n$, а степень по переменной x_m равна i_m. Степень многочлена $f(x)$ есть максимум полных степеней одночленов, которые входят в $f(x)$ с ненулевыми коэффициентами. Степень по x_m есть максимум степеней по x_m одночленов, которые входят в $f(x)$ с ненулевыми коэффициентами. Обозначим эти два числа через $\deg f(x)$ и $\deg_m f(x)$. Тогда

(a) $\deg f(x)\, g(x) = \deg f(x) + \deg g(x)$;

(b) $\deg_m f(x)\, g(x) = \deg_m f(x) + \deg_m g(x)$.

Если все одночлены, входящие в $f(x)$, имеют степень l, то $f(x)$ называется *однородным* многочленом степени l.

Например, если $f(x) = 1 + x_1 x_2 + x_2 x_3 + x_4^3$, то $\deg f(x) = 3$, $\deg_1 f(x) = \deg_2 f(x) = \deg_3 f(x) = 1$ и $\deg_4 f(x) = 3$. Многочлен $f(x)$ неоднороден, в то время как $h(x) = x_1^3 + x_2^3 + x_3^3 + x_1 x_2 x_3$ однороден степени 3.

Однородный многочлен иногда называется *формой*. Форма степени 2 называется *квадратичной формой*, а форма степени 3 — *кубической формой* и т. д.

Предположим, что K — некоторое поле, содержащее F. Если $f(x) \in F[x_1, x_2, \ldots, x_n]$ и $a \in A^n(K)$, то мы можем подставить a_i вместо x_i и вычислить $f(a)$.

Это показывает, что $f(x)$ определяет функцию из $A^n(K)$ в K, которая переводит a в $f(a)$. Точка $a \in A^n(K)$, для которой $f(a) = 0$, называется нулем функции $f(x)$.

Если K — конечное поле из q элементов, то $x^q - x$ определяет нулевую функцию на $A^1(K)$. Таким образом, ненулевой многочлен может давать нулевую функцию. Этого не может случиться, если K бесконечно (см. упражнения).

Для ненулевого многочлена $f(x)$ положим $H_f(K) = \{a \in A^n(K) \mid f(a) = 0\}$; $H_f(K)$ называется *гиперповерхностью, определяемой f, в $A^n(K)$*. Если K конечно, то $H_f(K)$ — конечное множество и естественно поставить вопрос о числе точек в $H_f(K)$. В гл. 8 мы имели дело с несколькими частными случаями этой задачи.

Мы хотим определить теперь проективную гиперповерхность. Пусть $h(x) \in F[x_0, x_1, \ldots, x_n]$ — ненулевой однородный многочлен степени d. Как и прежде, K есть поле, содержащее F. Для $\gamma \in K^*$ имеем $h(\gamma x) = \gamma^d h(x)$. Отсюда следует, что если $a \in$

$\in A^{n+1}(K)$ и $h(a) = 0$, то $h(\gamma a) = 0$. Таким образом, мы можем положить $\bar{H}_h(K) = \{[a] \in P^n(K) \mid h(a) = 0\}$. Это множество называется *гиперповерхностью, определенной h, в $P^n(K)$*. Если K конечно, мы можем опять поставить вопрос о числе точек в $\bar{H}_h(K)$.

В более общем виде, если $f_1, \ldots, f_m$ — многочлены в $F[x_1, \ldots, x_n]$, положим $V = \{(a_1, \ldots, a_n) \mid a_i \in F, i = 1, \ldots, n, f_j(a_1, \ldots, a_n) = 0, j = 1, \ldots, m\}$. V называется *алгебраическим множеством*, определенным над полем F. Если идеал, определенный многочленами $f_1, \ldots, f_m$ в $F[x_1, \ldots, x_n]$, прост, то V называется *алгебраическим многообразием*. Аналогично, множество общих проективных нулей конечного набора однородных многочленов из $F[x_0, \ldots, x_n]$ называется *проективным алгебраическим множеством*.

Оказывается что работа с проективными пространствами приводит к более цельным результатам, чем работа с аффинными пространствами. Мы проиллюстрируем это, определив проективное замыкание аффинной гиперповерхности.

Пусть $f(x) \in F[x_1, x_2, \ldots, x_n]$, и определим $\bar{f}(y) = \bar{f}(y_0, y_1, \ldots, y_n)$ посредством формулы

$$\bar{f}(y) = y_0^{\deg f} f\left(\frac{y_1}{y_0}, \frac{y_2}{y_0}, \ldots, \frac{y_n}{y_0}\right).$$

Мы вскоре убедимся, что $\bar{f}$ — однородный многочлен. Он приводит к гиперповерхности в $P^n(K)$. Грубо говоря, новая гиперповерхность получается из $H_f(K)$ добавлением бесконечно удаленных точек.

Лемма 2. *$\bar{f}(y)$ — однородный многочлен степени* $\deg f$. *Кроме того,* $\bar{f}(1, y_1, y_2, \ldots, y_n) = f(y_1, y_2, \ldots, y_n)$.

Доказательство. Положим $d = \deg f$ и рассмотрим одночлен $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$ степени $l \leqslant d$. Тогда $y_0^d (y_1/y_0)^{i_1} \ldots (y_n/y_0)^{i_n} = y_0^{d-l} y_1^{i_1} y_2^{i_2} \ldots y_n^{i_n}$, причем последний одночлен имеет степень d. Таким образом, в $\bar{f}(y)$ все одночлены имеют степень d, что доказывает первое утверждение.

Второе утверждение следует из определения. □

Например, если $f(x) = x_1^3 + x_2^3 - 1$, то $\bar{f}(y) = y_1^3 + y_2^3 - y_0^3$; если $f(x) = 1 + 2x_1^3 - 3x_2^2$, то $\bar{f}(y) = y_0^3 + 2y_1^3 - 3y_0 y_2^2$.

Рассмотрим гиперповерхность $H_f(K) \subset A^n(K)$. Многочлен $\bar{f}(y)$ однороден по переменным $y_0, y_1, \ldots, y_n$, а поэтому $\bar{f}$ определяет гиперповерхность $\bar{H}_{\bar{f}}(K)$ в $P^n(K)$. Эта гиперповерхность называется *проективным замыканием* $H_f(K)$ в $P^n(K)$.

Пусть $\lambda\colon A^n(K) \to P^n(K)$ определено равенством $\lambda(a_1, a_2, \ldots, a_n) = [1, a_1, a_2, \ldots, a_n]$. Отображение λ взаимно однозначно,

и, кроме того, образ $H_f(K)$ при λ содержится в $\bar{H}_{\bar{f}}(K)$, так как, очевидно,

$$\bar{f}([1, a_1 \ldots a_n]) = f(a_1, \ldots, a_n) = 0$$

для всех $a \in H_f(K)$. Вообще говоря, гиперповерхность $\bar{H}_{\bar{f}}(K)$ имеет больше точек, чем $H_f(K)$, поскольку в ней еще имеется пересечение с бесконечно удаленной гиперплоскостью.

На примерах все это станет нагляднее, но, прежде чем их приводить, напомним определения отображений φ и λ и приведем диаграммную картинку для $P^n(K)$:

λ: $A^n(K) \to P^n(K)$ задается формулой

$$\lambda(a_1, a_2, \ldots, a_n) = [1, a_1, a_2, \ldots, a_n],$$

φ: $P^n(K) - \overline{H} \to A^n(K)$ задается формулой

$$\varphi([b_0, b_1, \ldots, b_n]) = \left(\frac{b_1}{b_0}, \frac{b_2}{b_0}, \ldots, \frac{b_n}{b_0}\right).$$

$P^n(K)$

$\operatorname{Im}\lambda \approx A^n(K)$	$\overline{H} \approx P^{n-1}(K)$
Конечные точки	Бесконечно удаленные точки

Примеры

1. $f(x) = x_1^2 + x_2^2 - 1$ над полем $F = \mathbf{Z}/p\mathbf{Z}$.

Как мы видели в гл. 8, § 3, уравнение $f(x) = 0$ имеет $p - 1$ решений при $p \equiv 1$ (4) и $p + 1$ решений при $p \equiv 3$ (4).

$\bar{f}(y_0, y_1, y_2) = y_1^2 + y_2^2 - y_0^2$. Решения $[p_0, p_1, p_2]$, где $p_0 \neq 0$, соответствуют аффинным решениям $(p_1/p_0, p_2/p_0)$. Предположим, что $[0, p_1, p_2]$ — решение. Тогда $p_1^2 + p_2^2 = 0$, или $(p_2/p_1)^2 = -1$. При $p \equiv 1$ (4) существует такой элемент $a \in F$, что $a^2 = -1$, и в этом случае имеется две бесконечно удаленные точки, а именно $[0, 1, a]$ и $[0, 1, -a]$. При $p \equiv 3$ (4) не существует элемента $a \in F$ с $a^2 = -1$, а следовательно, не существует бесконечно удаленных точек. В обоих случаях, однако, гиперповерхность $\bar{H}_{\bar{f}}(F)$ имеет точно $p + 1$ точек.

2. $f(x) = x_1^n + x_2^n - 1$ над $F = \mathbf{Z}/p\mathbf{Z}$ при $p \equiv 1$ (n).

Тогда $\bar{f}(y) = y_1^n + y_2^n - y_0^n$. Таким образом, бесконечно удаленные точки на $\bar{H}_{\bar{f}}(F)$ имеют вид $[0, y_1, y_2]$, где $y_1^n + y_2^n = 0$. Если -1 не является n-й степенью в F, то не существует бесконечно удаленных точек. Если $a^n = -1$ для некоторого $a \in F$, то уравнение $x^n = -1$ имеет n решений в поле F [это следует из

предложения 4.2.1, так как $p \nmid (n)!$. Обозначим эти решения через $a_1 = a$, a_2, ..., a_n. Тогда $|0, 1, a_1|$, ..., $|0, 1, a_n|$ — бесконечно удаленные точки, являющиеся нулями для $\bar{f}(y)$. В обозначениях гл. 8, § 4, число бесконечно удаленных точек равно $\delta_n(-1)\,n$ и $N(x_1^n + x_2^n = 1) + \delta_n(-1)\,n$ есть число точек на проективной гиперповерхности (кривой), определенной уравнением $y_1^n + y_2^n - y_0^n = 0$. Так как число точек в $P^1(F)$ равно $p + 1$, формулу из предложения 8.4.1 можно интерпретировать следующим образом: число точек на проективной кривой $y_1^n + y_2^n - y_0^n = 0$ над $\mathbf{Z}/p\mathbf{Z}$ отличается от числа точек на проективной прямой на величину, которая не превосходит $(n-1)(n-2)\sqrt{p}$.

Этот результат является частным случаем так называемой гипотезы Римана для конечных полей, в которой утверждается, грубо говоря, что над конечным полем из q элементов число точек на проективной кривой отличается от числа точек на проективной прямой на величину, которая не превосходит удвоенный род (число, определяемое кривой [1])), умноженный на $\sqrt{q}$.

Частные случаи этой гипотезы были доказаны различными авторами: Гауссом, Герглотцом, Хассе и Дэвенпортом. В полной общности эта теорема была доказана Вейлем.

3. $f(x) = x_1^2 + x_2^2 + \ldots + x_m^2 - 1$ над $F = \mathbf{Z}/p\mathbf{Z}$, где m четно. Число конечных точек равно $p^{m-1} - (-1)^{(m/2)((p-1)/2)} p^{(m/2)-1}$ (см. предложение 8.6.1). Так как $\bar{f}(y) = y_1^2 + y_2^2 + \cdots + y_m^2 - y_0^2$, то число бесконечно удаленных точке равно числу решений уравнения $y_1^2 + y_2^2 + \ldots + y_m^2 = 0$ в $P^{m-1}(F)$. Число аффинных решений задается формулой

$$N = p^{m-1} + (-1)^{(m/2)((p-1)/2)}(p-1)\,p^{(m/2)-1}$$

(см. упр. 19 гл. 8), так что число проективных решений равно

$$\frac{N-1}{p-1} = p^{m-2} + p^{m-3} + \cdots + p + 1 + (-1)^{(m/2)((p-1)/2)} p^{(m/2)-1}.$$

Добавляя число конечных решений к бесконечно удаленным решениям, получаем

$$p^{m-1} + p^{m-2} + \cdots + p + 1.$$

Это довольно примечательный результат. В нем утверждается, что число точек на проективной гиперповерхности, определяемой уравнением $y_1^2 + y_2^2 + \ldots + y_m^2 - y_0^2 = 0$, точно равно числу точек в $P^{m-1}(\mathbf{Z}/p\mathbf{Z})$.

[1]) Для неособой проективной кривой степени n род равен $(n-1)(n-2)/2$, см. [219], гл. III. — *Прим. ред.*

Существует более простой способ получения этого результата. Вместо того чтобы рассматривать отдельно конечные и бесконечно удаленные точки, мы просто подсчитываем число M аффинных решений уравнения $y_1^2 + y_2^2 + \ldots + y_m^2 - y_0^2 = 0$ в $A^{m+1}(F)$, а затем вычисляем $(M-1)/(p-1)$. Так как $m+1$ нечетно, число M равно p^m (см. упр. 19 гл. 8). Таким образом, $(M-1)/(p-1) = p^{m-1} + p^{m-2} + \ldots + p + 1$.

§ 2. Теорема Шевалле

В этом параграфе F будет обозначать конечное поле из q элементов.

Если q — простое число, т. е. $F = \mathbf{Z}/q\mathbf{Z}$, то уравнение $x_1^{q-1} + x_2^{q-1} + \ldots + x_q^{q-1} = 0$ не имеет решений, кроме $(0, 0, \ldots, 0)$, так как a^{q-1} равно 1 или 0 в зависимости от того, будет ли $a \neq 0$ или $a = 0$ для $a \in F$. Таким образом, выписанный многочлен принимает значения $0, 1, 2, \ldots, q-1$ и равен нулю лишь при $x_1 = x_2 = \ldots = x_{q-1} = 0$. Заметим, что у этого многочлена число переменных равно степени.

В 1935 г. Артин сформулировал в виде гипотезы следующую теорему, которая почти тотчас же была доказана Шевалле [16].

Теорема 1. *Пусть* $f(x) \in F[x_1, x_2, \ldots, x_n]$, *и предположим, что*

(a) $f(0, 0, \ldots, 0) = 0$;

(b) $n > d = \deg f$.

Тогда f *имеет по крайней мере два нуля в* $A^n(F)$.

Прежде чем приступить к доказательству, мы выведем непосредственное следствие из этой теоремы.

Следствие. *Пусть* $h(y) \in F[y_0, y_1, \ldots, y_n]$ — *однородный многочлен степени* $d > 0$. *Если* $n + 1 > d$, *то множество* $\bar{H}_h(F)$ *непусто.*

Доказательство. Так как h однороден, $(0, 0, \ldots, 0)$ будет его нулем. По теореме 1 h имеет другой нуль, $(a_0, a_1, \ldots, a_n)$. Очевидно, что $[a_0, a_1, \ldots, a_n] \in \bar{H}_h(F)$. □

Нам понадобится следующая элементарная лемма.

Лемма 1. *Пусть* $f(x_1, x_2, \ldots, x_n)$ — *многочлен, степень которого по каждой переменной меньше* q. *Если* f *равен нулю на всем* $A^n(F)$, *то он — нулевой многочлен.*

Доказательство. Применим индукцию по n. Если $n = 1$, то $f(x)$ — многочлен от одной переменной степени $< q$ с q различными корнями, а именно всеми элементами поля F. Таким образом, f — нулевой многочлен.

Предположим, что наш результат доказан для $n - 1$, и рассмотрим

$$f(x_1, x_2, \ldots, x_n).$$

Мы можем записать

$$f(x_1, \ldots, x_n) = \sum_{i=0}^{q-1} g_i(x_1, \ldots, x_{n-1}) x_n^i.$$

Выберем $a_1, a_2, \ldots, a_{n-1} \in F$. Тогда $\sum_{i=0}^{q-1} g_i(a_1, a_2, \ldots, a_{n-1}) x_n^i$ имеет q корней, а потому $g_i(a_1, a_2, \ldots, a_{n-1}) = 0$. По индукции каждый многочлен g_i нулевой, а следовательно, нулевым будет и f. □

Напомним, что $f(x) = x^q - x$ — ненулевой многочлен, который равен нулю на всем $A^1(F)$, так что предположение леммы существенно.

Назовем многочлен *редуцированным*, если он имеет степень $< q$ по каждой переменной. Два многочлена f, g называются *эквивалентными*, если $f(a) = g(a)$ для всех $a \in A^n(F)$. В таком случае мы пишем $f \sim g$.

Лемма 2. *Каждый многочлен $f(x) \in F[x_1, \ldots, x_n]$ эквивалентен редуцированному многочлену.*

Доказательство. Рассмотрим случай одной переменной. Очевидно, что $x^q \sim x$. Если $m > 0$ — целое число, то пусть l — наименьшее положительное число, для которого $x^m \sim x^l$. Мы утверждаем, что $l < q$. Если это не так, то $l = qs + r$, где $0 \leqslant r < q$ и $s \neq 0$. Тогда $x^l = (x^q)^s x^r \sim x^{r+s}$. Поскольку $s + r \leqslant l$, это противоречит минимальности l.

В случае n переменных рассмотрим одночлен $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$. В силу того что было сказано, $x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \sim x_1^{j_1} x_2^{j_2} \ldots x_n^{j_n}$, где $j_k < q$ для $k = 1, 2, \ldots, n$. Лемма 2 непосредственно следует из этого замечания. □

Теперь мы можем доказать теорему 1. Предположим, что $(0, 0, \ldots, 0)$ — единственный нуль многочлена f. Тогда $1 - f^{q-1}$ принимает значение 1 в $(0, 0, \ldots, 0)$ и значение нуль во всех других точках. Так же ведет себя и многочлен

$$(1 - x_1^{q-1})(1 - x_2^{q-1}) \ldots (1 - x_n^{q-1}).$$

Таким образом,

$$1 - f^{q-1} - (1 - x_1^{q-1})(1 - x_2^{q-1}) \dots (1 - x_n^{q-1})$$

равен нулю на всем $A^n(F)$. Заменим $1 - f^{q-1}$ эквивалентным редуцированным многочленом g. Тогда

$$g - (1 - x_1^{q-1}) \cdots (1 - x_n^{q-1})$$

имеет степень $< q$ по каждой из своих переменных и равен нулю на всем $A^n(F)$. В силу леммы 1 он — нулевой многочлен. Таким образом, $\deg g = n(q-1)$. С другой стороны,

$$\deg g \leqslant \deg (1 - f^{q-1}) = d(q-1).$$

Напомним, что $d = \deg f$. Отсюда вытекает, что $n \leqslant d$, а это противоречит предположению. Следовательно, f должен иметь более чем один нуль.

Мы приведем другое доказательство теоремы 1, принадлежащее Аксу [3]. Оно основано на следующей лемме.

Лемма 3. *Пусть $i_1, i_2, \dots, i_n$ — неотрицательные целые числа. Тогда*

$$\sum_{a \in A^n(F)} a_1^{i_1} a_2^{i_2} \dots a_n^{i_n} = 0,$$

за исключением случая, когда все i_j отличны от нуля и делятся на $q-1$.

Доказательство. Предположим сначала, что $n = 1$. Если $i = 0$, то $\sum_{a \in F} a^0 = q = 0$ в F. Предположим, что $i \neq 0$. Группа F^* циклическая. Пусть b — ее образующий. Если $q - 1 \nmid i$, то

$$\sum_{a \in F} a^i = \sum_{k=0}^{q-2} b^{ki} = \frac{b^{(q-1)i} - 1}{b^i - 1} = 0.$$

В общем случае

$$\sum_{a \in A^n(F)} a_1^{i_1} a_2^{i_2} \dots a_n^{i_n} = \left(\sum_{a_1 \in F} a_1^{i_1}\right)\left(\sum_{a_2 \in F} a_2^{i_2}\right) \cdots \left(\sum_{a_n \in F} a_n^{i_n}\right).$$

Лемма 3 теперь очевидна.

Следует отметить, что если $q - 1 \mid i_j$ и $i_j \neq 0$ для всех j, то значение написанной выше суммы равно $(q-1)^n$.

Возвращаясь к теореме 1, обозначим через N_f число решений уравнения $f(x) = 0$ в $A^n(F)$. Мы покажем, что $p \mid N_f$, где p —

характеристика поля F. Это уточнение теоремы Шевалле было впервые получено Варнингом [78].

Как мы видели, $1 - f^{q-1}$ принимает значение 1 в нулях многочлена f и значение нуль в других точках.

Таким образом,

$$\overline{N}_f = \sum_{a \in A^n(F)} (1 - f(a)^{q-1}),$$

где $\overline{N}_f$ — класс вычетов числа N_f по модулю p, рассматриваемый как элемент поля F.

Пусть $x_1^{i_1}x_2^{i_2} \ldots x_n^{i_n}$ — одночлен, встречающийся в $1 - f(x)^{q-1}$. Так как этот многочлен имеет степень $d(q-1)$, то $i_j < q-1$ при некотором j, так как в противном случае степень рассматриваемого одночлена была бы $\geqslant n(q-1)$, а мы предположили, что $d < n$. В силу леммы 3

$$\sum_{a \in A^n(F)} a_1^{i_1}a_2^{i_2} \cdots a_n^{i_n} = 0.$$

Так как $1 - f(x)^{q-1}$ является линейной комбинацией одночленов, отсюда следует, что $\overline{N}_f = 0$, т. е. $p \mid N_f$.

Варнинг смог доказать, что $N_f \geqslant q^{n-d}$. Несколько в ином направлении пошел Акс, показав, что $q^b \mid N_f$, где b — наибольшее целое число $< n/d$. Подробности см. в [78] и [3].

§ 3. Суммы Гаусса и Якоби над конечными полями

Пусть $\zeta_p = e^{2\pi i/p}$ и $F_p = \mathbf{Z}/p\mathbf{Z}$. В гл. 8 существенную роль играла функция $\psi\colon F_p \to \mathbf{C}$, задаваемая равенством $\psi(t) = \zeta_p^t$. Для перенесения основных результатов гл. 8 на произвольное конечное поле F нам понадобится аналог функции ψ для поля F. Мы получаем его с помощью взятия следа.

Предположим, что F имеет $q = p^n$ элементов. Для $\alpha \in F$ положим $\mathrm{tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \ldots + \alpha^{p^{n-1}}$ и назовем $\mathrm{tr}(\alpha)$ *следом* элемента α.

Предложение 10.3.1. *Если* $\alpha, \beta \in F$ *и* $\alpha \in F_p$, *то*
(a) $\mathrm{tr}(\alpha) \in F_p$;
(b) $\mathrm{tr}(\alpha + \beta) = \mathrm{tr}(\alpha) + \mathrm{tr}(\beta)$;
(c) $\mathrm{tr}(a\alpha) = a\,\mathrm{tr}(\alpha)$;
(d) tr *отображает* F *на* F_p.

Доказательство. (a) Имеем

$$\left(\alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}\right)^p = \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-1}} + \alpha^{p^n}.$$

Так как $\alpha^{p^n} = \alpha^q = \alpha$, то мы видим, что $\mathrm{tr}(\alpha)^p = \mathrm{tr}(\alpha)$. Это доказывает свойство (a) (см. предложение 7.1.1, следствие 1).

(b) $\mathrm{tr}(\alpha+\beta) = (\alpha+\beta) + (\alpha+\beta)^p + \cdots + (\alpha+\beta)^{p^{n-1}} =$

$= (\alpha+\beta) + (\alpha^p+\beta^p) + \cdots + (\alpha^{p^{n-1}} + \beta^{p^{n-1}}) =$

$= (\alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}) + (\beta + \beta^p + \cdots + \beta^{p^{n-1}}) =$

$= \mathrm{tr}(\alpha) + \mathrm{tr}(\beta).$

(c) $\mathrm{tr}(a\alpha) = a\alpha + a^p\alpha^p + \cdots + a^{p^{n-1}}\alpha^{p^{n-1}} =$

$= a(\alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}) =$

$= a\,\mathrm{tr}(\alpha).$

Мы использовали тот факт, что $a^p = a$ для $a \in F_p$.

(d) Многочлен $x + x^p + \ldots + x^{p^{n-1}}$ имеет, самое большее, p^{n-1} корней в F. Так как F содержит p^n элементов, то существует такой элемент $\alpha \in F$, что $\mathrm{tr}(\alpha) = c \neq 0$. Если $b \in F_p$, то, используя свойство (c), получаем $\mathrm{tr}((b/c)\alpha) = (b/c)\,\mathrm{tr}(\alpha) = b$. Таким образом, область значений следа есть все F_p. □

Мы определяем теперь $\psi\colon F \to \mathbf{C}$ формулой $\psi(\alpha) = \zeta_p^{\mathrm{tr}(\alpha)}$. Если $F = F_p$, это совпадает с прежним определением.

Предложение 10.3.2. *Функция ψ обладает следующими свойствами* [1]):

(a) $\psi(\alpha+\beta) = \psi(\alpha)\psi(\beta)$;

(b) *существует такой элемент* $\alpha \in F$, *что* $\psi(\alpha) \neq 1$;

(c) $\sum_{\alpha \in F} \psi(\alpha) = 0$.

Доказательство. (a) $\psi(\alpha+\beta) = \zeta_p^{\mathrm{tr}(\alpha+\beta)} = \zeta_p^{\mathrm{tr}(\alpha)+\mathrm{tr}(\beta)} = \zeta_p^{\mathrm{tr}(\alpha)}\zeta_p^{\mathrm{tr}(\beta)} = \psi(\alpha)\psi(\beta)$.

(b) Функция tr есть эпиморфное отображение, так что существует такой элемент $\alpha \in F$, что $\mathrm{tr}(\alpha) = 1$. Тогда $\psi(\alpha) = \zeta_p \neq 1$.

(c) Пусть $S = \sum_{\alpha \in F} \psi(\alpha)$. Выберем β, такой, что $\psi(\beta) \neq 1$. Тогда $\psi(\beta)\,S = \sum_{\alpha \in F} \psi(\beta)\psi(\alpha) = \sum_{\alpha \in F} \psi(\beta+\alpha) = S$. Отсюда следует, что $S = 0$. □

---

[1]) Функции ψ, обладающие свойством (a) и такие, что $\psi(0) = 1$, называются *аддитивными* характерами поля F. — *Прим. ред.*

Предложение 10.3.3. *Пусть* $\alpha, x, y \in F$. *Тогда*

$$\frac{1}{q}\sum_{\alpha \in F} \psi(\alpha(x-y)) = \delta(x, y),$$

где $\delta(x, y) = 1$, *если* $x = y$, *и нуль в противном случае.*

Доказательство. Если $x = y$, то

$$\sum_{\alpha \in F} \psi(\alpha(x-y)) = \sum_{\alpha \in F} \psi(0) = q.$$

Если $x \neq y$, то $x - y \neq 0$ и $\alpha(x-y)$ пробегает все поле F, когда α пробегает все F. Таким образом,

$$\sum_{\alpha \in F} \psi(\alpha(x-y)) = \sum_{\beta \in F} \psi(\beta) = 0$$

в силу свойства (c) предложения 10.3.2. □

Предложение 10.3.3 обобщает следствие 1 леммы 1 из гл. 6.

В гл. 7 было доказано, что мультипликативная группа конечного поля циклическая. Основываясь на этом факте, нетрудно убедиться в том, что все определения и предложения § 1 гл. 8 могут быть применены к F так же, как и к F_p. Следует лишь заменить p на q всюду, где оно появляется. Значит, мы можем предполагать, что теория мультипликативных характеров справедлива и для поля F.

Мы теперь можем определить для поля F суммы Гаусса.

Определение. Пусть χ — некоторый характер поля F и $\alpha \in F^*$. Пусть

$$g_\alpha(\chi) = \sum_{t \in F} \chi(t)\psi(\alpha t).$$

$g_\alpha(\chi)$ называется *суммой Гаусса на* поле F (или поля F), принадлежащей характеру χ.

С заменой p на q теперь для суммы $g_\alpha(\chi)$ могут быть доказаны предложения 8.2.1 и 8.2.2. В доказательстве предложения 8.2.2 используется предложение 10.3.3.

В частности, $|g_\alpha(\chi)| = q^{1/2}$ и $g_\alpha(\chi)\, g_\alpha(\chi^{-1}) = \chi(-1)\, q$ для $\chi \neq \varepsilon$.

Общая теория сумм Якоби и связь между суммами Гаусса и Якоби, развитая в § 5 гл. 8, также обобщается без труда (опять с заменой всюду p на q). Все результаты § 7 гл. 8 тоже верны. Читатель имеет возможность вернуться к этим параграфам и убедиться в том, что обобщение их определений и результатов в самом деле не представляет особого труда.

В качестве упражнения в работе с этими новыми инструментами мы приведем теорему, которая по существу является переформулировкой некоторых наших более ранних результатов. Эта теорема будет использована также в гл. 11.

Теорема 2. *Предположим, что F — поле из q элементов и $q \equiv 1\ (m)$. Однородное уравнение $a_0y_0^m + a_1y_1^m + \ldots + a_ny_n^m = 0$, $a_0, a_1, \ldots, a_n \in F^*$, определяет гиперповерхность в $P^n(F)$. Число точек на этой гиперповерхности задается выражением*

$$q^{n-1} + q^{n-2} + \cdots + q + 1 + \frac{1}{q-1} \sum_{\chi_0, \chi_1, \ldots, \chi_n} \chi_0(a_0^{-1}) \ldots \chi_n(a_n^{-1}) J_0(\chi_0, \chi_1, \ldots, \chi_n), \quad (1)$$

где $\chi_i^m = \varepsilon$, $\chi_i \neq \varepsilon$ и $\chi_0\chi_1 \ldots \chi_n = \varepsilon$.

Кроме того, при этих условиях

$$\frac{1}{q-1} J_0(\chi_0, \chi_1, \ldots, \chi_n) = \frac{1}{q} g(\chi_0) g(\chi_1) \ldots g(\chi_n). \quad (2)$$

Доказательство. Число N точек на гиперповерхности в $A^{n+1}(F)$, определенной уравнением $a_0y_0^m + a_1y_1^m + \ldots + a_ny_n^m = 0$, задается формулой

$$q^n + \sum_{\chi_0, \chi_1, \ldots, \chi_n} \chi_0(a_0^{-1}) \chi_1(a_1^{-1}) \ldots \chi_n(a_n^{-1}) J_0(\chi_0, \chi_1, \ldots, \chi_n),$$

где характеры χ_i удовлетворяют условиям из теоремы. Это следует из теоремы 5 гл. 8. Нужное нам число равно $(N - 1)/(q - 1)$, что и приводит к (1).

Согласно предложению 8.5.1, п. (c),

$$J_0(\chi_0, \chi_1, \ldots, \chi_n) = \chi_0(-1)(q-1) J(\chi_1, \chi_2, \ldots, \chi_n). \quad (3)$$

В силу теоремы 3 гл. 8

$$J(\chi_1, \chi_2, \ldots, \chi_n) = \frac{g(\chi_1) g(\chi_2) \cdots g(\chi_n)}{g(\chi_1\chi_2 \cdots \chi_n)}. \quad (4)$$

Умножим числитель и знаменатель правой части на $g(\chi_0)$. Так как $\chi_0\chi_1 \ldots \chi_n = \varepsilon$, то $g(\chi_0) g(\chi_1\chi_2 \ldots \chi_n) = \chi_0(-1) q$. Объединяя это с равенствами (3) и (4), получаем (2). □

Замечания

Хорошее введение в геометрию над конечными полями имеется в книге [7]. Авторы обсуждают аффинную, проективную и даже гиперболическую геометрии. Имеется также хотя и короткая, но полезная библиография.

Гипотеза Артина о многочленах над конечными полями высказывалась значительно раньше Диксоном (Bull. Amer. Math. Soc., 15 (1909), 338—347). Первое из приведенных нами доказательств есть оригинальное доказательство Шевалле [16]. Второе доказательство принадлежит Аксу [3], и его можно найти в [37] и [68]. Доказательство Варнинга более сильного результата можно найти в его статье [78], а также в [9].

В 1884 г. Мейер смог доказать, что квадратичная форма над полем рациональных чисел от пяти или более переменных имеет рациональный нуль, если она имеет вещественный нуль. Хассе смог доказать, что тот же самый результат, соответствующим образом обобщенный, верен над любым полем алгебраических чисел. Исходя из этого и из других рассмотрений, Артин пришел к гипотезе о том, что над некоторым классом числовых полей форма степени d от $n > d^2$ переменных всегда имеет нетривиальный нуль. Он также высказал аналогичные гипотезы для других типов полей. Обсуждение этого круга вопросов см. в статье [53], а также в книге [37], в которой содержатся контрпримеры к гипотезе Артина для p-адических полей, которые были открыты в 1966 г. Тершаняном. Другие контрпримеры были получены вскоре после этого Мануэлем [1]). Многое еще предстоит открыть в этой области, которая является одной из наиболее захватывающих в современной теории чисел.

Для случая когда основное поле есть поле рациональных функций над конечным полем, гипотеза Артина, упомянутая выше, была доказана Карлитцом [11]. Кроме того, если F — конечное поле и $K = F(x)$, то каждая форма степени d от более чем d^2 переменных имеет нетривиальный нуль в K. В доказательстве искусно используется теорема Шевалле, доказанная в этой главе. Этот результат является частным случаем общего результата Ленга (см. [53]. — *Ред.*).

Многие из наиболее важных достижений в теории чисел требуют основательного знания современной алгебраической геометрии. В качестве не слишком сложного введения в алгебраическую геометрию можно порекомендовать [135]. Более насыщенное введение имеется в [219]. Наконец, читателю с хорошим знанием коммутативной алгебры мы рекомендуем [144].

Упражнения

1. Показать, что если K — бесконечное поле и $f(x_1, x_2, \ldots, x_n)$ — ненулевой многочлен с коэффициентами из K, то f не является тождественным нулем на $A^n(K)$. [*Указание.* Доказательство аналогично доказательству леммы 1 из § 2.]

[1]) С другой стороны, Акс и Кохэн, используя средства математической логики, показали, что для любой степени d существует такое конечное множество $c(d)$ простых чисел, что гипотеза Артина верна для форм степени d над полями p-адических чисел с $p \notin c(d)$ [1*]. — *Прим. ред.*

2. В § 1 утверждалось, что H, бесконечно удаленная гиперплоскость в $P^n(F)$, имеет структуру пространства $P^{n-1}(F)$. Проверить это построением взаимно однозначного отображения из $P^{n-1}(F)$ на H.

3. Предположим, что поле F имеет q элементов. Воспользоваться разложением $P^n(F)$ на конечные и бесконечно удаленные точки для получения другого доказательства формулы для числа точек в $P^n(F)$.

4. Гиперповерхность, определенная однородным многочленом $a_0x_0 + a_1x_1 + \cdots + a_nx_n$ степени 1, называется гиперплоскостью. Показать, что любая гиперплоскость в $P^n(F)$ имеет то же число точек, что и $P^{n-1}(F)$.

5. Пусть $f(x_0, x_1, x_2)$ — однородный многочлен степени n в $F[x_0, x_1, x_2]$. Предположим, что не каждый нуль многочлена $a_0x_0 + a_1x_1 + a_2x_2$ является нулем f. Доказать, что в $P^2(F)$ имеется, самое большее, n общих нулей многочленов f и $a_0x_0 + a_1x_1 + a_2x_2$. Геометрически это означает, что кривая степени n и прямая имеют не более n общих точек за исключением случая, когда прямая содержится в кривой.

6. Пусть F — поле из q элементов. Пусть $M_n(F)$ — множество $(n \times n)$-матриц с коэффициентами из F. Пусть $SL_n(F)$ — подмножество матриц с определителем 1. Показать, что $SL_n(F)$ можно рассматривать как гиперповерхность в $A^{n^2}(F)$. Найти формулу для числа точек этой гиперповерхности. [*Ответ.* $(q-1)^{-1}(q^n-1)(q^n-q)\ldots(q^n-q^{n-1})$.]

7. Пусть $f \in F[x_0, x_1, x_2, \ldots, x_n]$. Можно формально определить частные производные $\partial f/\partial x_0, \partial f/\partial x_1, \ldots, \partial f/\partial x_n$. Предположим, что f — форма степени m. Доказать, что $\sum_{i=0}^{n} x_i(\partial f/\partial x_i) = mf$. Этот результат принадлежит Эйлеру. [*Указание.* Рассмотреть сначала случай, когда f — одночлен.]

8 (продолжение). Пусть f — однородный многочлен. Точка $\bar{a}$ на гиперповерхности, определенной f, называется *особой*, если она одновременно является нулем всех частных производных функции f. Показать, что если степень многочлена f взаимно проста с характеристикой, то общий нуль всех частных производных будет автоматически нулем f.

9. Показать, что если m взаимно просто с характеристикой поля F, то гиперповерхность, определенная многочленом $a_0x_0^m + a_1x_1^m + \cdots + a_nx_n^m$, не имеет особых точек.

10. Некоторая точка на аффинной гиперповерхности называется *особой*, если соответствующая ей точка на проективном замыкании особая. Показать, что это эквивалентно следующему определению. Пусть $f \in F[x_1, x_2, \ldots, x_n]$ не обязательно однороден и $a \in H_f(F)$. Тогда a — особая точка, если она является общим нулем для $\partial f/\partial x_i$, $i = 1, 2, \ldots, n$.

11. Показать, что начало координат является особой точкой на кривой, определенной уравнением $y^2 - x^3 = 0$.

12. Показать, что кривая, определенная уравнением $x^2 + y^2 + x^2y^2 = 0$, имеет две бесконечно удаленные точки и что обе они особые.

13. Предположим, что характеристика поля F отлична от 2, и рассмотрим кривую, определенную уравнением $ax^2 + bxy + cy^2 = 1$, где $a, b, c \in F^*$. Показать, что если $b^2 - 4ac \notin F^2$, то в $P^2(F)$ не существует бесконечно удаленных точек, лежащих на кривой. Если $b^2 - 4ac \in F^2$, то показать, что существует одна или две бесконечно удаленных точки в зависимости от того, будет $b^2 - 4ac = 0$ или нет. Если $b^2 - 4ac = 0$, то показать, что бесконечно удаленная точка на кривой особая.

14. Рассмотрим кривую, определенную уравнением $y^2 = x^3 + ax + b$. Показать, что она не имеет особых точек (конечных или бесконечных), если $4a^3 + 27b^2 \neq 0$.

15. Пусть $\mathbf{Q}$ — поле рациональных чисел и p — простое число. Показать, что форма

$$x_0^{n+1} + px_1^{n+1} + p^2x_2^{n+1} + \cdots + p^n x_n^{n+1}$$

не имеет нулей в $P^n(\mathbf{Q})$. [*Указание.* Если $\bar{a}$ — нуль формы, то можно предполагать, что компоненты a — целые числа и что они не все делятся на p.]

16. Показать, что для каждого $m > 0$ и конечного поля F_q существует форма степени m от m переменных без нетривиального нуля. [*Указание.* Показать, что если $\omega_1, \omega_2, \ldots, \omega_m$ — базис для F_{q^m} над F_q, то

$$f(x_1, x_2, \ldots, x_m) = \prod_{i=0}^{m-1} (\omega_1^{q^i} x_1 + \cdots + \omega_m^{q^i} x_m)$$

обладает требуемыми свойствами.]

17. Пусть $g_1, g_2, \ldots, g_m \in F_q[x_1, x_2, \ldots, x_n]$ — однородные многочлены степени d и $n > md$. Доказать, что для них существует общий нетривиальный нуль. [*Указание.* Для многочлена из упр. 17 рассмотреть многочлен $f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$.]

18. Охарактеризовать те расширения F_{p^n} поля F_p, для которых след тождественно равен нулю на F_p.

19. Показать, что если $\alpha \in F_q$ имеет нулевой след, то $\alpha = \beta - \beta^p$ при некотором $\beta \in F_q$.

20. Пусть ψ — отображение из F_q в $\mathbf{C}^*$, для которого $\psi(\alpha + \beta) = \psi(\alpha)\psi(\beta)$ при всех $\alpha, \beta \in F_q$. Показать, что существует такое $\gamma \in F_q$, что $\psi(x) = \zeta^{\mathrm{tr}(\gamma x)}$ при всех $x \in F_q$, где $\zeta = e^{2\pi i/p}$.

21. Показать, что для суммы Гаусса $g_\alpha(\chi)$ на F_q, определенной в § 3,

(a) $g_\alpha(\chi) = \overline{\chi(\alpha)}\, g(\chi)$;

(b) $g(\chi^{-1}) = g(\bar{\chi}) = \chi(-1)\, \overline{g(\chi)}$;

(c) $|g_\alpha(\chi)| = q^{1/2}$;

(d) $g(\chi)\, g(\chi^{-1}) = \chi(-1)\, q$.

22. Предположим, что f — функция, отображающая F в $\mathbf{C}$. Положить $\hat{f}(s) = (1/q) \sum_t f(t)\, \overline{\psi(st)}$ и доказать, что $f(t) = \sum_s \hat{f}(s)\psi(st)$. Последняя сумма называется *разложением f в конечную сумму Фурье.*

23. В упр. 23 в качестве f взять нетривиальный характер χ и показать, что $\hat{\chi}(s) = (1/q)\, g_{-s}(\chi)$.

Глава 11

ДЗЕТА-ФУНКЦИЯ

Дзета-функция алгебраического многообразия сыграла доминирующую роль в современном развитии диофантовой геометрии.

Для одного класса кривых над конечным полем понятие дзета-функции было введено Артином в 1924 *г. По аналогии с классической дзета-функцией Римана он предположил, что для определенных им функций справедлива гипотеза Римана. В частных случаях он смог ее доказать. Замечательно, что результаты такого типа можно найти уже у Гаусса (конечно, Гаусс формулировал свои результаты иначе, чем Артин). Вейль смог доказать (в* 1948 *г.), что гипотеза Римана для неособых кривых над конечным полем справедлива в общем виде.*

В 1949 *г. Вейль опубликовал в журнале* «Bulletin of the American Mathematical Society» *статью, озаглавленную «Число решений уравнений над конечными полями». В этой статье он определил дзета-функцию для алгебраического многообразия и выдвинул ряд гипотез. Вейль также доказал справедливость своих гипотез для кривых. Те же результаты были получены им для одного класса проективных гиперповерхностей. Часть этого материала будет изложена далее. Большая часть необходимых средств уже была изложена. Основной новый результат, который будет нам нужен, — это соотношение Хассе — Дэвенпорта между суммами Гаусса. Доказательство этого соотношения, данное Вейлем, существенно проще оригинального. Мы приведем доказательство, принадлежащее Монски, которое еще проще, чем доказательство Вейля, хотя и далеко не тривиально.*

В 1973 *г. Делиню удалось доказать гипотезы Вейля во всей общности. Его доказательство использует новейшие достижения современной алгебраической геометрии и само представляет собой одно из самых замечательных математических достижений нашего столетия.*

§ 1. Дзета-функция проективной гиперповерхности

В § 2 гл. 7 мы показали, что если $F = \mathbf{Z}/p\mathbf{Z}$ и $s \geqslant 1$ — целое число, то существует содержащее F поле K из p^s элементов. Тот же результат остается верным в общем случае. А именно, если F —

конечное поле из q элементов и $s \geqslant 1$ — целое число, то существует содержащее F поле F_s из q^s элементов (это поле в наших прежних обозначениях есть F_{q^s}). Доказательство в общем случае почти совпадает с доказательством в частном случае (см. упражнения к гл. 7).

Пусть теперь $f(y) \in F[y_0, y_1, \ldots, y_n]$ — однородный многочлен и N_s — число точек на проективной гиперповерхности $\bar{H}_f(F_s) \subset P^n(F_s)$. Другими словами, N_s есть число нулей многочлена f в $P^n(F_s)$. Мы хотим исследовать, как числа N_s зависят от s.

В конце этого параграфа мы докажем, что N_s зависит лишь от s, а не от поля F_s. Это получится сразу же, как только мы покажем, что любые два поля, содержащие F и имеющие одинаковую размерность над F, изоморфны.

Для изучения чисел N_s мы вводим степенной ряд $\sum_{s=1}^{\infty} N_s u^s$. Во всех дальнейших рассмотрениях можно иметь дело лишь с формальными степенными рядами и, таким образом, избежать всех вопросов о сходимости. Для тех, кому это понятие непривычно, заметим, что $N_s \leqslant (q^{s(n+1)} - 1)/(q^s - 1) < (n+1)\, q^{sn}$. Отсюда следует, что наш ряд сходится для всех комплексных чисел u, таких, что $|u| < q^{-n}$, и определяет в этом круге аналитическую функцию.

Пусть $\exp u = 1 + \sum_{s=1}^{\infty} (1/s!)\, u^s$.

Определение. *Дзета-функция гиперповерхности*, определенной многочленом f (или *дзета-функция многочлена* f), есть ряд

$$Z_f(u) = \exp\left(\sum_{s=1}^{\infty} \frac{N_s u^s}{s}\right).$$

$Z_f(u)$ можно рассматривать либо как формальный степенной ряд, либо как функцию комплексной переменной, определенную и аналитическую в круге $\{u \in \mathbf{C} \mid |u| < q^{-n}\}$.

Может показаться странным обращение к $Z_f(u)$ вместо того, чтобы прямо рассматривать ряд $\sum_{s=1}^{\infty} N_s u^s$. Причины, главным образом, исторического характера, хотя, как мы увидим, с дзета-функцией легче иметь дело. См. замечания в конце этого параграфа.

В качестве первого примера рассмотрим бесконечно удаленную гиперплоскость. По определению это множество точек $[a_0, a_1, \ldots, a_n] \in P^n(F)$ с $a_0 = 0$. Оно определяется уравнением $x_0 = 0$.

Как мы отмечали в гл. 10, нетрудно убедиться в том, что $\overline{H}_{x_0}(F_s)$ имеет то же число точек, что и $P^{n-1}(F(s))$, т. е.

$$N_s = q^{s(n-1)} + q^{s(n-2)} + \cdots + q^s + 1.$$

Отсюда следует, что

$$\sum_{s=1}^{\infty} \frac{N_s u^s}{s} = \sum_{m=0}^{n-1} \left(\sum_{s=1}^{\infty} \frac{(q^m u)^s}{s} \right) = -\sum_{m=0}^{n-1} \ln(1 - q^m u). \qquad (1)$$

Мы воспользовались тождеством $\sum_{s=1}^{\infty} w^s/s = \ln(1-w)$. Возведение e в степень обеих частей равенства (1) приводит к

$$Z_{x_0}(u) = (1 - q^{n-1}u)^{-1}(1 - q^{n-2}u)^{-1} \ldots (1 - qu)^{-1}(1 - u)^{-1}.$$

В частности, мы видим, что $Z_{x_0}(u)$ — рациональная функция от u.

Мы произведем сейчас вычисления для более сложного примера. Рассмотрим гиперповерхность, определенную уравнением $-y_0^2 + y_1^2 + y_2^2 + y_3^2 = 0$. Для вычисления N_1 воспользуемся теоремой 2 из гл. 10. Сводя ее к нашему частному случаю, получаем, что

$$N_1 = q^2 + q + 1 + \chi(-1)\frac{1}{q} g(\chi)^4,$$

где χ — характер порядка 2 на F. Как мы знаем, $g(\chi)^2 = \chi(-1)q$. *Таким образом*, $N_1 = q^2 + q + 1 + \chi(-1)q$.

Для вычисления N_s мы должны заменить q на q^s и χ на χ_s, характер порядка 2 на F_s:

$$N_s = q^{2s} + q^s + 1 + \chi_s(-1)q^s.$$

Если -1 есть квадрат в F, то $\chi_s(-1) = 1$ для всех s. Если -1 — не квадрат в F, то, как нетрудно видеть, $\chi_s(-1) = -1$ для нечетных s и $\chi_s(-1) = 1$ для четных s.

В первом случае

$$\sum_{s=1}^{\infty} \frac{N_s u^s}{s} = \sum_{s=1}^{\infty} \frac{(q^2u)^s}{s} + 2\sum_{s=1}^{\infty} \frac{(qu)^s}{s} + \sum_{s=1}^{\infty} \frac{u^s}{s},$$

так что

$$Z(u) = (1 - q^2u)^{-1}(1 - qu)^{-2}(1 - u)^{-1}.$$

Во втором случае последний член приводит к сумме

$$\sum_{s=1}^{\infty} \frac{(-qu)^s}{s} = -\ln(1 + qu).$$

Таким образом, в этом случае

$$Z(u) = (1 - q^2u)^{-1}(1 - qu)^{-1}(1 + qu)^{-1}(1 - u)^{-1}.$$

Заметим, что в первом случае дзета-функция имеет полюс в $u = q^{-1}$ порядка 2, в то время как во втором случае в $u = q^{-1}$ имеется полюс порядка 1. Это находится в соответствии с гипотезой Тейта, связывающей порядок полюса в $u = q^{-1}$ с определенными геометрическими свойствами гиперповерхности. Мы не можем останавливаться более подробно на этом вопросе [1]).

В качестве последнего примера рассмотрим кривую $y_0^3 + y_1^3 + y_2^3 = 0$ над $F = \mathbf{Z}/p\mathbf{Z}$, где p — простое число, сравнимое с 1 по модулю 3.

Опять применяя для нашего случая теорему 2 гл. 10, находим, что

$$N_1 = p + 1 + \frac{1}{p} g(\chi)^3 + \frac{1}{p} g(\chi^2)^3.$$

Здесь χ — кубический характер на $\mathbf{Z}/p\mathbf{Z}$. Мы знаем, что $g(\chi)^3 = p\pi$, где $\pi = J(\chi, \chi)$ и $\pi\bar{\pi} = p$. Таким образом,

$$N_1 = p + 1 + \pi + \bar{\pi}.$$

Из соотношения Хассе — Дэвенпорта, которое будет доказано позже, следует, что

$$N_s = p^s + 1 - (-\pi)^s - (-\bar{\pi})^s.$$

Вычисление показывает, что

$$Z_f(u) = \frac{(1 + \pi u)(1 + \bar{\pi} u)}{(1 - u)(1 - pu)}.$$

---

[1]) В алгебраической геометрии с каждым неособым алгебраическим многообразием связывают группу классов дивизоров (подмногообразий коразмерности один) относительно линейной эквивалентности — группу Пикара. Ее конструкция является обобщением рассматриваемой в гл. 12 конструкции группы классов идеалов кольца целых алгебраических чисел (подробности см. в [144], гл. 2, § 6, или в [219], гл. 3, § 1—3). Группа Пикара поверхности над конечным полем конечно порождена, и гипотеза Тейта утверждает, что ее ранг равен порядку полюса дзета-функции поверхности в точке $u = q^{-1}$ (см. [226] и [21*]). В нашей ситуации поверхность в первом случае является распадающейся квадрикой, т. е. изоморфна над основным полем $P^1 \times P^1$, и ее группа Пикара имеет вид $\mathbf{Z}e_1 \oplus \mathbf{Z}e_2$, где e_1, e_2 — классы прямых P^1 из приведенного выше изоморфизма. Во втором случае квадрика распадается лишь над квадратичным расширением основного поля и ее группа Пикара равна $\mathbf{Z}e$ (класс e связан с диагональю в соответствующем разложении в произведение P^1 и P^1). — *Прим. ред.*

Числитель может быть вычислен явно. В гл. 8 мы доказали, что $\pi + \bar{\pi} = A$, где A однозначно определено условием $4p = A^2 + 27B^2$ и $A \equiv 1 \pmod 3$ (3).

Таким образом, окончательное выражение есть

$$Z_f(u) = \frac{1 + Au + pu^2}{(1-u)(1-pu)}.$$

В этом примере $Z_f(u)$ — рациональная функция; ее числитель и знаменатель суть многочлены с целыми коэффициентами. Нули функции $Z_f(u)$ — числа π^{-1}, $\bar{\pi}^{-1}$ — оба имеют абсолютную величину $p^{-1/2}$.

В более общем виде пусть $f(x_0, x_1, x_2) \in F[x_0, x_1, x_2]$ — ненулевой однородный многочлен, неособый над любым алгебраическим расширением поля F. В этом случае Вейль смог доказать, что дзета-функция многочлена f имеет вид

$$\frac{P(u)}{(1-u)(1-qu)},$$

где $P(u)$ — многочлен с целыми коэффициентами степени $(d-1)(d-2)$, причем d — степень f. Кроме того, если α — корень многочлена $P(u)$, то $|\alpha| = q^{-1/2}$ [1]). Последнее утверждение называется гипотезой Римана для кривых.

[Чтобы увидеть связь с классической гипотезой Римана, сделаем замену переменных $u = q^{-s}$ и положим $\zeta_f(s) = Z_f(q^{-s})$. Функция $\zeta_f(s)$ — прямой аналог классической дзета-функции (см. конец этого параграфа). Условие, что корни $Z_f(u)$ имеют абсолютное значение $q^{-1/2}$, эквивалентно условию, что вещественная часть корней $\zeta_f(s)$ равна 1/2.]

Во всех рассмотренных примерах дзета-функция рациональна. В 1959 г. Дворк доказал, что любое алгебраическое множество имеет рациональную дзета-функцию [26]. Его доказательство исключительно красиво, но, к сожалению, основано на методах, лежащих вне рамок этой книги.

Наши примеры наводят на мысль дать другую характеризацию условия того, что дзета-функция рациональна.

Непосредственно из определения следует, что если дзета-функция разложена в степенной ряд около начала координат, то его постоянный член равен 1. Следовательно, если $Z_f(u) = P(u)/Q(u)$, где $P(u)$ и $Q(u)$ — многочлены, то можно предполагать, что

---

[1]) Отсюда легко следует, что $|N - q - 1| \leqslant 2g\sqrt{q}$, где N — число точек, определенных над конечным полем F_q, неособой проективной кривой рода g. В настоящее время известны более точные оценки. Так, Ж.-П. Серр доказал, что $|N - q - 1| \leqslant g[2\sqrt{q}]$ (см. [30*]). — *Прим. ред.*

$P(0) \cdot Q(0) = 1$ (доказать это). При таком предположении дзета-функция может быть разложена на множители следующим образом:

$$Z_j(u) = \frac{\prod_i (1-\alpha_i u)}{\prod_j (1-\beta_j u)},$$

где $\alpha_i, \beta_j \in \mathbf{C}$. Мы можем теперь доказать

Предложение 11.1.1. *Дзета-функция рациональна тогда и только тогда, когда существуют комплексные числа α_i и β_j, для которых*

$$N_s = \sum_j \beta_j^s - \sum_i \alpha_i^s.$$

Доказательство. Предположим, что дзета-функция рациональна. Тогда по сделанному выше замечанию

$$Z(u) = \frac{\prod_i (1-\alpha_i u)}{\prod_j (1-\beta_j u)},$$

где $\alpha_i, \beta_j \in \mathbf{C}$. Возьмем логарифмические производные от обеих частей:

$$\frac{Z'(u)}{Z(u)} = \sum_i \frac{-\alpha_i}{1-\alpha_i u} - \sum_j \frac{-\beta_j}{1-\beta_j u}.$$

Умножим обе части этого равенства на u и воспользуемся формулой геометрической прогрессии для разложения в степенные ряды. В результате получим

$$\frac{uZ'(u)}{Z(u)} = \sum_{s=1}^{\infty} \left(\sum_j \beta_j^s - \sum_i \alpha_i^s \right) u^s. \tag{2}$$

Вычислим теперь левую часть другим способом. По определению

$$Z(u) = \exp \sum_{s=1}^{\infty} \frac{N_s u^s}{s}.$$

Взяв логарифмическую производную от обеих частей и умножив затем обе части на u, получим

$$\frac{uZ'(u)}{Z(u)} = \sum_{s=1}^{\infty} N_s u^s. \tag{3}$$

Сравнивая коэффициенты при u^s в равенствах (2) и (3), приходим к соотношению

$$N_s = \sum_j \beta_j^s - \sum_i \alpha_i^s.$$

Обратное утверждение следует из прямого подсчета, который мы уже проделывали в частных случаях. Восстановить детали предоставляется читателю. □

Остается доказать, что число N_s не зависит от выбора поля F_s. Читатель может просто принять этот факт на веру и перейти к § 2.

Предположим, что E и E' — два поля, содержащие F, и оба состоят из q^s элементов.

Предложение 11.1.2. *E и E' изоморфны над F, т. е. существует такое отображение $\sigma\colon E \to E'$, что*

(a) *σ взаимно однозначно и эпиморфно;*

(b) *$\sigma(a) = a$ для всех $a \in F$;*

(c) *$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ для всех $\alpha, \beta \in E$;*

(d) *$\sigma(\alpha\beta) = \sigma(\alpha)\,\sigma(\beta)$ для всех $\alpha, \beta \in E$.*

Доказательство. Мы покажем, что оба поля E и E' изоморфны над F полю $F[x]/(f(x))$ для некоторого неприводимого многочлена $f(x) \in F[x]$.

Для начала отметим, что существует такое $\alpha' \in E'$, что $E' = F(\alpha')$ (например, можно в качестве α' взять примитивный корень степени $q^s - 1$ из единицы). Пусть $f(x) \in F[x]$ — приведенный неприводимый многочлен для α'. Тогда $E' \approx F[x]/(f(x))$. Так как α' удовлетворяет уравнению $x^{q^s} - x = 0$, то $f(x) \mid x^{q^s} - x$.

Так как E имеет q^s элементов, то $x^{q^s} - x = \prod_{\alpha \in E} (x - \alpha)$. Отсюда следует, что $f(\alpha) = 0$ для некоторого $\alpha \in E$.

Таким образом, $F(\alpha) \approx F[x]/(f(x))$ будет подполем в E, состоящим из q^s элементов. Отсюда получаем, что $E = F(\alpha) \approx \approx F[x]/(f(x)) \approx F(\alpha') = E'$. □

Мы можем теперь использовать введенный изоморфизм σ для построения отображения $\bar{\sigma}$ из $P^n(E)$ в $P^n(E')$. А именно, полагаем

$$\bar{\sigma}([\alpha_0, \ldots, \alpha_n]) = [\sigma(\alpha_0), \ldots, \sigma(\alpha_n)].$$

$\bar{\sigma}$ взаимно однозначно и сюръективно. Кроме того, если $f(y_0, y_1, \ldots, y_n) \in F[y_0, y_1, \ldots, y_n]$, то $\bar{\sigma}$, ограниченное на проективную гиперповерхность $\bar{H}_f(E)$, будет отображать ее на проективную гиперповерхность $\bar{H}_f(E')$. Это доказывает независимость чисел N_s от выбора поля F_s. Проверка деталей предоставляется читателю.

Мы закончим этот параграф обсуждением аналогии между конгруэнц-дзета-функцией и дзета-функцией Римана.

Дзета-функция Римана $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ может быть записана в силу фундаментальной теоремы арифметики в виде бесконечного произведения $\prod_p (1 - p^{-s})^{-1}$ по всем простым числам p (см. упр. 25 из гл. 2). Мы получим аналогичное бесконечное произведение для $Z_f(u)$ по определенным объектам, называемым простыми дивизорами соответствующего алгебраического множества. Это будет сделано с минимальным использованием техники алгебраической геометрии.

Если F — конечное поле из q элементов, то рассмотрим произвольное алгебраическое множество V в $A^n(F)$. Как в начале параграфа, мы можем тогда определить дзета-функцию V над F как

$$\exp\left(\sum_{s=1}^{\infty} \frac{N_s u^s}{s}\right),$$

где N_s — число точек в $A^n(F_{q^s})$, удовлетворяющих уравнениям, определяющим V. Мы рассматриваем аффинное алгебраическое множество, а не проективное алгебраическое множество лишь для упрощения рассуждений. Кроме того, удобно работать с одним полем $K \supset F$, которое алгебраично над F и содержит расширение степени s поля F для каждого целого числа $s \geqslant 1$. Из предложения 7.1.1 следует, что K тогда содержит точно одно поле, имеющее q^s элементов. Простое построение такого поля проводится в упражнениях. Это поле определяется однозначно с точностью до изоморфизма и называется *алгебраическим замыканием* поля F. Мы можем тогда рассматривать $A^n(K)$ и расширить V до алгебраического множества, все еще обозначаемого через V, в $A^n(K)$ с N_s точками, координаты которых лежат в F_{q^s}.

Если $\alpha = (a_1, a_2, \ldots, a_n) \in V$, то пусть F_{q^d} — наименьшее подполе, содержащее F и $a_1, a_2, \ldots, a_n$. Мы говорим, что α — точка *степени* d. Так как $a^q = a$ для $a \in F$, то точки α, α^q, α^{q^2}, ..., $\alpha^{q^{d-1}}$ тоже лежат в V, где возведение в степень означает возведение каждой координаты в соответствующую степень. Кроме того, эти точки различны (в силу, скажем, следствия к предложению 7.1.1).

Определение. *Простой дивизор* на V есть множество вида $\{\alpha^{q^j} \mid j = 0, 1, 2, \ldots, d-1\}$, где α — точка на V степени d.

Простые дивизоры традиционно обозначаются через $\mathfrak{P}$. Степень дивизора $\mathfrak{P}$, $\deg \mathfrak{P}$, есть d.

Простые дивизоры, как нетрудно убедиться, расслаивают $V \subset A^n(K)$. Кроме того, если α — точка на V с координатами из F_{q^s}, то она, согласно предложению 7.1.5, определяет единственный простой дивизор $\mathfrak{P}$ степени d для некоторого $d \mid s$. Этот простой дивизор содержит d точек множества V, координаты которых принадлежат F_{q^s}. Если обозначить через a_d число простых дивизоров на V степени d (это число конечно), то, согласно предыдущему, справедлив следующий важный результат.

Лемма 1. $N_s = \sum_{d \mid s} d a_d$.

Теперь мы можем сформулировать основной результат этого параграфа.

Предложение 11.1.3. $Z_V(u) = \prod_{\mathfrak{P}} (1/(1 - u^{\deg \mathfrak{P}}))$.

Доказательство. Правая часть, очевидно, равна

$$\prod_{n=1}^{\infty} \left(\frac{1}{1-u^n}\right)^{a_n}.$$

Логарифмическая производная этого выражения есть

$$\frac{1}{u} \sum_{n=1}^{\infty} \frac{n a_n u^n}{1-u^n}.$$

Разлагая знаменатель в геометрическую прогрессию и вычисляя коэффициент при u^m, получаем

$$\frac{1}{u} \sum_{m=1}^{\infty} \left(\sum_{d \mid m} d a_d\right) u^m,$$

что, согласно лемме 1, превращается в

$$\sum_{m=1}^{\infty} N_m u^{m-1}.$$

Интегрирование и взятие степени приводит к нужному результату. □

Этот результат показывает, что $Z(u)$ имеет целые коэффициенты. Аналогия с дзета-функцией Римана становится еще более прозр-

рачной, если ввести новую переменную s, связанную с u соотношением $u = q^{-s}$. Тогда

$$Z(q^{-s}) = \prod_{\mathfrak{P}} \left(\frac{1}{1 - q^{-s \deg \mathfrak{P}}} \right) = \prod_{\mathfrak{P}} \left(\frac{1}{1 - (1/N(\mathfrak{P})^s)} \right),$$

что совершенно аналогично дзета-функции Римана.

§ 2. След и норма в конечных полях

В § 3 гл. 10 было введено понятие следа. Здесь мы это понятие обобщаем и, кроме того, определяем норму в конечных полях.

Пусть F — конечное поле из q элементов и E — содержащее F поле из q^s элементов.

Определение. Если $\alpha \in E$, то *след* элемента α из E в F определяется как

$$\mathrm{tr}_{E/F}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{s-1}}.$$

Норма элемента α из E в F определяется как

$$N_{E/F}(\alpha) = \alpha \cdot \alpha^q \ \ldots \ \alpha^{q^{s-1}}.$$

Следующие два предложения описывают основные свойства следа и нормы.

Предложение 11.2.1. *Если* $\alpha, \beta \in E$ *и* $a \in F$, *то*
(a) $\mathrm{tr}_{E/F}(\alpha) \in F$;
(b) $\mathrm{tr}_{E/F}(\alpha + \beta) = \mathrm{tr}_{E/F}(\alpha) + \mathrm{tr}_{E/F}(\beta)$;
(c) $\mathrm{tr}_{E/F}(a\alpha) = a\,\mathrm{tr}_{E/F}(\alpha)$;
(d) $\mathrm{tr}_{E/F}$ *отображает* E *на* F.

Предложение 11.2.2. *Если* $\alpha, \beta \in E$ *и* $a \in F$, *то*
(a) $N_{E/F}(\alpha) \in F$;
(b) $N_{E/F}(\alpha\beta) = N_{E/F}(\alpha)\, N_{E/F}(\beta)$;
(c) $N_{E/F}(a\alpha) = a^s N_{E/F}(\alpha)$;
(d) $N_{E/F}$ *отображает* E^* *на* F^*.

Доказательство. Доказательство предложения 11.2.1 совершенно аналогично доказательству предложения 10.3.1 и будет опущено.

Для доказательства предложения 11.2.2 заметим, что

$$N_{E/F}(\alpha)^q = (\alpha \cdot \alpha^q \ \ldots \ \alpha^{q^{s-1}})^q = \alpha^q \cdot \alpha^{q^2} \ \ldots \ \alpha^{q^s} = N_{E/F}(\alpha).$$

Таким образом, $N_{E/F}(\alpha) \in F$.

Далее,

$$N_{E/F}(\alpha\beta) = (\alpha\beta)\cdot(\alpha\beta)^q \cdot \ldots \cdot (\alpha\beta)^{q^{s-1}} =$$

$$= (\alpha\cdot\alpha^q \cdot \ldots \cdot \alpha^{q^{s-1}})\cdot(\beta\cdot\beta^q \cdot \ldots \cdot \beta^{q^{s-1}}) = N_{E/F}(\alpha)\, N_{E/F}(\beta).$$

Это доказывает п. (b).

Для доказательства п. (c) заметим, что $N_{E/F}(a) = a\cdot a^q \cdot \ldots \cdot a^{q^{s-1}} = a^s$ для $a \in F$, так как $a^q = a$. Далее следует применить п. (b).

Наконец, рассмотрим ядро гомоморфизма $N_{E/F}$, т. е. множество всех $\alpha \in E$, для которых $N_{E/F}(\alpha) = 1$. Элемент α принадлежит ядру тогда и только тогда, когда

$$1 = \alpha\cdot\alpha^q\cdot \ldots \cdot\alpha^{q^{s-1}} = \alpha^{1+q+\ldots+q^{s-1}} = \alpha^{(q^s-1)/(q-1)}.$$

Так как $(q^s - 1)/(q - 1) \mid q^s - 1$, то из предложения 7.1.2 следует, что уравнение $x^{(q^s-1)/(q-1)} = 1$ имеет $(q^s - 1)/(q - 1)$ решений в E. Согласно элементарной теории групп, образ $N_{E/F}(E^*)$ имеет $q - 1$ элементов, что в точности совпадает с числом элементов в F^*. Следовательно, $N_{E/F}$ сюръективно. □

Для заданной башни полей $F \subset E \subset K$ имеем соотношение $[K : F] = [K : E]\,[E : F]$. Этот результат нетрудно доказать в общем виде. Если все три поля конечны, его можно доказать следующим образом. Пусть q — число элементов в F. Тогда число элементов в E и число элементов в K суть $q^{[E:F]}$ и $q^{[K:F]}$ соответственно. Рассматривая K как расширение E, мы можем выразить число элементов в нем как $(q^{[E:F]})^{[K:E]}$. Таким образом,

$$q^{[K:F]} = q^{[E:F]\,[K:E]},$$

а потому $[K : F] = [E : F]\,[K : E]$.

Мы теперь можем доказать еще одно свойство следа и нормы, которое будет полезно в дальнейшем.

Предложение 11.2.3. *Пусть $F \subset E \subset K$ — три конечных поля и $\alpha \in K$. Тогда*

(a) $\mathrm{tr}_{K/F}(\alpha) = \mathrm{tr}_{E/F}(\mathrm{tr}_{K/E}(\alpha))$;

(b) $N_{K/F}(\alpha) = N_{E/F}(N_{K/E}(\alpha))$.

Доказательство. Мы докажем лишь свойство (a). Доказательство свойства (b) аналогично.

Пусть $d = [E : F]$, $m = [K : E]$ и $n = [K : F]$. Как было отмечено выше, $n = dm$.

Число элементов в E есть $q_1 = q^d$. Таким образом,

$$\mathrm{tr}_{K/E}(\alpha) = \alpha + \alpha^{q_1} + \ldots + \alpha^{q_1^{m-1}}$$

и

$$\mathrm{tr}_{E/F}(\mathrm{tr}_{K/E}(\alpha)) = \sum_{i=0}^{d-1} \mathrm{tr}_{K/E}(\alpha)^{q^i} = \sum_{i=0}^{d-1}\sum_{j=0}^{m-1} \alpha^{q_1^j q^i} =$$
$$= \sum_{i=1}^{d-1}\sum_{j=0}^{m-1} \alpha^{q^{dj+i}} = \sum_{k=0}^{n-1} \alpha^{q^k} = \mathrm{tr}_{K/F}(\alpha).$$

Мы воспользовались тем фактом, что, когда j меняется от 0 до $m-1$ и i меняется от 0 до $d-1$, величина $dj+i$ меняется от 0 до $md-1 = n-1$. □

Предположим теперь, что $F \subset K$ — конечные поля, $n = [K : F]$ и $\alpha \in K$. Пусть $E = F(\alpha)$ и $f(x) \in F[x]$ — минимальный многочлен для α над F. Согласно следствию предложения 7.2.2, $[E : F] = d$, где d — степень многочлена $f(x)$.

Предложение 11.2.4. *Запишем* $f(x) = x^d - c_1 x^{d-1} + \ldots + (-1)^d c_d$. *Тогда*

(a) $f(x) = (x-\alpha)(x-\alpha^q)\ \ldots\ (x-\alpha^{q^{d-1}})$;

(b) $\mathrm{tr}_{K/F}(\alpha) = (n/d)\, c_1$;

(c) $N_{K/F}(\alpha) = c_d^{n/d}$.

Доказательство. Так как коэффициенты многочлена f удовлетворяют условию $a^q = a$, то

$$0 = f(\alpha)^q = f(\alpha^q).$$

Таким образом, α^q есть корень f. Аналогично,

$$0 = (f(\alpha^q))^q = f(\alpha^{q^2}).$$

Значит, α^{q^2} есть корень f. Продолжая это рассуждение, получаем, что α, α^q, α^{q^2}, ..., $\alpha^{q^{d-1}}$ суть корни f. Если мы сможем показать, что все эти корни различны, то утверждение (a) будет установлено.

Предположим, что $0 \leqslant i \leqslant j < d$ и $\alpha^{q^i} = \alpha^{q^j}$. Положим $k = j - i$. Мы покажем, что $k = 0$.

Имеем

$$\alpha^{q^i} = \alpha^{q^j} = (\alpha^{q^k})^{q^i},$$

откуда следует, что

$$(\alpha - \alpha^{q^k})^{q^i} = 0,$$

а потому

$$\alpha = \alpha^{q^k}.$$

Так как $f(x)$ — минимальный многочлен для α, отсюда следует, что $f(x)$ делит $x^{q^k} - x$, а потому по теореме 1 из гл. 7 имеем $d \mid k$. Но $0 \leqslant k < d$, так что $k = 0$ и утверждение (а) доказано.

Из утверждения (а) непосредственно следует, что $c_1 = \mathrm{tr}_{E/F}(\alpha)$ и $c_d = N_{E/F}(\alpha)$.

Так как $\alpha \in E = F(\alpha)$, то $\mathrm{tr}_{K/E}(\alpha) = [K : E]\,\alpha = (n/d)\,\alpha$ и $N_{K/E}(\alpha) = \alpha^{n/d}$.

В силу предложения 11.2.3

$$\mathrm{tr}_{K/F}(\alpha) = \mathrm{tr}_{E/F}(\mathrm{tr}_{K/E}(\alpha)) = \mathrm{tr}_{E/F}\left(\frac{n}{d}\alpha\right) = \frac{n}{d}\mathrm{tr}_{E/F}(\alpha) = \frac{n}{d}c_1.$$

Аналогично,

$$N_{K/F}(\alpha) = N_{E/F}(N_{K/E}(\alpha)) = N_{E/F}(\alpha^{n/d}) = N_{E/F}(\alpha)^{n/d} = c_d^{n/d}. \quad \square$$

§ 3. Рациональность дзета-функции гиперповерхности

$$a_0x_0^m + a_1x_1^m + \ldots + a_nx_n^m = 0$$

Пусть $f(x_0, x_1, \ldots, x_n)$ обозначает многочлен из заглавия этого параграфа [заметим, что это *не* $f(x)$ из § 2]. Предположим, что его коэффициенты принадлежат F, конечному полю из q элементов, и что $q \equiv 1\ (m)$. Мы должны исследовать число N_s элементов в $\bar{H}_f(F_s)$, где $[F_s : F] = s$. Теорема 2 из гл. 10 показывает, что N_s задается выражением

$$q^{s(n-1)} + q^{s(n-2)} + \ldots + q^s + 1 + \frac{1}{q^s}\sum_{\chi_0^{(s)}, \ldots, \chi_n^{(s)}} \chi_0^{(s)}(a_0^{-1}) \ldots \chi_n^{(s)}(a_n^{-1})\, g(\chi_0^{(s)}) \ldots g(\chi_n^{(s)}), \quad (4)$$

где q^s — число элементов в F_s и $\chi_i^{(s)}$ — такие мультипликативные характеры поля F_s, что $\chi_i^{(s)m} = \varepsilon$, $\chi_i^{(s)} \neq \varepsilon$ и $\chi_0^{(s)}\chi_1^{(s)} \ldots \chi_n^{(s)} = \varepsilon$.

Мы должны проанализировать члены $\chi_i^{(s)}(a_i^{-1})$ и $g(\chi_i^{(s)})$. Для этого мы сначала свяжем характеры поля F_s с характерами поля F.

Пусть χ — некоторый характер поля F, и положим $\chi' = \chi \circ N_{F_s/F}$, т. е. $\chi'(\alpha) = \chi(N_{F_s/F}(\alpha))$ для $\alpha \in F_s$. Тогда, используя предложение 11.2.2, видим, что χ' — характер поля F_s, а, кроме того,

(a) $\chi \neq \rho$ означает, что $\chi' \neq \rho'$;
(b) $\chi^m = \varepsilon$ означает, что $\chi'^m = \varepsilon$;
(c) $\chi'(a) = \chi(a)^s$ для всех $a \in F$.

Отсюда легко следует, что когда χ пробегает характеры поля F порядка, делящего m, то χ' пробегает характеры поля F_s порядка, делящего m.

Сумма в (4) теперь может быть переписана в виде

$$\sum_{\chi_0, \ldots, \chi_n} \chi_0(a_0^{-1})^s \ldots \chi_n(a_n^{-1})^s g(\chi_0') \ldots g(\chi_n'), \qquad (5)$$

где $\chi_0, \ldots, \chi_n$ — характеры поля F, удовлетворяющие условиям $\chi_i^m = \varepsilon$, $\chi_i \neq \varepsilon$ и $\chi_0\chi_1 \ldots \chi_n = \varepsilon$.

Остается проанализировать сумму Гаусса $g(\chi')$. Это составляет содержание следующей теоремы Хассе — Дэвенпорта (см. [23]).

Теорема 1. $(-g(\chi))^s = -g(\chi')$.

Мы отложим доказательство этого соотношения.

Из теоремы 1 и равенств (4) и (5) следует, что N_s задается значением

$$\sum_{k=0}^{n-1} q^{ks} + (-1)^{n+1} \sum_{\chi_0, \chi_1, \ldots, \chi_n} \left[\frac{(-1)^{n+1}}{q} \chi_0(a_0^{-1}) \ldots \right.$$

$$\left. \ldots \chi_n(a_n^{-1})\, g(\chi_0) \ldots g(\chi_n) \right]^s, \qquad (6)$$

где вторая сумма подчинена тем же условиям, что и (5).

Применение предложения 11.1.1 дает основной результат этой главы.

Теорема 2. *Пусть $a_0, a_1, \ldots, a_n \in F^*$, где F — конечное поле из q элементов и $q \equiv 1\ (m)$. Пусть $f(x_0, \ldots, x_n) = a_0x_0^m + a_1x_1^m + \ldots + a_nx_n^m$. Тогда дзета-функция $Z_f(u)$ есть рациональная функция вида*

$$\frac{P(u)^{(-1)^n}}{(1-u)(1-qu)\ldots(1-q^{n-1}u)},$$

где $P(u)$ — многочлен

$$\prod_{\chi_0, \chi_1, \ldots, \chi_n} \left(1 - (-1)^{n+1} \frac{1}{q} \chi_0(a_0^{-1}) \ldots \chi_n(a_n^{-1}) g(\chi_0) g(\chi_1) \ldots g(\chi_n) u\right),$$

причем $(n+1)$-набор $\chi_0, \chi_1, \ldots, \chi_n$ подчинен условиям $\chi_i^m = \varepsilon$, $\chi_i \neq \varepsilon$ и $\chi_0\chi_1 \ldots \chi_n = \varepsilon$.

Сделаем несколько замечаний:

(1) степень многочлена $P(u)$ можно вычислить явно. Она равна

$$m^{-1}[(m-1)^{n+1}+(-1)^{n+1}(m-1)].$$

(2) Так как $|g(\chi)| = q^{1/2}$, то из явного выражения для $P(u)$ следует, что нули $Z_f(u)$ имеют абсолютное значение $q^{-((n-1)/2)}$. Это согласуется с общей гипотезой Римана.

(3) Если записать $P(u) = \prod(1-\alpha u)$, то числа α целые алгебраические.

В этом нетрудно убедиться. Каждое α имеет вид

$$\zeta \frac{1}{q} g(\chi_0) \cdots g(\chi_n),$$

где ζ — корень из единицы и $\chi_0\chi_1 \ldots \chi_n = \varepsilon$. Используя следствие 1 теоремы 3 из гл. 8, мы видим, что

$$\frac{1}{q} g(\chi_0) g(\chi_1) \cdots g(\chi_n) = \chi_n(-1) J(\chi_0, \chi_1, \ldots, \chi_{n-1}).$$

Сумма Якоби есть сумма корней из единицы, а потому целое алгебраическое число.

Таким образом, $\alpha = \zeta\chi_n(-1) J(\chi_0, \chi_1, \ldots, \chi_{n-1})$ — тоже целое алгебраическое число.

Пусть $f(x_0, x_1, \ldots, x_n)$ — однородная форма степени d с коэффициентами в конечном поле F. Кроме того, предположим, что частные производные $f_{x_0}, \ldots, f_{x_n}$ не имеют общего нуля в $P^n(F)$ ни для какого алгебраического расширения поля F. В этом случае мы говорим, что проективная гиперповерхность, определяемая f, *абсолютно неособа*. Рассмотрим в этой ситуации дзета-функцию $Z(t)$ гиперповерхности $f = 0$. Гипотезы Вейля (теперь теоремы) утверждают следующее:

(a) $Z(t)$ — рациональная функция, которая может быть записана в виде

$$Z(t) = \frac{P(t)^{(-1)^n}}{(1-t)(1-qt)\ldots(1-q^{n-1}t)},$$

где $P(t)$ — многочлен с целыми коэффициентами.

(b) $P(t) = (1-a_1t)(1-a_2t)\ldots(1-a_mt)$. Отображение $a \to q^{n-1}/a$ является биекцией множества $a_1, \ldots, a_m$.

(c) $|a_i| = q^{(n-1)/2}$.

(d) Степень многочлена $P(t)$ равна $d^{-1}[(d-1)^{n-1} + (-1)^{n+1}(d-1)]$.

Приведенное утверждение об абсолютном значении корней известно как гипотеза Римана для гиперповерхностей. Доказательство пп. (a), (b) и (d) принадлежит Дворку [26]. Доказательство гипотезы Римана принадлежит Делиню (1973 г.) (См. [11*]. —

Ред.) За общими формулировками гипотез Вейля мы отсылаем читателя к [80] и [161] [1]).

§ 4. Доказательство соотношения Хассе—Дэвенпорта

Пусть F — конечное поле из q элементов и F_s — такое поле, содержащее F, что $[F_s : F] = s$. Пусть χ — нетривиальный мультипликативный характер поля F и $\chi' = \chi \circ N_{F_s/F}$. Тогда χ' — характер поля F_s. Мы хотим сравнить суммы Гаусса $g(\chi)$ и $g(\chi')$.

Напомним определение $g(\chi)$ (см. гл. 10, § 3):

$$g(\chi) = \sum_{t \in F} \chi(t)\,\psi(t),$$

где $\psi(t)$ равно $\zeta_p^{\mathrm{tr}(t)}$. Функция следа в этом определении совпадает с функцией tr_{F/F_p}, введенной в этой главе. Так как мы рассматриваем более чем одно поле, важно добавлять к следу индекс. Далее,

$$g(\chi') = \sum_{t \in F_s} \chi'(t)\,\psi'(t),$$

где $\psi'(t) = \zeta^{\mathrm{tr}_{F_s/F_p}(t)}$. Так как $\mathrm{tr}_{F_s/F_p}(t) = \mathrm{tr}_{F/F_p}(\mathrm{tr}_{F_s/F}(t))$, то $\psi' = \psi \circ \mathrm{tr}_{F_s/F}$.

Для приведенного многочлена $f(x) = x^n - c_1 x^{n-1} + \ldots + (-1)^n c_n$ из $F[x]$ положим $\lambda(f) = \psi(c_1)\,\chi(c_n)$.

Лемма 1. $\lambda(fg) = \lambda(f)\,\lambda(g)$ *для всех приведенных* $f,\ g \in F[x]$.

Доказательство. Если $g(x) = x^m - b_1 x^{m-1} + \ldots + (-1)^m b_m$, то $f(x)\,g(x) = x^{n+m} - (b_1 + c_1)\,x^{m+n-1} + \ldots + (-1)^{m+n} b_m c_n$. Таким образом,

$$\lambda(fg) = \psi(b_1 + c_1)\,\chi(b_m c_n) = \psi(b_1)\,\psi(c_1)\,\chi(b_m)\,\chi(c_n) =$$
$$= \psi(b_1)\,\chi(b_m)\,\psi(c_1)\,\chi(c_n) = \lambda(g)\,\lambda(f). \qquad \square$$

Лемма 2. *Пусть* $\alpha \in F_s$ *и* $f(x)$ *— приведенный неприводимый многочлен для* α *над* F. *Тогда*

$$\lambda(f)^{s/d} = \chi'(\alpha)\,\psi'(\alpha), \quad \textit{где } d = \deg f.$$

---

[1]) Другое доказательство утверждений (a), (b) и (d) дано Гротендиком с помощью теории этальных когомологий, существование которой было предсказано Вейлем в [80]. Изложение в см. [144], добавление C, и [16*]. —*Прим. ред.*

Доказательство. Этот результат легко следует из предложения 11.2.4. А именно, если $f(x) = x^d - c_1 x^{d-1} + \ldots + (-1)^d c_d$, то

$$\mathrm{tr}_{F_s/F}(\alpha) = \frac{s}{d} c_1 \quad \text{и} \quad N_{F_s/F}(\alpha) = c_d^{s/d}.$$

Далее $\lambda(f) = \psi(c_1)\chi(c_d)$, так что

$$\lambda(f)^{s/d} = \psi(c_1)^{s/d}\chi(c_d)^{s/d} = \psi\left(\frac{s}{d} c_1\right)\chi\left(c_d^{s/d}\right) =$$

$$= \psi\left(\mathrm{tr}_{F_s/F}(\alpha)\right)\chi\left(N_{F_s/F}(\alpha)\right) = \psi'(\alpha)\chi'(\alpha). \qquad \square$$

Лемма 3. *$g(\chi') = \sum (\deg f)\,\lambda(f)^{s/\deg f}$, где сумма берется по всем приведенным многочленам кольца $F[x]$ степени, делящей s.*

Доказательство. Согласно теореме 1 гл. 7, обобщенной на случай, когда в качестве основного поля берется F, $x^{q^s} - x$ является произведением всех неприводимых приведенных многочленов степени, делящей s. Отсюда следует, что все корни каждого такого неприводимого многочлена лежат в F_s и, обратно, каждый элемент из F_s обращает в нуль такой многочлен.

Пусть $f(x)$ — приведенный неприводимый многочлен степени $d \mid s$. Пусть $\alpha_1, \alpha_2, \ldots, \alpha_d \in F_s$ — его корни. Тогда, согласно лемме 2,

$$\sum_{i=1}^{d} \chi'(\alpha_i)\psi'(\alpha_i) = d\lambda(f)^{s/d}.$$

Суммирование по всем многочленам требуемого типа приводит к доказываемому результату. $\square$

Теперь мы можем доказать соотношение Хассе — Дэвенпорта. Доказательство основано на следующем тождестве:

$$\sum_f \lambda(f)\, t^{\deg f} = \prod_f (1 - \lambda(f)\, t^{\deg f})^{-1}, \tag{7}$$

где сумма берется по всем приведенным многочленам, а произведение — по всем приведенным неприводимым многочленам в $F[x]$.

Это тождество получается разложением каждого члена $(1 - \lambda(f)\, t^{\deg f})^{-1}$ в геометрическую прогрессию с использованием того факта, что каждый приведенный многочлен может быть однозначно записан в виде произведения приведенных неприводимых многочленов. Дополнить детали предоставляется читателю в качестве упражнения.

Далее,

$$\sum_f \lambda(f)\, t^{\deg f} = \sum_{s=0}^{\infty} \Big(\sum_{\deg f = s} \lambda(f) \Big)\, t^s.$$

Мы полагаем $\lambda(1) = 1$, так как это необходимо для выполнения равенства (7).

Для $s = 1$ получаем

$$\sum_{\deg f = 1} \lambda(f) = \sum_{a \in F} \lambda(x - a) = \sum_{a \in F} \chi(a)\, \psi(a) = g(\chi).$$

Для $s > 1$

$$\sum_{\deg f = s} \lambda(f) = \sum_{c_i \in F} \lambda(x^s - c_1 x^{s-1} + \ldots + (-1)^s c_s) =$$

$$= q^{s-2} \sum_{c_1,\, c_s} \chi(c_s)\, \psi(c_1) = q^{s-2} \Big(\sum_{c_s} \chi(c_s) \Big) \Big(\sum_{c_1} \psi(c_1) \Big) = 0.$$

Объединяя все предыдущее вместе, убеждаемся в том, что левая часть равенства (7) сводится к $1 + g(\chi)\, t$. Используя это, возьмем логарифм от обеих частей равенства (7), продифференцируем и умножим обе части полученного результата на t. Это приводит к равенству

$$\frac{g(\chi)\, t}{1 + g(\chi)\, t} = \sum_f \frac{\lambda(f)\, (\deg f)\, t^{\deg f}}{1 - \lambda(f)\, t^{\deg f}}.$$

Разлагая знаменатели в геометрическую прогрессию, получаем

$$\sum_{s=1}^{\infty} (-1)^{s-1}\, g(\chi)^s\, t^s = \sum_f \Big(\sum_{r=1}^{\infty} (\deg f)\, \lambda(f)^r\, t^{r \deg f} \Big).$$

Приравнивание коэффициентов при t^s дает

$$(-1)^{s-1}\, g(\chi)^s = \sum_{\deg f \mid s} (\deg f)\, \lambda(f)^{s/\deg f}.$$

Согласно лемме 3, правая часть равна $g(\chi')$. Это завершает доказательство. □

§ 5. Последняя запись

Последняя запись математического дневника Гаусса — это формулировка следующей замечательной гипотезы:

Предположим, что $p \equiv 1$ (4). Тогда число решений сравнения $x^2 + y^2 + x^2y^2 \equiv 1$ (p) равно $p + 1 - 2a$, где $p = a^2 + b^2$ и $a + bi \equiv 1$ $(2 + 2i)$.

Надо дать некоторые пояснения. Если $p \equiv 1$ (4), то в силу предложения 8.3.1 $p = a^2 + b^2$ при некоторых целых a и b. Если a

выбрать нечетным, а b четным, то они будут определены однозначно с точностью до знака. Сравнение $a + bi \equiv 1\ (2 + 2i)$ определяет знак a. Мы приведем более простую формулировку этого факта.

Лемма. *Если* $p \equiv 1\ (4)$, $p = a^2 + b^2$ *и* $a + bi \equiv 1\ (2 + 2i)$, *то* a *нечетно и* b *четно. Более того, если* $4 \mid b$, *то* $a \equiv 1\ (4)$; *если же* $4 \nmid b$, *то* $a \equiv -1\ (4)$.

Доказательство. Из того, что $a + bi \equiv 1\ (2 + 2i)$, следует, что $a + bi \equiv 1\ (2)$, а значит, a нечетно и b четно.

Так как $4 = -2(i - 1)(i + 1)$, то при $4 \mid b$ имеем $a + bi \equiv a\ (2 + 2i) \equiv 1\ (2 + 2i)$. Беря сопряжение, получаем $a \equiv 1\ (2 - 2i)$. Таким образом, $(2 + 2i)(2 - 2i) = 8 \mid (a - 1)^2$ и $a \equiv 1\ (4)$.

Если $4 \nmid b$, то $b = 4k + 2$ для некоторого k. Таким образом, $a + bi \equiv a + 2i\ (2 + 2i) \equiv 1\ (2 + 2i)$. Так как $2i \equiv -2\ (2 + 2i)$, то $a \equiv 3\ (2 + 2i) \equiv -1\ (2 + 2i)$. Как и прежде, $8 \mid (a + 1)^2$, так что $a \equiv -1\ (4)$. □

Теорема. *Рассмотрим кривую* C, *определенную многочленом* $x^2t^2 + y^2t^2 + x^2y^2 - t^4$ *над* F_p, *где* $p \equiv 1\ (4)$. *Запишем* $p = a^2 + b^2$ *с нечетным* a *и четным* b. *Если* $4 \mid b$, *то выберем* $a \equiv 1\ (4)$; *если* $4 \nmid b$, *то выберем* $a \equiv -1\ (4)$. *Тогда число точек на* C *в* $P^2(F_p)$ *равно* $p - 1 - 2a$.

Дзета-функция кривой C *равна*

$$Z(u) = \frac{1 - 2au + pu^2}{1 - pu}(1 - u).$$

Прежде чем приступить к доказательству, сделаем несколько замечаний.

Ответ $p - 1 - 2a$ отличается от числа $p + 1 - 2a$, указанного Гауссом. Дело в том, что Гаусс считает, что на бесконечности лежат четыре точки, в то время как простое вычисление показывает, что $[0, 1, 0]$ и $[0, 0, 1]$, согласно нашему определению, — единственные бесконечно удаленные точки. Поэтому наш ответ отличается от его ответа на 2.

Так как независимо от p имеются две бесконечно удаленные точки, достаточно подсчитать число конечных точек, т. е. решений уравнения $x^2 + y^2 + x^2y^2 = 1$.

В качестве примера рассмотрим $p = 5$. Так как $5 = 1^2 + 2^2$, то $4 \nmid b$, а потому мы должны взять $a = -1$. Формула $p - 1 - 2a$ дает в этом случае ответ 6.

Действительно, в дополнение к двум бесконечно удаленным точкам точки $(1, 0)$, $(-1, 0)$, $(0, 1)$ и $(0, -1)$ есть остальные точки нашей кривой над полем F_p.

Вид указанной дзета-функции может вызвать удивление. Объяснение состоит в том, что две бесконечно удаленные точки являются особыми. Таким образом, вид этой дзета-функции не противоречит нашим более ранним наблюдениям [1]).

Мы приступаем теперь к доказательству теоремы. Обозначим через C_1 кривую, задаваемую уравнением $x^2 + y^2 + x^2y^2 = 1$, а через C_2 — кривую, задаваемую уравнением $w^2 = 1 - z^4$. Мы построим отображения из C_1 в C_2 и из C_2 в C_1.

Заметим, что из

$$x^2 + y^2 + x^2y^2 = 1$$

следуют равенства

$$(1 + x^2)\, y^2 = 1 - x^2$$

и

$$[(1 + x^2)\, y]^2 = 1 - x^4.$$

Поэтому если (a, b) лежит на C_1, то $(a, (1 + a^2)\, b)$ лежит на C_2. Пусть

$$\lambda\,(x, y) = (x, (1 + x^2)\, y).$$

λ отображает C_1 в C_2. Нетрудно убедиться в том, что это отображение взаимно однозначно.

Далее, положим

$$\mu\,(z, w) = \left(z, \frac{w}{1 + z^2}\right).$$

Отображение μ определено не во всех точках. Если $\alpha \in F_p$ таково, что $\alpha^2 = -1$, то $(\alpha, 0)$ и $(-\alpha, 0)$ лежат на C_2, но μ в этих точках не определено. Оно определено во всех других точках кривой C_2 и отображает эти точки в C_1. Нетрудно проверить, что μ обратно λ всюду, где оно определено. Таким образом,

$$N_1 = N_2 - 2,$$

где N_1 и N_2 — числа конечных точек над полем F_p на C_1 и C_2 соответственно.

N_2 можно вычислить, используя теорему 5 гл. 8. Применяя теорему 5 к $w^2 + z^4 = 1$, видим, что

$$N_2 = p + J\,(\rho, \chi) + J\,(\rho, \chi^2) + J\,(\rho, \chi^3),$$

где ρ — характер порядка 2, а χ — характер порядка 4.

---

[1]) Если C — наша кривая, рассматриваемая на проективной плоскости, то существует неособая кривая C', отображающаяся на C так, что над двумя особыми бесконечно удаленными точками лежат четыре рациональные (и неособые) точки кривой C'. Дзета-функция $Z_{C'}(u)$ имеет вид, предписываемый результатами § 3, а дзета-функция $Z_C(u)$ получается из нее умножением на $(1 - u)^2$ (это множители эйлерова разложения для $Z_{C'}(u)$, отвечающие двум «лишним» точкам на C'). — *Прим. ред.*

Так как $\chi^2 = \rho$, то $J(\rho, \chi^2) = J(\rho, \rho) = -\rho(-1) = -1$. Кроме того, поскольку $\chi^4 = \varepsilon$, то $\chi^3 = \bar{\chi}$, а потому $J(\rho, \chi^3) = J(\rho, \bar{\chi}) = \overline{J(\rho, \chi)}$.

Пусть $\pi = -J(\rho, \chi)$. Тогда

$$N_2 = p - 1 - \pi - \bar{\pi}.$$

ρ принимает значения ± 1, а χ принимает значения $\pm 1, \pm i$. Таким образом, $\pi = a + bi$, где $a, b \in \mathbf{Z}$. Кроме того, $|J(\rho, \chi)|^2 = p$, так что $a^2 + b^2 = \pi\bar{\pi} = p$. Отсюда следует, что $N_2 = p - 1 - 2a$ и $N_1 = p - 3 - 2a$. Так как C_1 имеет две бесконечно удаленные точки, то общее число точек на C_1 над F_p задается формулой

$$N = p - 1 - 2a.$$

Для завершения первой части теоремы достаточно в силу леммы доказать, что $\pi \equiv 1\ (2 + 2i)$. Это достигается при помощи следующего изящного вычисления, приведенного у Хассе — Дэвенпорта [23].

Заметим, что $\rho(a) - 1 \equiv 0\ (2)$ и $\chi(a) - 1 \equiv 0\ (1 + i)$ для всех $a \neq 0$ в F_p. Первое утверждение очевидно; второе следует из того, что $1 - 1 = 0$, $-1 - 1 = -(1 - i)(1 + i)$, $-i - 1 = -(1 + i)$ и $i - 1 = i(1 + i)$. Таким образом, если $a \neq 0$ и $b \neq 0$, то $(\rho(a) - 1)(\chi(b) - 1) \equiv 0\ (2 + 2i)$. Это сравнение тривиально верно для пар $a = 0$, $b = 1$ и $a = 1$, $b = 0$. Поэтому

$$\sum_{a+b=1} (\rho(a) - 1)(\chi(b) - 1) \equiv 0\ (2 + 2i).$$

Раскрывая скобки, получаем

$$-\pi - \sum_b \chi(b) - \sum_a \rho(a) + p \equiv 0\ (2 + 2i).$$

Второй и третий члены равны нулю. Таким образом,

$$\pi \equiv p\ (2 + 2i) \equiv 1\ (2 + 2i).$$

Последний шаг получается в силу того, что $p \equiv 1\ (4)$ по предположению и $2 + 2i$ делит 4; в самом деле, $4 = (1 - i)(2 + 2i)$.

Для вычисления дзета-функции достаточно заметить, что в силу соотношения Хассе — Дэвенпорта число точек на $x^2t^2 + y^2t^2 + x^2y^2 - t^4 = 0$ в $P^2(F_{p^s})$ равно

$$p^s - 1 - (-J(\rho, \chi))^s - (-\overline{J(\rho, \chi)})^s = p^s - 1 - \pi^s - \bar{\pi}^s.$$

Таким образом,

$$Z(u) = \frac{(1 - \pi u)(1 - \bar{\pi} u)}{(1 - pu)}(1 - u) = \frac{1 - 2au + pu^2}{1 - pu}(1 - u).$$

Замечания

Как мы уже упоминали, понятие конгруэнц-дзета-функции было введено Артином в его диссертации [2]. В этой работе он получил аналог гипотезы Римана для приблизительно 40 кривых вида $y^2 = f(x)$, где f — кубический многочлен или многочлен четвертой степени. В 1934 г. Хассе доказал, что этот результат верен в общем виде для кубик (случай эллиптических кривых). В полной общности гипотеза Римана для произвольных неособых кривых была доказана Вейлем в 1948 г. Его доказательство далеко не элементарно и использует тонкую технику алгебраической геометрии.

Гипотеза Вейля о том, что дзета-функция любого алгебраического многочлена рациональна, была доказана в 1959 г. Дворком с использованием p-адического анализа [26].

В 1969 г. С. А. Степанову удалось получить элементарное доказательство гипотезы Римана для кривых [222]. Полное изложение метода Степанова имеется в книге [218]. Этот метод был еще упрощен Бомбьери, который, используя теорему Римана — Роха, дает полное доказательство на пяти страницах [98]. Более сильные оценки в частных случаях были получены в [221]. Для анализа доказательства Делиня и исторического обсуждения вопроса в целом читателю следует обратиться к [161]. В этой статье содержится также обширная библиография по данному вопросу. См. также обзор [248]. Открытие этих замечательных теорем обсуждается в первом томе собрания сочинений Вейля [241], с. 568—569. Наконец, упомянем статью [160] [1]).

§ 5 о гипотезе Гаусса логически находится не на месте, так как его следовало бы включить в гл. 8. Мы посчитали возможным поместить его в эту главу в силу того, что связь между этой гипотезой и гипотезой Римана — Вейля еще раз обнаруживает замечательную остроту интуиции Гаусса и то, как его влияние продолжает сказываться вплоть до наших дней.

В настоящее время доступно новое издание математического дневника Гаусса, переведенного с латинского языка на немецкий, с историческим обзором Бирмана и комментариями Вуссинга [137]. В этом важном историческом документе сообщается об основных открытиях Гаусса между 1796 и 1814 годами. Интересно отметить, что как первая (§ 11 гл. 9), так и последняя записи относятся к круговым полям. Дополнительную биографическую информацию о Гауссе см. в [143] и в биографии, написанной недавно Бюхлером [101].

---

[1]) См. также примечание к § 3. — *Прим. ред.*

Упражнения

1. Предположим, что степенной ряд $1 + a_1u + a_2u^2 + \cdots$ можно записать в виде отношения двух многочленов $P(u)/Q(u)$. Показать, что можно считать $P(0) = Q(0) = 1$.

2. Доказать обращение предложения 11.1.1.

3. Восстановить детали доказательства того, что N_s не зависит от поля F_s (см. последний абзац § 1).

4. Вычислить дзета-функцию поверхности $x_0x_1 - x_2x_3 = 0$ над F_p.

5. Вычислить настолько явно, насколько возможно, дзета-функцию поверхности $a_0x_0^2 + a_1x_1^2 + \cdots + a_nx_n^2$ над F_q, где q нечетно. Ответ зависит от нечетности или четности n и альтернативы $q \equiv 1$ (4) или $q \equiv 3$ (4).

6. Рассмотрим $x_0^3 + x_1^3 + x_2^3 = 0$ как уравнение над F_4, полем из четырех элементов. Показать, что на этой кривой в $P^2(F_4)$ существует девять точек. Вычислить дзета-функцию. (*Ответ.* $(1 + 2u)^2/((1 - u)(1 - 4u))$.)

7. Это упражнение следует выполнять при некотором знакомстве с проективной геометрией. Пусть N_s — число прямых в $P^n(F_{p^s})$. Найти N_s и вычислить $\sum_{s=1}^{\infty} N_s u^s/s$. (Множество прямых в проективном пространстве является алгебраическим многообразием, называемым *грассмановым*. Грассмановым многообразием будет и множество плоскостей, трехмерных линейных подпространств и т. д.)

8. Если f — неоднородный многочлен, можно рассмотреть дзета-функцию проективного замыкания гиперповерхности, определяемой этим многочленом (см. гл. 10). Один из способов вычислить ее состоит в подсчете числа точек на $H_f(F_q)$ и затем в добавлении к нему числа бесконечно удаленных точек. Например, рассмотрим $y^2 = x^3$ над F_{p^s}. Показать, что она имеет одну бесконечно удаленную точку. Начало координат $(0, 0)$, очевидно, лежит на этой кривой. Если $x \neq 0$, то записать $(y/x)^2 = x$ и показать, что на этой кривой дополнительно имеется $p^s - 1$ точек. Всего получается $p^s + 1$ точек, и дзета-функция над F_p равна $(1 - pu)^{-1}(1 - u)^{-1}$.

9. Вычислить дзета-функцию кривой $y^2 = x^3 + x^2$ над F_q.

10. Если $A \neq 0$ в F_q и $q \equiv 1$ (3), то показать, что дзета-функция кривой $y^2 = x^3 + A$ над F_q имеет вид

$$Z(u) = (1 + au + qu^2)/(1 - u)(1 - qu),$$

где $a \in \mathbf{Z}$ и $|a| \leqslant 2q^{1/2}$.

11. Рассмотрим кривую $y^2 = x^3 - Dx$ над F_p, где $D \neq 0$. Обозначим эту кривую через C_1. Показать, что замена $x = (u + v^2)/2$ и $y = v(u + v^2)/2$ отображает C_1 в кривую C_2, задаваемую уравнением $u^2 - v^4 = 4D$. Показать, что при любом заданном конечном поле число конечных точек на C_1 на единицу больше, чем число конечных точек на C_2.

12 (продолжение). Показать, что если $p \equiv 3$ (4), то число проективных точек на C_1 в точности равно $p + 1$. Если $p \equiv 1$ (4), то показать, что ответом будет $p + 1 + \overline{\chi(D)}\, J(\chi, \chi^2) + \chi(D)\, \overline{J(\chi, \chi^2)}$, где χ — характер порядка 4 на F_p.

13 (продолжение). При $p \equiv 1$ (4) вычислить дзета-функцию для $y^2 = x^3 - Dx$ над F_p в терминах π и $\chi(D)$, где $\pi = -J(\chi, \chi^2)$. Это вычисление в несколько более сложном виде содержится в [23]. Полученный результат играл ключевую роль в недавней эмпирической работе Берча и Суиннертона-Дайера по эллиптическим кривым.

14. Предположим, что $p \equiv 1$ (4), и рассмотрим кривую $x^4 + y^4 = 1$ над F_p. Пусть χ — характер порядка 4 и $\pi = -J(\chi, \chi^2)$. Получить формулу для числа проективных точек над F_p и вычислить дзета-функцию. Оба ответа должны зависеть лишь от π. [*Указание.* См. упр. 7 и 16 из гл. 8, но использовать их надо с осторожностью ввиду того, что там учитывались лишь конечные точки.]

15. Найти число точек на кривой $x^2 + y^2 + x^2y^2 = 1$ для $p = 13$ и $p = 17$. Применить как формулу из § 5, так и прямое вычисление.

16. Пусть F — поле из q элементов и F_s — расширение степени s. Если χ — характер поля F, то пусть $\chi' = \chi \circ N_{F_s/F}$. Показать, что

(a) χ' — характер поля F_s;
(b) из $\chi \neq \rho$ следует, что $\chi' \neq \rho'$;
(c) из $\chi^m = \varepsilon$ следует, что $\chi'^m = \varepsilon$;
(d) $\chi'(a) = \chi(a)^s$ для $a \in F$;
(e) в то время как χ пробегает все характеры поля F порядка, делящего m, χ' пробегает все характеры поля F_s порядка, делящего m (здесь мы предполагаем, что $q \equiv 1\ (m)$).

17. В теореме 2 показать, что числитель дзета-функции $P(u)$ имеет степень $m^{-1}((m-1)^{n+1} + (-1)^{n+1}(m-1))$.

18. Пусть используются обозначения из упр. 16. С помощью соотношения Хассе—Дэвенпорта показать, что

$$J(\chi_1', \chi_2', \ldots, \chi_n') = (-1)^{(s-1)(n-1)} J(\chi_1, \chi_2, \ldots, \chi_n)^s,$$

где χ_i — нетривиальные характеры поля F и $\chi_1\chi_2 \ldots \chi_n \neq \varepsilon$.

19. Доказать тождество

$$\sum \lambda(f) t^{\deg f} = \prod (1 - \lambda(f) t^{\deg f})^{-1},$$

где сумма берется по всем приведенным многочленам в $F[t]$, а произведение — по всем приведенным неприводимым многочленам в $F[t]$; λ определено в § 4.

20. Если в теореме 2 в качестве основного поля рассмотреть F_s вместо F, то получим другую дзета-функцию, $Z_f^{(s)}(u)$. Показать, что $Z_f^{(s)}(u)$ и $Z_f(u)$ связаны равенством

$$Z_f^{(s)}(u) = Z_f(u)\, Z_f(\rho u) \ldots Z_f(\rho^{s-1} u),$$

где $\rho = e^{2\pi i/s}$.

21. В упр. 6 мы рассматривали уравнение $x_0^3 + x_1^3 + x_2^3 = 0$ над полем из четырех элементов. Рассмотреть то же самое уравнение над полем из двух элементов. Осложнение здесь состоит в том, что $2 \not\equiv 1\ (3)$, а поэтому наши обычные вычисления не проходят. Доказать, что в любом расширении поля $\mathbf{Z}/2\mathbf{Z}$ нечетной степени каждый элемент является кубом и что в любом расширении четной степени 3 делит порядок мультипликативной группы. Воспользоваться этой информацией для вычисления дзета-функции над $\mathbf{Z}/2\mathbf{Z}$. [*Ответ.* $(1 + 2u^2)/(1 - u)(1 - 2u)$.]

22. При помощи идей из упр. 21 показать, что теорема 2 остается верной (в подходящем смысле) даже без предположения $q \equiv 1\ (m)$.

23. Пусть $p_1 < p_2 < p_3 < \cdots$ обозначает положительные простые числа, расположенные в порядке возрастания. Пусть $N_m = p_1^m p_2^m \ldots p_m^m$ и E_m обозначает поле из q^{N_m} элементов. Показать, что E_m можно рассматривать как подполе E_{m+1} и что $E = \bigcup E_m$ — расширение поля $E_0 = F$, конечного поля из q элементов, обладающее следующим свойством: для каждого положительного целого числа n поле E содержит одно и только одно подполе F_n, состоящее из q^n элементов.

Глава 12

ТЕОРИЯ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

В этой главе мы введем понятие поля алгебраических чисел и изложим основные свойства этого поля. Наш подход будет классическим, причем излагаются лишь те вопросы, которые понадобятся в последующих главах. Изучение таких полей и их связь с другими ветвями математики составляют значительную часть современных исследований. Наша цель состоит в изложении той части общей теории, которая нужна при изучении законов взаимности высших степеней. Читателю, интересующемуся более систематическим изложением теории полей алгебраических чисел, следует обратиться к любой стандартной книге на эту тему, например [207], [168], [140], [183].

Мы предполагаем, что читатель знаком с теорией сепарабельных расширений полей (изложение этой теории можно найти, например, в [150] [1]). *Некоторые результаты приведены в упражнениях.*

§ 1. Алгебраические подготовительные результаты

В этом параграфе мы напоминаем некоторые факты из теории полей и доказываем ряд результатов о дискриминантах.

Пусть L/K — конечное алгебраическое расширение поля K. Размерность пространства L/K, $[L : K]$, будет обозначаться через n.

Предположим, что $\alpha_1, \alpha_2, \ldots, \alpha_n$ — базис L/K и $\alpha \in L$. Тогда $\alpha\alpha_i = \sum_j a_{ij}\alpha_j$, где $a_{ij} \in K$.

Определение. *Норма* элемента α, $N_{L/K}(\alpha)$, — это $\det(a_{ij})$. *След* элемента α, $t_{L/K}(\alpha)$, есть $a_{11} + a_{22} + \ldots + a_{nn}$.

Нетрудно убедиться в том, что это определение не зависит от выбора базиса. В дальнейшем изложении норма и след будут

---

[1]) Все необходимое можно также найти в [4*] или [15*]. — *Прим. ред.*

обозначаться через N и t, так как расширение L/K будет фиксировано.

Если $\alpha, \beta \in L$ и $a \in K$, то $N(\alpha\beta) = N(\alpha)\,N(\beta)$, $t(\alpha + \beta) = t(\alpha) + t(\beta)$, $N(a\alpha) = a^n N(\alpha)$ и $t(a\alpha) = at(\alpha)$. Если $\alpha \neq 0$, то $N(\alpha)\,N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = N(1) = 1$. Таким образом, если $\alpha \neq 0$, то $N(\alpha) \neq 0$ и $N(\alpha^{-1}) = N(\alpha)^{-1}$. Если L/K сепарабельно, то функция t не равна тождественно нулю. Если $\operatorname{char} K = 0$, то это очевидно, ибо $t(1) = n \neq 0$. Единственные поля характеристики $p > 0$, которые мы будем рассматривать, — это конечные поля, а в таком случае результат следует из предложения 11.2.1 (d).

Предположим, что L/K сепарабельно, и пусть $\sigma_1, \sigma_2, \ldots, \sigma_n$ — различные изоморфизмы поля L в некоторое фиксированное алгебраическое замыкание поля K, которые оставляют элементы из K на месте. Для $\alpha \in L$ обозначим $\sigma_j(\alpha)$ через $\alpha^{(j)}$. Элементы $\alpha^{(j)}$ называются *сопряженными* к α. Здесь $\alpha^{(1)}$ есть α.

Используя линейную алгебру, можно показать (см. упр. 21—23), что $t(\alpha) = \alpha^{(1)} + \alpha^{(2)} + \ldots + \alpha^{(n)}$ и $N(\alpha) = \alpha^{(1)}\alpha^{(2)} \ldots \alpha^{(n)}$. Если $\alpha \in L$, то рассмотрим

$$f(x) = (x - \alpha^{(1)})(x - \alpha^{(2)}) \ldots (x - \alpha^{(n)}).$$

Тогда $f(x) \in K[x]$. Коэффициент при x^{n-1} равен $-t(\alpha)$, а свободный член равен $(-1)^n N(\alpha)$. Читателю следует убедиться в том, что наши определения нормы и следа обобщают определения из гл. 11, § 2 [1]).

Определение. Если $\alpha_1, \alpha_2, \ldots, \alpha_n$ — некоторый n-набор элементов из L, то мы определяем *дискриминант* $\Delta(\alpha_1, \ldots, \alpha_n)$ как $\det(t(\alpha_i\alpha_j))$.

Предложение 12.1.1. *Если* $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$, *то* $\alpha_1, \ldots, \alpha_n$ *образуют базис в* L/K. *Если* L/K *сепарабельно и* $\alpha_1, \ldots, \alpha_n$ — *базис в* L/K, *то* $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$.

Доказательство. Предположим, что $\alpha_1, \ldots, \alpha_n$ линейно зависимы. Тогда существуют $a_1, \ldots, a_n \in K$, не все равные нулю, для которых $\sum a_i\alpha_i = 0$. Умножим это равенство на α_j и возьмем след. В результате получим

$$\sum_i a_i t(\alpha_i\alpha_j) = 0, \quad j = 1, 2, \ldots, n.$$

Это показывает, что матрица $(t(\alpha_i\alpha_j))$ вырожденна, так что ее определитель равен нулю.

---

[1]) В предыдущей главе для следа использовалось обозначение $\operatorname{tr}_{L/K}$. — *Прим. ред.*

Предположим теперь, что $\alpha_1, \ldots, \alpha_n$ — базис и $\Delta(\alpha_1, \ldots, \alpha_n) = 0$. Тогда система линейных уравнений

$$\sum_i x_i t(\alpha_i \alpha_j) = 0, \quad j = 1, \ldots, n,$$

имеет нетривиальное решение $x_i = a_i \in K$, $i = 1, \ldots, n$. Пусть $\alpha = \sum a_i \alpha_i \neq 0$. Тогда $t(\alpha \alpha_j) = 0$ для $j = 1, 2, \ldots, n$, а так как $\alpha_1, \ldots, \alpha_n$ — базис, отсюда следует, что $t(\alpha\beta) = 0$ для всех $\beta \in L$. Это означает, что след тождественно равен нулю, но это не так, ибо L/K сепарабельно. Отсюда получаем второе утверждение. □

Предложение 12.1.2. *Предположим, что* $\alpha_1, \ldots, \alpha_n$ *и* $\beta_1, \ldots, \beta_n$ *— базисы в* L/K. *Пусть* $\alpha_i = \sum_j a_{ij}\beta_j$. *Тогда*

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det(a_{ij})^2 \Delta(\beta_1, \ldots, \beta_n).$$

Доказательство. Возьмем след от обеих частей равенства $\alpha_i \alpha_k = \sum_j \sum_l a_{ij} a_{kl} \beta_j \beta_l$. Пусть $A = (t(\alpha_i \alpha_j))$, $B = (t(\beta_i \beta_j))$ и $C = (a_{ij})$. Тогда мы получаем матричное равенство $A = C'BC$, где C' — матрица, транспонированная к C. Взяв определители от обеих частей последнего равенства и использовав то, что $\det C = \det C'$, устанавливаем доказываемый результат. □

Предложение 12.1.3. *Для* $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ *и сепарабельного расширения* L/K

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det(\alpha_i^{(j)})^2.$$

Доказательство. Имеем $t(\alpha_i \alpha_j) = \alpha_i^{(1)}\alpha_j^{(1)} + \alpha_i^{(2)}\alpha_j^{(2)} + \ldots + \alpha_i^{(n)}\alpha_j^{(n)}$. Пусть $A = (t(\alpha_i \alpha_j))$ и $B = (\alpha_i^{(k)})$. Тогда $A = BB'$. Взятие определителей от обеих частей этого матричного равенства приводит к нужному результату. □

Предложение 12.1.4. *Предположим, что* $1, \beta, \ldots, \beta^{n-1}$ *лежат в* L *и линейно независимы над* K. *Пусть* $f(x) \in K[x]$ *— минимальный многочлен для* β *над* K. *Если* L/K *сепарабельно, то*

$$\Delta(1, \beta, \ldots, \beta^{n-1}) = (-1)^{n(n-1)/2} N(f'(\beta)),$$

где $f'(x)$ *— формальная производная для* $f(x)$.

Доказательство. Матрица $((\beta^{(i)})^j)$, где $j = 1, \ldots, n$ и $i = 0, \ldots, n-1$, является матрицей вандермондовского типа, так что ее определитель равен

$$\prod_{i<j} (\beta^{(j)} - \beta^{(i)}).$$

Поэтому

$$\Delta(1, \beta, \ldots, \beta^{n-1}) = (-1)^{n(n-2)/2} \prod_{i \neq j} (\beta^{(i)} - \beta^{(i)}).$$

Далее, $f(x) = \prod_i (x - \beta^{(i)})$, а потому $f'(\beta^{(i)}) = \prod_i (\beta^{(i)} - \beta^{(i)})$ с $i \neq j$. Так как $f'(\beta^{(i)}) = (f'(\beta))^{(i)}$, мы получим доказываемый результат, если возьмем произведения по j. □

§ 2. Однозначность разложения на множители в полях алгебраических чисел

Элементарная теория чисел имеет дело со свойствами натуральных чисел 1, 2, 3, ... При изучении этих свойств становится необходимым рассматривать кольцо целых чисел $\mathbf{Z}$, а затем поле рациональных чисел $\mathbf{Q}$. Чтобы разобраться в биквадратичном законе взаимности, Гаусс ввел в рассмотрение кольцо $\mathbf{Z}[i]$. Аналогично, при изучении высших законов взаимности и последней теоремы Ферма (см. гл. 14) были введены другие кольца. В конце концов появились общие понятия поля алгебраических чисел и кольца целых алгебраических чисел (главным образом благодаря усилиям Куммера и Дедекинда).

Определение. Подполе F поля комплексных чисел называется *полем алгебраических чисел*, если $[F : \mathbf{Q}]$ конечно. Если F — такое поле, то подмножество в нем, состоящее из целых алгебраических чисел, образует кольцо D, называемое *кольцом целых алгебраических чисел* в F.

Предложение 6.1.2 показывает, что поле алгебраических чисел состоит из алгебраических чисел (а именно, следует положить $V = F$ и выбрать базис $\gamma_1, \ldots, \gamma_n$ в F над $\mathbf{Q}$).

Пусть Ω — множество всех алгебраических целых чисел. Тогда предложение 6.1.5 показывает, что Ω — кольцо. Так как $D = \Omega \cap F$, то D — тоже кольцо. Мы будем часто ссылаться на D просто как на кольцо целых чисел в F.

Оказывается, что в общем случае D не является областью с однозначным разложением на множители (упр. 7). Однако D обладает почти столь же хорошим свойством. А именно, каждый ненулевой идеал может быть однозначно представлен в виде произведения простых идеалов. Область целостности с таким свойством называется дедекиндовым кольцом. В этом параграфе, следуя методу Гурвица [154] (с. 236—243), мы докажем, что D — дедекиндово кольцо.

Всюду далее слово «идеал» будет обозначать ненулевой идеал. Мы надеемся, что это не вызовет недоразумений.

Лемма 1. *Предположим, что* $\beta \in F$. *Существует такое* $b \in \mathbf{Z}$, $b \neq 0$, *что* $b\beta \in D$.

Доказательство. β удовлетворяет уравнению $a_0\beta^n + a_1\beta^{n-1} + \ldots + a_n = 0$, где $a_i \in \mathbf{Z}$, $a_0 \neq 0$. Умножим обе части равенства на a_0^{n-1} и заметим, что

$$(a_0\beta)^n + a_1(a_0\beta)^{n-1} + \ldots + a_n a_0^{n-1} = 0.$$

Это доказывает, что $a_0\beta$ — целое алгебраическое число, так как для всех $i \geqslant 1$ будет $a_i a_0^{i-1} \in \mathbf{Z}$. □

Предложение 12.2.1. *Каждый идеал* A *в* D *содержит некоторый базис поля* F *над* $\mathbf{Q}$.

Доказательство. Пусть $\beta_1, \ldots, \beta_n$ — какой-либо базис в F над $\mathbf{Q}$. В силу предыдущей леммы существует такое число $b \in \mathbf{Z}$, $b \neq 0$, что $b\beta_1, \ldots, b\beta_n \in D$. Выберем $\alpha \in A$, $\alpha \neq 0$. Тогда элементы $b\beta_1\alpha, \ldots, b\beta_n\alpha$ принадлежат A и образуют базис поля F над $\mathbf{Q}$. □

В первом параграфе мы рассматривали расширение L/K поля K и след, норму и дискриминант какого-либо базиса. Здесь мы фиксируем расширение $F/\mathbf{Q}$ и рассматриваем все эти понятия для этого расширения.

Если $\alpha \in D$, то мы утверждаем, что $N(\alpha)$ и $t(\alpha)$ принадлежат $\mathbf{Z}$. Чтобы убедиться в этом, заметим, что если α удовлетворяет приведенному уравнению с коэффициентами в $\mathbf{Z}$, то ему же удовлетворяют и все сопряженные к α. Таким образом, $N(\alpha)$ и $t(\alpha)$, которые суть соответственно произведение и сумма сопряженных к числу α, являются целыми алгебраическими числами. Они также принадлежат $\mathbf{Q}$, так что в силу предложения 6.1.1 они принадлежат $\mathbf{Z}$. Из того, что след обладает этим свойством, вытекает, что если $\alpha_1, \ldots, \alpha_n$ — некоторый базис поля F над $\mathbf{Q}$ и все α_i лежат в D, то $\Delta(\alpha_1, \ldots, \alpha_n) \in \mathbf{Z}$.

Заметим, что дискриминант базиса может быть отрицательным. Например, пусть $i = \sqrt{-1}$, и рассмотрим базис $1, i$ расширения $\mathbf{Q}(i)/\mathbf{Q}$. Простое вычисление показывает, что $\Delta(1, i) = -4$.

Предложение 12.2.2. *Пусть* A — *идеал в* D, *и предположим, что* $\alpha_1, \ldots, \alpha_n \in A$ — *базис в* $F/\mathbf{Q}$ *с минимальным* $|\Delta(\alpha_1, \ldots, \alpha_n)|$. *Тогда* $A = \mathbf{Z}\alpha_1 + \mathbf{Z}\alpha_2 + \ldots + \mathbf{Z}\alpha_n$.

Доказательство. Поскольку абсолютная величина дискриминанта какого-либо базиса в A является положительным целым числом, такой базис с минимальным $|\Delta(\alpha_1, \ldots, \alpha_n)|$ существует.

Предположим, что $\alpha \in A$, и запишем $\alpha = \gamma_1\alpha_1 + \gamma_2\alpha_2 + \ldots + \gamma_n\alpha_n$, где $\gamma_i \in \mathbf{Q}$. Нам надо показать, что γ_i лежат в $\mathbf{Z}$. Предположим, что это не так. Тогда некоторое γ_i не лежит в $\mathbf{Z}$, и, производя перенумерацию, если необходимо, мы можем считать, что $\gamma_1 \notin \mathbf{Z}$. Запишем $\gamma_1 = m + \theta$, где $m \in \mathbf{Z}$ и $0 < \theta < 1$. Пусть $\beta_1 = \alpha - m\alpha_1$, $\beta_2 = \alpha_2$, ..., $\beta_n = \alpha_n$. Тогда β_1, β_2, ..., β_n лежат в A и образуют базис в $F/\mathbf{Q}$. Так как $\beta_1 = \theta\alpha_1 + \gamma_2\alpha_2 + \ldots + \gamma_n\alpha_n$, то матрица перехода от одного базиса к другому равна

$$\begin{pmatrix} \theta & \gamma_2 & \gamma_3 & \ldots & \gamma_n \\ 0 & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}$$

В силу предложения 12.1.2 $\Delta(\beta_1, \ldots, \beta_n) = \theta^2\Delta(\alpha_1, \ldots, \alpha_n)$, что противоречит минимальности $|\Delta(\alpha_1, \ldots, \alpha_n)|$, ибо $0 < \theta < 1$. Таким образом, все γ_i лежат в $\mathbf{Z}$ и $A = \mathbf{Z}\alpha_1 + \ldots + \mathbf{Z}\alpha_n$, как и утверждалось. □

Если $\alpha_1, \alpha_2, \ldots, \alpha_n \in A$ — базис поля F над $\mathbf{Q}$ и $A = \mathbf{Z}\alpha_1 + \ldots + \mathbf{Z}\alpha_n$, то мы говорим, что $\alpha_1, \ldots, \alpha_n$ — *целый* базис кольца A. Из предложения 12.1.2 следует, что дискриминанты двух любых целых базисов кольца A совпадают. Это общее значение называется *дискриминантом* кольца A и обозначается через $\Delta(A)$. Дискриминант кольца D особенно важен и, допуская вольность речи, назовем $\delta_F = \Delta(D)$ дискриминантом расширения $F/\mathbf{Q}$.

Мы воспользуемся теперь последним предложением для получения некоторых важных свойств кольца D. Напомним наше соглашение о том, что все рассматриваемые идеалы ненулевые.

Лемма 2. *Если $A \subset D$ — некоторый идеал, то $A \cap \mathbf{Z} \neq 0$.*

Доказательство. Пусть $\alpha \in A$, $\alpha \neq 0$. Существуют такие $a_i \in \mathbf{Z}$, что $\alpha^m + a_1\alpha^{m-1} + \ldots + a_m = 0$. Так как мы работаем в поле, можно считать, что $a_m \neq 0$. Но тогда $0 \neq a_m \in A \cap \mathbf{Z}$. □

Предложение 12.2.3. *Для любого идеала A факторкольцо D/A конечно.*

Доказательство. В силу леммы 2 существует элемент $a \in A \cap \mathbf{Z}$, $a \neq 0$. Пусть (a) — главный идеал, порожденный элементом a в D. Так как $D/(a)$ отображается на D/A, то достаточно показать, что $D/(a)$ конечно. На самом деле мы покажем, что оно состоит точно из a^n элементов.

Согласно предложению 12.2.2, мы можем записать $D = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 + \ldots + \mathbf{Z}\omega_n$. Пусть $S = \{\gamma_i\omega_i \mid 0 \leqslant \gamma_i < a\}$.

Мы утверждаем, что S является множеством представителей для $D/(a)$. Предположим, что $\omega = \sum m_i\omega_i \in D$. Запишем $m_i = q_i a + \gamma_i$, где $0 \leqslant \gamma_i < a$. Тогда очевидно, что $\omega \equiv \sum \gamma_i\omega_i$ (a).

Таким образом, каждый класс смежности содержит некоторый элемент из S. Если $\sum \gamma_i\omega_i$ и $\sum \gamma_i'\omega_i$ находятся в S и лежат в одном классе смежности по модулю (a), то используя тот факт, что ω_i линейно независимы, мы убеждаемся в том, что $\gamma_i - \gamma_i'$ делится на a в $\mathbf{Z}$. Так как $0 \leqslant \gamma_i, \gamma_i' < a$, отсюда следует, что $\gamma_i = \gamma_i'$. Таким образом, S есть множество представителей классов смежности и $D/(a)$ содержит a^n элементов, как и утверждалось. □

Следствие 1. *D — нётерово кольцо, т. е. каждая возрастающая цепочка его идеалов $A_1 \subset A_2 \subset A_3 \subset \ldots$ стабилизируется. Другими словами, существует такое $N > 0$, что $A_m = A_{m+1}$ для всех $m \geqslant N$.*

Доказательство. Так как D/A_1 конечно, то существует лишь конечное число идеалов, содержащих A_1. □

Следствие 2. *Каждый простой идеал в D максимален.*

Доказательство. Если P — простой идеал, то D/P — конечная область целостности. Такое кольцо обязательно является полем (см. упр. 19). Таким образом, D/P — поле, а потому P максимален. □

Кольцо D является также *целозамкнутым*. Это означает, что если $\alpha \in F$ удовлетворяет приведенному многочлену с коэффициентами из D, то $\alpha \in D$. В этом нетрудно убедиться, используя предложение 6.1.4. В стандартных учебниках по алгебре показано, что если некоторая область целостности нётерова, целозамкнута и каждый ненулевой простой идеал максимален, то каждый идеал будет произведением однозначно определенных простых идеалов, т. е. такое кольцо будет дедекиндовой областью. Тот факт, что D — дедекиндова область, мы получим другим способом, используя одно очень важное свойство числовых полей, а именно, что число классов кольца D конечно (см. ниже).

Наша ближайшая цель состоит в доказательстве следующих двух результатов:

(1) Если A, B и C — идеалы и $AB = AC$, то $B = C$.

(2) Если A и B — идеалы и $A \subset B$, то существует такой идеал C, что $A = BC$.

Они будут доказаны далее. Мы начнем с рассмотрения частного случая п. (1).

Лемма 3. *Пусть* $A \subset D$ — *идеал. Если* $\beta \in F$ *таково, что* $\beta A \subset A$, *то* $\beta \in D$.

Доказательство. Согласно предложению 12.2.2, A — конечно порожденный $\mathbf{Z}$-модуль, так что результат следует из предложения 6.1.4. □

Лемма 4. *Если* A *и* B — *идеалы в* D *и* $A = AB$, *то* $B = D$.

Доказательство. Пусть $\alpha_1, \alpha_2, \ldots, \alpha_n$ — целый базис для A. Так как $A = AB$, то можно найти такие элементы $b_{ij} \in B$, что $\alpha_i = \sum_j b_{ij}\alpha_j$. Отсюда следует, что определитель матрицы $(b_{ij} - \delta_{ij})$ равен нулю. Выписывая его, получаем, что $1 \in B$, т. е. $B = D$. □

Предложение 12.2.4. *Пусть* A, $B \subset D$ — *идеалы и предположим, что* $\omega \in D$ *таково, что* $(\omega)\,A = BA$. *Тогда* $(\omega) = B$.

Доказательство. Если $\beta \in B$, то $(\beta/\omega)\,A \subset A$, так что по лемме 3 $\beta/\omega \in D$. Отсюда следует, что $B \subset (\omega)$, а поэтому $\omega^{-1}B \subset D$ — идеал. Так как $A = \omega^{-1}BA$, то лемма 4 показывает, что $\omega^{-1}B = D$, т. е. $B = (\omega)$, как и требовалось. □

Следующее определение играет основополагающую роль в теории алгебраических чисел.

Определение. Два идеала A, $B \subset D$ называются *эквивалентными*, $A \sim B$, если существуют такие ненулевые α, $\beta \in D$, что $(\alpha)\,A = (\beta)\,B$. Это понятие является отношением эквивалентности. Его классы эквивалентности называются *классами идеалов*. Число классов идеалов h_F называется *числом классов* поля F. (Мы убедимся в том, что h_F конечно.)

Простая проверка того, что $A \sim B$ является отношением эквивалентности, предоставляется читателю.

Стоит отметить, что $h_F = 1$ тогда и только тогда, когда D — область главных идеалов (ОГИ). Чтобы убедиться в этом, предположим, что $h_F = 1$, и пусть A — некоторый идеал. Так как $A \sim D$, то существуют такие α, $\beta \in D$, что $(\alpha)\,A = (\beta)\,D = (\beta)$. Таким образом, $\beta/\alpha \in A$ и $A = (\beta/\alpha)$, т. е. каждый идеал главный. С другой стороны, очевидно, что если D — ОГИ, то $h_F = 1$.

Таким образом, мы видим, что число классов измеряет, в некотором смысле, как далеко D отстоит от ОГИ (см. упр. 15, 16 и [184]).

Следующая лемма принадлежит Гурвицу [154], с. 237. Воспользовавшись ею, мы покажем, что h_F конечно. Следует отметить, что эта лемма является (слабым) обобщением алгоритма Евклида на произвольное числовое поле.

Лемма 5. *Существует положительное целое число M, зависящее лишь от F, со следующим свойством. Для заданных $\alpha, \beta \in D$, $\beta \neq 0$, существуют такое целое число t, $1 \leqslant t \leqslant M$, и элемент $\omega \in D$, что $|N(t\alpha - \omega\beta)| < |N(\beta)|$.*

Доказательство. Мы сначала слегка переформулируем утверждение. Пусть $\gamma = \alpha/\beta \in F$. Тогда достаточно показать, что для всех $\gamma \in F$ существует такое M, что $|N(t\gamma - \omega)| < 1$ при некоторых $1 \leqslant t \leqslant M$ и $\omega \in D$.

Пусть $\omega_1, \omega_2, \ldots, \omega_n$ — целый базис в D. Для $\gamma \in F$ имеем $\gamma = \sum_{i=1}^{n} \gamma_i \omega_i$ с $\gamma_i \in \mathbf{Q}$. Заметим, что

$$|N(\gamma)| = \left|\prod_j \left(\sum_i \gamma_i \omega_i^{(j)}\right)\right| \leqslant C \left(\max_i |\gamma_i|\right)^n,$$

где $C = \prod_j \left(\sum_i |\omega_i^{(j)}|\right)$. Выберем $m > \sqrt[n]{C}$ и положим $M = m^n$.

Для $\gamma \in F$, $\gamma = \sum_{i=1}^{n} \gamma_i \omega_i$, запишем $\gamma_i = a_i + b_i$, где $a_i \in \mathbf{Z}$ и $0 \leqslant b_i < 1$. Пусть $[\gamma] = \sum_{i=1}^{n} a_i \omega_i$ и $\{\gamma\} = \sum_{i=1}^{n} b_i \omega_i$. Тогда $\gamma = [\gamma] + \{\gamma\}$, где $[\gamma] \in D$ и координаты $\{\gamma\}$ лежат между 0 и 1.

Отобразим F в евклидово n-мерное пространство $\mathbf{R}^n$ посредством $\varphi\left(\sum_{i=1}^{n} \gamma_i \omega_i\right) = (\gamma_1, \gamma_2, \ldots, \gamma_n)$. Для любого $\gamma \in F$ точка $\varphi(\{\gamma\})$ лежит в единичном кубе. Разобьем единичный куб на m^n подкубов со стороной $1/m$. Рассмотрим точки $\varphi(\{k\gamma\})$ для $1 \leqslant k \leqslant m^n + 1$. Тогда, так как точек больше, чем подкубов, по крайней мере две из них должны лежать в одном и том же подкубе; пусть это будут точки, соответствующие $h\gamma$ и $l\gamma$. Если записать $h\gamma = [h\gamma] + \{h\gamma\}$ и $l\gamma = [l\gamma] + \{l\gamma\}$ и произвести вычитание, мы получим $t\gamma = \omega + \delta$, где (предполагая, что $h > l$) $t = h - l \leqslant m^n = M$, $\omega \in D$ и абсолютная величина координат δ меньше или равна $1/m$.

Согласно предыдущему замечанию, $N(\delta) \leqslant C(1/m)^n = C/m^n < 1$. □

Теорема 1. *Число классов поля F конечно.*

Доказательство. Пусть A — какой-либо идеал в D. Для $\alpha \in A$, $\alpha \neq 0$, $|N(\alpha)|$ — положительное целое число. Выберем $\beta \in A$, $\beta \neq 0$, так, чтобы $|N(\beta)|$ было минимальным. Для любого $\alpha \in A$ существует такое t, $1 \leqslant t \leqslant M$, что $|N(t\alpha - \omega\beta)| < |N(\beta)|$ с $\omega \in D$. Так как $t\alpha - \omega\beta \in A$, то $t\alpha - \omega\beta = 0$. Отсюда следует, что $M!\,A \subset (\beta)$. Пусть $B = (1/\beta)\,M!\,A \subset D$. Тогда B — идеал и $M!\,A = (\beta)\,B$. Поскольку $\beta \in A$, то $M!\,\beta \in (\beta)\,B$, так что $M! \in B$. В силу предложения 12.2.3 $M!$ может содержаться лишь в конечном числе идеалов. Мы показали, что $A \sim B$, где B — один из конечного набора идеалов. Следовательно, h_F конечно, что и утверждалось. □

Интересным и важным приложением этой теоремы является следующее предложение.

Предложение 12.2.5. *Для любого идеала $A \subset D$ существует такое целое число k, $1 \leqslant k \leqslant h_F$, что A^k — главный идеал.*

Доказательство. Рассмотрим множество идеалов $\{A^i \mid 1 \leqslant i \leqslant h_F + 1\}$. По крайней мере два из этих идеалов должны лежать в одном и том же классе, скажем $A^i \sim A^j$, где $i < j$. Существуют такие α, $\beta \in D$, что $(\alpha)\,A^i = (\beta)\,A^j$. Пусть $k = j - i$ и $B = A^k$. Мы покажем, что идеал B главный.

Поскольку очевидно, что $(\alpha)\,A^i = (\beta)\,BA^i$, то $(\alpha/\beta)\,A^i \in A^i$, так что $\alpha/\beta \in D$. Положим $\omega = \alpha/\beta$. Тогда $(\omega)\,A^i = BA^i$. Согласно предложению 12.2.4, $(\omega) = B$. □

Заметим, что множество классов идеалов может быть превращено в группу. Пусть $\overline{A}$ обозначает класс идеала A. Мы определяем произведение классов $\overline{A}$ и $\overline{B}$ как $\overline{AB}$. Нетрудно проверить, что это определение корректно, т. е. если $\overline{A} = \overline{A_1}$ и $\overline{B} = \overline{B_1}$, то $\overline{AB} = \overline{A_1B_1}$. Ассоциативность следует из того, что умножение идеалов ассоциативно. Класс кольца D служит единичным элементом. Наконец, последнее предложение показывает, что обратным для $\overline{A}$ будет класс $\overline{A^{k-1}}$. Изучение структуры группы классов идеалов было одной из важнейших задач с тех пор, как это понятие было введено.

Как следствие того, что классы идеалов образуют группу, получается, что идеал A^{h_F} является главным для всех идеалов A. Это не будет использоваться в оставшейся части главы.

Мы можем теперь доказать два результата, упомянутые ранее (перед леммой 3).

Предложение 12.2.6. *Если A, B и C — идеалы и $AB = AC$, то $B = C$.*

Доказательство. В силу последнего предложения существует такое $k > 0$, что $A^k = (\alpha)$. Умножив $AB = AC$ на A^{k-1}, получим $(\alpha) B = (\alpha) C$. Отсюда следует, что $B = C$. □

Предложение 12.2.7. *Если A и B — идеалы и $B \supset A$, то существует такой идеал C, что $A = BC$.*

Доказательство. Как и выше, существует такое $k > 0$, что $B^k = (\beta)$. Далее, так как $A \subset B$, то $B^{k-1}A \subset B^k = (\beta)$, а значит, $C = (1/\beta) B^{k-1} A \subset D$ — идеал.

Таким образом, $BC = (1/\beta) B^k A = (1/\beta) (\beta) A = A$. □

Это предложение можно выразить фразой «содержать — значит делить».

Мы имеем теперь в распоряжении все нужные средства для получения однозначного разложения на простые идеалы.

Предложение 12.2.8. *Каждый идеал в D может быть представлен в виде произведения простых идеалов.*

Доказательство. Пусть A — какой-либо собственный идеал. Так как D/A конечно, то A содержится в некотором максимальном идеале P_1 (используя лемму Цорна, можно показать, что в произвольном коммутативном кольце с единицей любой собственный идеал содержится в некотором максимальном идеале). В силу последнего предложения $A = P_1 B_1$ для некоторого идеала B_1. Если $B_1 \neq D$, то B_1 содержится в некотором максимальном идеале P_2, так что $A = P_1 P_2 B_2$. Если $B_2 \neq D$, процесс можно продолжить. Заметим, что $A \subset B_1 \subset B_2 \subset \cdots$ — строго возрастающая цепь идеалов. Согласно следствию 1 предложения 12.2.3, после конечного числа шагов будет $B_t = D$. Таким образом, $A = P_1 P_2 \ldots P_t$. □

Пусть P — какой-либо простой идеал. Убывающая цепь $P \supset \supset P^2 \supset P^3 \ldots$ является строго убывающей, ибо если $P^i = P^{i+1}$ для некоторого i, то $PP^i = P^i$, так что $P = D$ по лемме 4. Этот факт является основой следующего определения.

Определение. Пусть P — какой-либо простой идеал и A — идеал. Тогда $\mathrm{ord}_P A$ — однозначно определенное неотрицательное целое число t, для которого $P^t \supset A$ и $P^{t+1} \not\supset A$.

Предложение 12.2.9. *Пусть P — какой-либо простой идеал и A и B — идеалы. Тогда*

(1) $\mathrm{ord}_P P = 1$;

(2) *если $P' \neq P$ прост, то* $\mathrm{ord}_P P' = 0$;

(3) $\mathrm{ord}_P AB = \mathrm{ord}_P A + \mathrm{ord}_P B$.

Доказательство. Первое утверждение очевидно. Что касается (2), то предположим, что $\mathrm{ord}_P P' > 0$. Тогда $P \supset P'$. Так как простые идеалы максимальны, то $P = P'$, что противоречит предположению.

Пусть $t = \mathrm{ord}_P A$ и $s = \mathrm{ord}_P B$. Согласно предложению 12.2.7, $A = P^t A_1$ и $B = P^s B_1$. По тому же предложению $P \not\supset A_1$ и $P \not\supset B_1$. Далее, $AB = P^{t+s} A_1 B_1$. Если $P^{s+t+1} \supset AB$, то $AB = P^{s+t+1} C$, так что, согласно предложению 12.2.6, $PC = A_1 B_1$. Отсюда следует, что $P \supset A_1 B_1$ и, поскольку P прост, $P \supset A_1$ или $P \supset B_1$. Получено противоречие.

Следовательно, $\mathrm{ord}_P AB = t + s = \mathrm{ord}_P A + \mathrm{ord}_P B$. □

Теорема 2. *Пусть $A \subset D$ — какой-либо идеал. Тогда*

$$A = \prod P^{a(P)},$$

где произведение берется по всем различным простым идеалам в D и $a(P)$ — неотрицательные целые числа, почти все равные нулю. Наконец, целые числа $a(P)$ однозначно определены соотношением $a(P) = \mathrm{ord}_P A$.

Доказательство. Представление в виде произведения получается из предложения 12.2.8.

Пусть P_0 — какой-либо простой идеал. Применим ord_{P_0} к обеим частям равенства из формулировки теоремы. Используя предложение 12.2.9, мы видим, что

$$\mathrm{ord}_{P_0} A = \sum_P a(P) \mathrm{ord}_{P_0}(P) = a(P_0).$$ □

§ 3. Ветвление и степень

Пусть P — какой-либо простой идеал в D. Согласно лемме 2, $P \cap \mathbf{Z}$ не равно нулю. Так как очевидно, что это пересечение есть простой идеал в $\mathbf{Z}$, то он должен порождаться некоторым простым числом p.

Определение. Число $e = \mathrm{ord}_P(p)$ называется *индексом ветвления* идеала P (здесь (p) — главный идеал, порожденный p в D).

D/P является конечным полем, содержащим $\mathbf{Z}/p\mathbf{Z}$. Таким образом, число элементов в D/P имеет вид p^f для некоторого $f \geqslant 1$. Число f называется степенью идеала P.

Пусть $p \in \mathbf{Z}$ — какое-либо простое число и $P_1, P_2, \ldots, P_g$ — простые идеалы в D, содержащие (p). Пусть e_i и f_i — индекс ветвления и степень идеала P_i. Согласно теореме 2, $(p) = P_1^{e_1} P_2^{e_2} \ldots P_g^{e_g}$.

Имеется замечательное соотношение между числами e_i, f_i и n.

Теорема 3. $\sum_{i=1}^{g} e_i f_i = n$.

Мы отложим доказательство до тех пор, пока будут получены некоторые необходимые дополнительные результаты.

Предложение 12.3.1. *Пусть R — какое-либо коммутативное кольцо с единицей. Пусть A_1, A_2, ..., A_g — такие идеалы, что $A_i + A_j = R$ для $i \neq j$. Положим $A = A_1 A_2 \dots A_g$. Тогда*

$$R/A \approx R/A_1 \oplus R/A_2 \oplus \dots \oplus R/A_g.$$

Доказательство. Пусть ψ_i — естественное отображение R на R/A_i, и определим ψ: $R \to R/A_1 \oplus \dots \oplus R/A_g$ посредством формулы $\psi(\gamma) = (\psi_1(\gamma), \psi_2(\gamma), \dots, \psi_g(\gamma))$. Мы покажем, что ψ эпиморфно и что его ядро равно A.

Чтобы показать, что ψ эпиморфно, достаточно убедиться в том, что для любых $\gamma_1, \gamma_2, \dots, \gamma_g \in R$ разрешима система сравнений $x_i \equiv \gamma_i (A_i)$, $i = 1, \dots, g$.

Раскрывая скобки в произведении $(A_1 + A_2)(A_1 + A_3) \dots (A_1 + A_g) = R$, убеждаемся в том, что все слагаемые, кроме последнего, содержатся в A_1. Таким образом, $A_1 + A_2 A_3 \dots A_g = R$. Существуют такие элементы $v_1 \in A_1$ и $u_1 \in A_2 \dots A_g$, что $u_1 + v_1 = 1$. Тогда $u_1 \equiv 1 (A_1)$ и $u_1 \equiv 0 (A_i)$ для $i \neq 1$. Аналогично, для каждого j существует такой элемент u_j, что $u_j \equiv 1 (A_j)$ и $u_j \equiv 0 (A_i)$ для $i \neq j$. Тогда очевидно, что $x = \gamma_1 u_1 + \gamma_2 u_2 + \dots + \gamma_g u_g$ будет решением нашей системы уравнений.

Показав, что ψ — эпиморфизм, исследуем теперь его ядро. Ясно, что $\ker \psi = A_1 \cap A_2 \cap \dots \cap A_g$. Мы должны показать, что при сделанных предположениях пересечение равно произведению. Это можно установить с помощью индукции по g. Предположим, что $g = 2$. Тогда, так как $A_1 + A_2 = R$, существуют такие $a_1 \in A_1$ и $a_2 \in A_2$, что $a_1 + a_2 = 1$. Если $a \in A_1 \cap A_2$, то $a = aa_1 + aa_2 \in A_1 A_2$. Это показывает, что $A_1 \cap A_2 \subset A_1 A_2$. Обратное включение очевидно, так что результат верен для $g = 2$. Предположим теперь, что $g > 2$ и результат верен для $g - 1$. Тогда $A_1 \cap A_2 \cap \dots \cap A_g = A_1 \cap A_2 A_3 \dots A_g$. Но $A_1 + A_2 A_3 \dots A_g = R$ по первой части доказательства. Таким образом, $A_1 \cap A_2 A_3 \dots A_g = A_1 A_2 \dots A_g$ и доказательство окончено. □

Это предложение называется китайской теоремой об остатках для колец. Мы возвращаемся от произвольного коммутативного кольца R к кольцу D.

Предложение 12.3.2. *Пусть $P \subset D$ — какой-либо простой идеал и p^f — число элементов в D/P. Число элементов в D/P^e равно p^{ef}.*

Доказательство. Утверждение верно для $e = 1$. Если $e > 1$, то P^{e-1}/P^e является подгруппой в D/P^e и факторгруппа изоморфна D/P^{e-1} (вторая теорема об изоморфизме). Если мы сможем показать, что P^{e-1}/P^e имеет p^f элементов, то результат будет получаться по индукции.

Так как $P^e \subset P^{e-1}$ — собственное вложение, то можно найти такой элемент $\alpha \in P^{e-1}$, что $\alpha \notin P^e$. Мы утверждаем, что $(\alpha) + P^e = P^{e-1}$. Поскольку $P^e \subset (\alpha) + P^e$, последний идеал должен быть степенью идеала P. Так как $(\alpha) + P^e \subset P^{e-1}$, то $(\alpha) + P^e = P^{e-1}$.

Отобразим D в P^{e-1}/P^e при помощи соответствия $\gamma \to \gamma\alpha + P^e$. Это отображение, как нетрудно убедиться, — эпиморфизм. Элемент γ принадлежит ядру тогда и только тогда, когда $\gamma\alpha \in P^e$, т. е. в том и только том случае, когда $\mathrm{ord}_P(\gamma\alpha) \geqslant e$. Но $\mathrm{ord}_P(\gamma\alpha) = \mathrm{ord}_P(\gamma) + \mathrm{ord}_P(\alpha) = \mathrm{ord}_P(\gamma) + e - 1$. Таким образом, γ лежит в ядре, если и только если $\mathrm{ord}_P(\gamma) \geqslant 1$, что эквивалентно включению $\gamma \in P$. Следовательно, $D/P \approx P^{e-1}/P^e$, а потому последняя группа имеет p^f элементов. □

Мы можем теперь доказать теорему 3. Напомним, что $(p) = P_1^{e_1}P_2^{e_2} \ldots P_g^{e_g}$. Нетрудно убедиться в том, что $P_i^{e_i} + P_j^{e_j} = D$ для $i \neq j$ (см. упр. 25). Согласно предложению 12.3.1.

$$D/(p) \approx D/P_1^{e_1} \oplus D/P_2^{e_2} \oplus \ldots \oplus D/P_g^{e_g}.$$

При доказательстве предложения 12.2.3 показано, что $|D/(p)| = p^n$. С другой стороны, предложение 12.3.2 показывает, что $|D/P_i^{f_i}|$ имеет $p^{e_i f_i}$ элементов. Таким образом,

$$p^n = p^{e_1 f_1} p^{e_2 f_2} \ldots p^{e_g f_g}.$$

Отсюда следует, что $n = e_1 f_1 + e_2 f_2 + \ldots + e_g f_g$, как и утверждалось. □

В случае когда $F/\mathbf{Q}$ — нормальное расширение, т. е. когда все изоморфизмы поля F в $\mathbf{C}$ в действительности являются автоморфизмами, теорема 3 может быть усилена. Предположим, что $F/\mathbf{Q}$ нормально, и пусть G — его группа Галуа. Если A — какой-либо идеал и $\sigma \in G$, положим $\sigma A = \{\sigma\alpha \mid \alpha \in A\}$. Нетрудно проверить, что σA — тоже идеал. Кроме того, $\sigma D = D$. Таким образом, $D/\sigma A = \sigma D/\sigma A \approx D/A$. В частности, это показывает, что если P — простой идеал, то σP — тоже простой идеал.

Предложение 12.3.3. *Пусть $p \in \mathbf{Z}$ — какое-либо простое число. Предположим, что P_i и P_j — простые идеалы в D, содержащие p. Тогда существует такой автоморфизм $\sigma \in G$, что $\sigma P_i = P_j$.*

Доказательство. Предположим, что существует простой идеал P_0, содержащий p и не принадлежащий множеству $\{\sigma P_i \mid \sigma \in G\}$. В силу предложения 12.3.1 можно найти такой элемент $\alpha \in D$, что $\alpha \equiv 0\ (P_0)$ и $\alpha \equiv 1\ (\sigma P_i)$ для всех $\sigma \in G$. Тогда $N(\alpha) = \prod_{\sigma \in G} \sigma\alpha \in P_0 \cap \mathbf{Z} = p\mathbf{Z}$. Отсюда следует, что $N(\alpha) \in P_i$, так что $\sigma\alpha \in P_i$ при некотором σ, ибо P_i — простой идеал. Но тогда $\alpha \in \sigma^{-1}P_i$, что противоречит сравнению $\alpha \equiv 1\ (\sigma^{-1}P_i)$.

Теорема 3′. *Предположим, что $F/\mathbf{Q}$ — нормальное расширение. Пусть $p \in \mathbf{Z}$ — какое-либо простое число, и запишем $(p) = P_1^{e_1}P_2^{e_2} \ldots P_g^{e_g}$. Тогда $e_1 = e_2 = \ldots = e_g$ и $f_1 = f_2 = \ldots = f_g$. Если e и f обозначают эти общие значения, то $efg = n$.*

Доказательство. Для фиксированного индекса i существует такой автоморфизм $\sigma \in G$, что $\sigma P_1 = P_i$. Так как $D/P_1 \approx D/\sigma P_1 = D/P_i$, то $f_1 = f_i$. Поэтому все f_i равны.

Применим σ к обеим частям разложения $(p) = P_1^{e_1} \ldots P_g^{e_g}$. Так как $p \in \mathbf{Z}$, очевидно, что $\sigma(p) = (p)$. Таким образом,

$$(p) = (\sigma P_1)^{e_1}(\sigma P_2)^{e_2} \ldots (\sigma P_g)^{e_g}.$$

В этом произведении показатель степени у $P_i = \sigma P_1$ равен e_1. В первом представлении показатель степени у P_i равен e_i. В силу однозначности разложения на простые идеалы мы должны иметь $e_1 = e_i$, так что все e_i равны.

Наконец, из $\sum e_i f_i = n$ непосредственно следует, что $efg = n$. □

Мы закончим этот параграф обсуждением (без доказательств) некоторых важных фактов о числовых полях. В наших приложениях мы обойдемся без этой общей теории.

Пусть $P \subset D$ — какой-либо простой идеал с индексом ветвления e. Пусть $p \cap \mathbf{Z} = p\mathbf{Z}$. Идеал P называется *разветвленным*, если $e > 1$. Можно показать, что P разветвлен лишь в случае, когда p делит $\delta_F = \Delta(D)$, дискриминант поля F. В частности, разветвлено лишь конечное число простых идеалов. Если $p \nmid \delta_F$, то (p) будет произведением разных простых идеалов в D. Важный результат Минковского состоит в том, что если $[F : \mathbf{Q}] > 1$, то $|\delta_F| > 1$. На самом деле Минковский получил более сильный результат, а именно, нашел точную нижнюю границу для $|\delta_F|$.

Важным следствием является то, что каждое числовое поле, большее чем $\mathbf{Q}$, содержит разветвленные простые идеалы.

Предположим теперь, что $F/\mathbf{Q}$ — нормальное расширение с группой Галуа G. Поставим в соответствие любому простому идеалу P группу $G(P) = \{\sigma \in G \mid \sigma P = P\}$. Она называется *группой разложения идеала* P. Поле D/P конечно и содержит $\mathbf{Z}/p\mathbf{Z}$. Оно является нормальным расширением поля $\mathbf{Z}/p\mathbf{Z}$. Обозначим получающуюся группу Галуа через $\bar{G}$. Имеется гомоморфизм из $G(P)$ в $\bar{G}$, задаваемый следующим образом. Если $\sigma \in G(P)$ и $\bar{\alpha}$ обозначает класс вычетов элемента α в D/P, то определим $\bar{\sigma}$ равенством $\bar{\sigma}(\bar{\alpha}) = \overline{\sigma\alpha}$. Это определение корректно, $\bar{\sigma} \in \bar{G}$ и $\sigma \to \bar{\sigma}$ — гомоморфизм. Можно показать, что это эпиморфизм (упр. 26). Пусть $T(P)$ обозначает его ядро. Оно называется *группой инерции* для P. Тогда

$$G(P)/T(P) \approx \bar{G}.$$

Нетрудно убедиться в том, что $|\bar{G}| = f$ и $|G(P)| = n/g = ef$. Отсюда следует, что $|T(P)| = e$. Таким образом, если P неразветвлен, то $G(P) \approx \bar{G}$.

Из теории конечных полей следует, что $\bar{G}$ — циклическая группа, порожденная автоморфизмом φ_p, который переводит $\bar{\alpha}$ в $\bar{\alpha}^p$. Если P неразветвлен, то существует единственный элемент $\sigma_P \in G(P)$, для которого $\bar{\sigma}_P = \varphi_p$. Этот автоморфизм σ_P называется *автоморфизмом Фробениуса*, соответствующим P. Заметим, что порядок элемента σ_P равен порядку элемента φ_p, т. е. f, степени идеала P. Оказывается, что бо́льшая часть арифметической теории полей алгебраических чисел концентрируется вокруг свойств автоморфизма Фробениуса. В следующей главе мы увидим иллюстрации этого утверждения.

Замечания

Результат о том, что кольцо целых чисел в произвольном поле алгебраических чисел является дедекиндовым кольцом, принадлежит Дедекинду и содержится в одиннадцатом дополнении к «Vorlesungen über Zahlentheorie» («Лекциям по теории чисел») Дирихле [127]. Этот результат затем был доказан также Кронекером, Гильбертом и Гурвицом. Группы инерции и разложения были введены Гильбертом (1894 г.) в его работе «Grundzüge einer Theorie des Galoisschen Zahlkörpers» («Основы теории нормальных числовых полей») (см. также § 39 в «Zahlbericht» («Докладах по теории чисел») Гильберта [151] и [121], т. 2, с. 43—49).

Можно показать в более общем виде, что если D — дедекиндово кольцо с полем частных k и K — конечное сепарабельное

расширение поля k, то целое замыкание D в K (упр. 27) будет дедекиндовым кольцом. Это следует из теоремы Э. Нётер, характеризующей дедекиндовы кольца как нётеровы области, которые целозамкнуты и в которых каждый ненулевой простой идеал максимален. С этим подходом можно познакомиться в [214]. В нашем подходе, как и в других классических подходах, существенно используется тот факт, что кольцо классов вычетов по модулю какого-либо ненулевого идеала конечно. Идея получения свойства дедекиндовости из конечности числа классов принадлежит Гурвицу. Следует заметить, что при нашем подходе не использовался тот факт, что число элементов в кольце классов вычетов является мультипликативной функцией идеала. В [103] показано, что из мультипликативности этого отображения следует свойство дедекиндовости. Обычный классический подход состоит в том, чтобы показать при помощи подходящего обобщения леммы Гаусса (упр. 4, гл. 6), что классы идеалов образуют группу.

В последнее время характеризация полей F с числом классов 2, принадлежащая Карлитцу (см. упр. 15 и 16), была обобщена в [117]. Среди других результатов там доказывается, что группа классов идеалов числового поля является циклической группой порядка 2, циклической группой порядка 3 или четверной группой Клейна тогда и только тогда, когда произведение двух неприводимых элементов может быть записано в виде произведения, самое большее, трех других неприводимых элементов.

Глубокий результат, высказанный Гильбертом в виде гипотезы и доказанный Фуртвенглером, состоит в доказательстве существования для каждого числового поля F расширения E, удовлетворяющего следующим условиям. Прежде всего степень E над F равна числу классов поля F. Каждый простой идеал $\mathfrak{P}$ для F разлагается в произведение h_F/f различных простых идеалов в E, где f — порядок класса идеалов для $\mathfrak{P}$ в группе классов. Каждый идеал F становится главным в E. Наконец, группа классов идеалов для F изоморфна группе Галуа поля E над F. Поле E единственно и называется *гильбертовым полем классов* для F. Существование гильбертова поля классов является ценным подспорьем при изучении структуры группы классов идеалов.

Действительное вычисление числа классов — трудное дело. Даже для квадратичных полей с малым дискриминантом это вычисление требует привлечения таких оценок (принадлежащих Минковскому), которые мы опустили. Эти вопросы обсуждаются в большинстве стандартных курсов по теории алгебраических чисел. Мы рекомендуем изложение в [183]. Эта книга содержит большое количество интересных упражнений.

В более современных изложениях стало обычным описывать группу классов идеалов в терминах дробных идеалов. Если D — область целостности с полем частных F, то *дробный идеал* A —

это D-подмодуль в F, для которого существует какой-либо элемент d в D с $dA \subset D$. Дробные идеалы могут очевидным способом перемножаться. Можно показать, что D — дедекиндово кольцо тогда и только тогда, когда (ненулевые) дробные идеалы образуют группу [214]. Подгруппа дробных идеалов вида fD, где f из F, состоит из главных дробных идеалов. Нетрудно показать, что группа классов идеалов поля алгебраических чисел изоморфна факторгруппе группы дробных идеалов по подгруппе главных дробных идеалов.

Упражнения

1. Найти минимальный многочлен для $\sqrt{3} + \sqrt{7}$.

2. Вычислить дискриминант поля $\mathbf{Q}(\sqrt{2} + \sqrt{5})$.

3. Описать единицы в $\mathbf{Q}(\sqrt{5})$.

4. Пусть D — кольцо целых чисел в $\mathbf{Q}(\sqrt{d})$. Показать, что при заданном $N > 0$ существует лишь конечное число элементов $\alpha \in D$, таких, что $\max(|\alpha|, |\alpha'|) \leqslant N$, где α' — сопряженное к α.

5. Обобщить упр. 4 на произвольное числовое поле.

6. Если D — кольцо целых чисел в поле алгебраических чисел и $\mathfrak{P}$ — такой простой идеал, что $\mathfrak{P} = (\alpha)$, то показать, что α — неприводимый элемент.

7. Показать, что число классов поля $\mathbf{Q}(\sqrt{-5})$ больше единицы.

8. Пусть F — числовое поле. Показать, что дискриминант δ_F сравним с 0 или 1 по модулю 4. Это одна из теорем Штикельбергера. Доказательство довольно хитроумное (см. [207], с. 97).

9. Вычислить дискриминант $\Delta(1, \alpha, \alpha^2)$ относительно $\mathbf{Q}$, где α — корень неприводимого многочлена $x^3 + px + q$, $p, q \in \mathbf{Q}$.

10. Если $R \subset S$ — области целостности, то $\alpha \in S$ называется *целым над* R, если $\alpha^m + b_1\alpha^{m-1} + \ldots + b_m = 0$ для подходящих m; $b_1, \ldots, b_m \in R$. Кольцо S называется *целым* над R, если каждый элемент из S цел над R. Доказать, что если S цело над R, то S — поле тогда и только тогда, когда R — поле.

11. Пусть $\alpha_1, \ldots, \alpha_n$ лежат в D, кольце целых чисел в числовом поле F, $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$. Показать, что если $\Delta(\alpha_1, \ldots, \alpha_n)$ — произведение различных простых чисел (т. е. Δ свободно от квадратов), то $\alpha_1, \ldots, \alpha_n$ составляют целый базис. Отсюда сделать вывод о том, что если d свободно от квадратов и $d \equiv 1$ (4), то $(1 + \sqrt{d})/2$, 1 образуют целый базис кольца целых чисел в $\mathbf{Q}(\sqrt{d})$.

12. Показать, что $\sin(\pi/12)$ — алгебраическое число.

13. Показать, что $(3, 1 + \sqrt{-5})$ — собственный идеал в $\mathbf{Z}[\sqrt{-5}]$. Простой ли он?

14. Построить неприводимый кубический многочлен над $\mathbf{Q}$, имеющий лишь вещественные корни.

15. Пусть F — некоторое поле алгебраических чисел, а D — кольцо его целых чисел. Предположим, что число классов поля равно 2. Показать, что если π — такой неразложимый элемент, что (π) не является простым, то $(\pi) = \mathfrak{P}_1\mathfrak{P}_2$, где $\mathfrak{P}_1$, $\mathfrak{P}_2$ суть (не обязательно различные) простые идеалы.

16 (Карлитц). Пусть F, D обозначают то же самое, что и в упр. 15. Показать, что если $\alpha \in D$ и $\alpha = \pi_1 \ldots \pi_t = \lambda_1 \ldots \lambda_s$ — два разложения α на неразложимые элементы, то $s = t$. [*Замечание.* Обращение утверждения тоже верно! (ср. [106]).]

17. Пусть $f(x)$, $g(x)$ — минимальные многочлены для α и β степеней n и m соответственно. Пусть корнями многочленов $f(x)$ и $g(x)$ в $\mathbf{C}$ будут соответственно $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ и $\beta = \beta_1, \beta_2, \ldots, \beta_m$. Напомним, что, согласно упр. 16 из

гл. 6, кратные корни отсутствуют. Выберем $t \in \mathbf{Q}$ так, что $\alpha_i + t\beta_j \neq \alpha + t\beta$ при $j \neq 1$ и всех i. Положим $\gamma = \alpha + t\beta$. Показать, что

(a) наибольшим общим делителем (в $\mathbf{C}[x]$) многочленов $f(\gamma - tx)$, $g(x)$ является $x - \beta$;

(b) (с другой стороны) наибольший общий делитель для $f(\gamma - tx)$ и $g(x)$ лежит в $\mathbf{Q}(\gamma)[x]$;

(c) $\beta \in \mathbf{Q}(\gamma)$, $\alpha \in \mathbf{Q}(\gamma)$.

18. (Теорема о примитивном элементе.) Показать, что если F — поле алгебраических чисел, то существует такой элемент $\gamma \in F$, что $\mathbf{Q}(\gamma) = F$.

19. Показать, что конечная область целостности является полем.

20. Пусть $K = F_2(x)$ и $L = K(\sqrt{x})$. Показать, что отображение следа тождественно равно нулю. (Напомним, что F_2 — конечное поле с двумя элементами.)

21. Пусть F — поле алгебраических чисел степени n. Для $\alpha \in F$ пусть T — линейное преобразование, определенное формулой $T(y) = \alpha y$. Показать, что $\det(xI - T) = f(x)^t$, где $t = n/\deg(f)$ и $f(x)$ — минимальный многочлен для α.

22. Пусть $F \subset E$ — поля алгебраических чисел. Показать, что каждый изоморфизм поля F в $\mathbf{C}$ имеет точно $[E : F]$ продолжений до изоморфизма поля E в $\mathbf{C}$.

23. Пусть F — поле алгебраических чисел степени n и $\sigma_1, \ldots, \sigma_n$ — различные изоморфизмы F в $\mathbf{C}$. Показать, что в обозначениях упр. 21 $f(x)^t = \prod_{i=1}^{n} (x - \sigma_i(\alpha))$ для $\alpha \in F$.

24. В обозначениях упр. 23 показать, что

$$N_{F/\mathbf{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \text{ и } t_{F/\mathbf{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

25. Пусть F — поле алгебраических чисел с кольцом целых чисел D. Показать, что если P и Q — различные простые идеалы, то $(P^a, Q^b) = D$, где a и b — положительные целые числа.

26. Пусть P — простой идеал в кольце целых чисел D какого-либо поля алгебраических чисел F. Показать, что если F нормально, то естественное отображение из группы разложения идеала P в группу Галуа поля классов вычетов по нему эпиморфно.

27. Если k — некоторое поле, содержащее кольцо D, то множество всех элементов из k, целых над D (упр. 10), называется целым замыканием кольца D в k. Показать, что целое замыкание является кольцом, которое целозамкнуто.

28. Пусть D — кольцо целых чисел в числовом поле F. Предположим, что $(p) = P^2A$ для простого p в $\mathbf{Z}$ и простого идеала P. Показать, что

(a) существует $\alpha \in PA$, такое, что $a \notin P^2A$;

(b) $(\alpha\beta)^p \in pD$ для всех $\beta \in D$;

(c) $(\mathrm{tr}(\alpha\beta))^p \equiv \mathrm{tr}((\alpha\beta)^p)$ (pD);

(d) $p \mid \mathrm{tr}(\alpha\beta)$ для всех $\beta \in D$;

(e) $p \mid \Delta$, дискриминант поля F. (Обязательно использовать то, что $\alpha \notin pD$.)

29. Пусть F — некоторое нормальное расширение поля $\mathbf{Q}$ с абелевой группой Галуа. Показать, что если $p \in \mathbf{Q}$ неразветвлен в F, то $\sigma_P = \sigma_{P'}$ для простых идеалов P и P', делящих p в F, где σ_P обозначает автоморфизм Фробениуса.

30. Для некоторого нечетного простого числа p рассмотрим $\mathbf{Q}(\sqrt{p})$. Для $q \neq p$ показать, что $\sigma_q(\sqrt{p}) = (p/q)\sqrt{p}$, где σ_q — автоморфизм Фробениуса для простого идеала в $\mathbf{Q}(\sqrt{p})$, лежащего над q.

31. Пусть F — поле алгебраических чисел и $\mathfrak{A}$ — некоторый идеал в кольце целых чисел поля F. Показать, что существует такое конечное расширение L поля F с кольцом целых чисел S, что $\mathfrak{A}S$ — главный идеал.

32. Пусть P — какой-либо простой идеал в кольце целых чисел D числового поля F. Показать, что если $a \equiv b \pmod{P^t}$ и $\operatorname{ord}_P b < t$, то $\operatorname{ord}_P a = \operatorname{ord}_P b$.

33. Пусть $K \subset L$ — числовые поля с кольцами целых чисел R и S соответственно. Показать, что если A и B — такие идеалы в R, что AS делит BS, то A делит B.

34. В обозначениях предыдущего упражнения показать, что $AS \cap R = A$.

Глава 13

КВАДРАТИЧНЫЕ И КРУГОВЫЕ ПОЛЯ

В предыдущей главе мы обсуждали общую теорию полей алгебраических чисел и их колец целых чисел. Теперь мы более детально рассмотрим два важных класса этих полей, которые впервые изучались в девятнадцатом веке Гауссом, Эйзенштейном, Куммером, Дирихле и другими в связи с теорией квадратичных форм, высшими законами взаимности и последней теоремой Ферма. Читателю, который интересуется историческим обзором по этому предмету, следует обратиться к книге [128], *а также к классическому курсу* [72].

В этой главе мы излагаем лишь те результаты, которые нам понадобятся в последующих главах. Основной результат состоит в описании того, как рациональные простые числа разлагаются в произведение простых идеалов. Наряду с этим мы не можем отказаться от возможности привести еще одно доказательство квадратичного закона взаимности, основанное на законах разложения в этих полях.

§ 1. Квадратичные числовые поля

Поле алгебраических чисел F будет называться *квадратичным*, если $[F : \mathbf{Q}] = 2$. Пусть $D \subset F$, — как обычно, кольцо целых чисел в F. Наша ближайшая цель — найти явно целый базис для D.

Пусть $F = \mathbf{Q}(\alpha)$. Элемент α должен удовлетворять квадратному уравнению $ax^2 + bx + c = 0$ с $a, b, c \in \mathbf{Z}$. Таким образом,

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Положим $A = b^2 - 4ac$. Тогда очевидно, что $F = \mathbf{Q}(\sqrt{A})$. Пусть $A = A_1^2 A_2$, где $A_1, A_2 \in \mathbf{Z}$ и A_2 свободно от квадратов. В таком случае $F = \mathbf{Q}(\sqrt{A_2})$. Мы показали (изменяя обозначения), что каждое квадратичное числовое поле имеет вид $\mathbf{Q}(\sqrt{d})$, где d — свободное от квадратов целое число.

Если σ — любой изоморфизм поля $F/\mathbf{Q}$ в $\mathbf{C}$, то мы применяем σ к $(\sqrt{d})^2 = d$ и получаем $(\sigma\sqrt{d})^2 = d$. Таким образом, $\sigma\sqrt{d} =$

$= \pm \sqrt{d}$. Отсюда следует, что $F/\mathbf{Q}$ — нормальное расширение. Его группа Галуа имеет два элемента, единицу и автоморфизм, переводящий $\sqrt{d}$ в $-\sqrt{d}$.

Каждый элемент поля F имеет вид $\alpha = r + s\sqrt{d}$ с $r, s \in \mathbf{Q}$. Нетривиальный автоморфизм переводит α в $\alpha' = r - s\sqrt{d}$. Таким образом, $t(\alpha) = \alpha + \alpha' = 2r$ и $N(\alpha) = \alpha\alpha' = r^2 - ds^2$.

Если $\gamma \in D$, то $t(\gamma)$ и $N(\gamma) \in \mathbf{Z}$. Обратно, если эти условия выполняются, то γ удовлетворяет уравнению $0 = (x - \gamma)(x - \gamma') = x^2 - t(\gamma)x + N(\gamma) \in \mathbf{Z}[x]$, которое показывает, что $\gamma \in D$. Таким образом, $\gamma \in D$ тогда и только тогда, когда $t(\gamma)$ и $N(\gamma) \in \mathbf{Z}$.

Предложение 13.1.1. *Если* $d \equiv 2, 3\ (4)$, *то* $D = \mathbf{Z} + \mathbf{Z}\sqrt{d}$. *Если* $d \equiv 1\ (4)$, *то* $D = \mathbf{Z} + \mathbf{Z}((-1 + \sqrt{d})/2)$.

Доказательство. Пусть $\gamma = r + s\sqrt{d}$, $r, s \in \mathbf{Q}$. Тогда $\gamma \in D$ в том и только том случае, когда $2r$ и $r^2 - s^2d \in \mathbf{Z}$. Так как $2r \in \mathbf{Z}$, из второго условия следует, что $4s^2d \in \mathbf{Z}$. Так как d свободно от квадратов, то $2s \in \mathbf{Z}$. Положим $2r = m$ и $2s = n$. Тогда из $r^2 - ds^2 \in \mathbf{Z}$ следует, что $m^2 - dn^2 \equiv 0\ (4)$.

Напомним, что квадрат сравним либо с 0, либо с 1 по модулю 4.

Если $d \equiv 2, 3\ (4)$, то $m^2 - dn^2 \equiv m^2 + 2n^2\ (4)$ или $m^2 - dn^2 \equiv m^2 + n^2\ (4)$. Единственная возможность, чтобы число $m^2 + 2n^2$ или число $m^2 + n^2$ делилось на 4, это чтобы оба числа m и n были четными. Это будет выполняться тогда и только тогда, когда r и s лежат в $\mathbf{Z}$. Тем самым получено первое утверждение.

Если $d \equiv 1\ (4)$, то $m^2 - dn^2$ сравнимо с $m^2 - n^2$ по модулю 4. Но $m^2 - n^2 \equiv 0\ (4)$, если и только если m и n имеют одинаковую четность, т. е. оба они либо нечетные, либо четные. Таким образом, $D = \{(m + n\sqrt{d})/2 \mid m \equiv n\ (2)\}$. Заметим, что

$$\frac{m + n\sqrt{d}}{2} = \frac{m + n}{2} + n\left(\frac{-1 + \sqrt{d}}{2}\right).$$

Так как $m \equiv n\ (2)$, то $(m + n)/2 \in \mathbf{Z}$. Таким образом, $D \subset \mathbf{Z} + \mathbf{Z}(-1 + \sqrt{d})/2$. Для получения обратного включения мы просто заметим, что $(-1 + \sqrt{d})/2 \in D$, ибо $d^2 \equiv 1\ (4)$ □

Теперь мы можем вычислить дискриминант квадратичных числовых полей.

Предложение 13.1.2. *Пусть* δ_F *обозначает дискриминант поля* F.

Если $d \equiv 2, 3 \pmod 4$, *то* $\delta_F = 4d$.
Если $d \equiv 1 \pmod 4$, *то* $\delta_F = d$.

Доказательство. При $d \equiv 2, 3 \pmod 4$ положим $\omega_1 = 1$ и $\omega_2 = \sqrt{d}$. Тогда

$$(t(\omega_i\omega_j)) = \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix}.$$

Таким образом, в этом случае $\delta_F = \det(t(\omega_i\omega_j)) = 4d$.

При $d \equiv 1 \pmod 4$ положим $\omega_1 = 1$ и $\omega_2 = (-1 + \sqrt{d})/2$. Тогда

$$(t(\omega_i\omega_j)) = \begin{pmatrix} 2 & -1 \\ -1 & (1+d)/2 \end{pmatrix}.$$

Значит, в этом случае $\delta_F = \det(t(\omega_i\omega_j)) = d$. □

Исследовав D и δ_F, мы хотим теперь выяснить, как рациональные простые числа $p \in \mathbf{Z}$ разлагаются в D. Из теоремы 3′ гл. 12 мы знаем, что $efg = 2$, так что возможны три случая: $e = 2$, $f = 1$, $g = 1$; $e = 1$, $f = 1$, $g = 2$; $e = 1$, $f = 2$, $g = 1$. Мы говорим соответственно, что число p *разветвляется*, *полностью разлагается или инертно* (inertial) (*остается простым*).

Если p — какое-либо простое число в $\mathbf{Z}$, то пусть P — простой идеал в D, содержащий p. Пусть $P' = \{\gamma' \mid \gamma \in P\}$.

Предложение 13.1.3. *Предположим, что* p *нечетно.*
(i) *Если* $p \nmid \delta_F$ *и* $x^2 \equiv d \pmod p$ *разрешимо в* $\mathbf{Z}$, *то* $(p) = PP'$, $P \neq P'$.
(ii) *Если* $p \nmid \delta_F$ *и* $x^2 \equiv d \pmod p$ *неразрешимо в* $\mathbf{Z}$, *то* $(p) = P$.
(iii) *Если* $p \mid \delta_F$, *то* $(p) = P^2$.

Доказательство. В случае (i) предположим, что $a^2 \equiv d \pmod p$, где $a \in \mathbf{Z}$. Мы утверждаем, что $(p) = (p, a + \sqrt{d})(p, a^2 - \sqrt{d})$. Действительно,

$$(p, a+\sqrt{d})(p, a-\sqrt{d}) = (p)(p, a+\sqrt{d}, a-\sqrt{d}, (a^2-d)/p).$$

Последний идеал совпадает с D, так как он содержит p и $2a$, а эти два числа взаимно просты. Мы утверждаем, что $(p, a + \sqrt{d}) \neq (p, a - \sqrt{d})$. Если бы эти идеалы были равны, то они содержали бы p и $2a$ и, таким образом, совпадали бы с D. В этом случае $(p) = D$. Таким образом, p полностью разлагается, что и утверждалось.

В случае (ii) мы утверждаем, что P имеет степень 2. Если степень P равна 1, то D/P имеет p элементов. Так как $\mathbf{Z}/p\mathbf{Z}$ вкладывается в D/P, отсюда следовало бы, что каждый класс смежности из D/P представляется рациональным целым числом. Пусть $a \in$

$\in \mathbf{Z}$ — такой элемент, что $a \equiv \sqrt{d}\ (P)$. Тогда $a^2 \equiv d\ (P)$ и $a^2 \not\equiv d\ (p)$, вопреки предположению. Таким образом, p остается простым, как и утверждалось.

Наконец, в случае (iii) мы утверждаем, что $(p) = (p, \sqrt{d})^2$. Действительно, $(p, \sqrt{d})^2 = (p)\,(p, \sqrt{d}, d/p)$. Последний идеал равен D, так как p и d/p взаимно просты (вспомним, что d свободно от квадратов). Таким образом, p разветвляется, как и утверждалось. □

Мы обсудим теперь разложение на простые идеалы простого числа $p = 2$. Напомним, что, согласно предложению 13.1.2, $2 \nmid \delta_F$ в том и только том случае, когда $d \equiv 1\ (4)$.

Предложение 13.1.4. *Предположим, что* $p = 2$.
(i) *Если* $2 \nmid \delta_F$ *и* $d \equiv 1\ (8)$, *то* $(2) = PP'$ *и* $P \neq P'$.
(ii) *Если* $2 \nmid \delta_F$ *и* $d \equiv 5\ (8)$, *то* $(2) = P$.
(iii) *Если* $2 \mid \delta_F$, *то* $(2) = P^2$.

Доказательство. Если $d \equiv 1\ (8)$, то мы утверждаем, что $(2) = (2, (1 + \sqrt{d})/2)\,(2, (1 - \sqrt{d})/2$. Действительно, $(2, (1 + \sqrt{d})/2)\,(2, (1 - \sqrt{d})/2) = (2)\,(2, 1 + \sqrt{d})/2, (1 - \sqrt{d})/2, (1 - d)/8)$. Последний идеал равен D, так как он содержит $1 = (1 + \sqrt{d})/2 + (1 - \sqrt{d})/2$. Кроме того, $(2, (1 + \sqrt{d})/2) \neq (2, (1 - \sqrt{d})/2)$, так как в противном случае этот идеал содержал бы 1, откуда следовало бы, что $(2) = D$.

Если $d \equiv 5\ (8)$, то мы утверждаем, что P имеет степень 2. Если это не так (как в п. (ii) предыдущего предложения), найдется такое целое число $a \in \mathbf{Z}$, что $a \equiv (1 + \sqrt{d})/2\ (P)$. Так как $(1 + \sqrt{d})/2$ удовлетворяет уравнению $x^2 - x + (1 - d)/4 = 0$, мы имели бы в таком случае $a^2 - a + (1 - d)/4 \equiv 0\ (P)$, а потому $a^2 - a + (1 - d)/4 \equiv 0\ (2)$. Число $a^2 - a$ четно при всех $a \in \mathbf{Z}$. Отсюда следует, что $(1 - d)/4 \equiv 0\ (2)$, или $d \equiv 1\ (8)$, вопреки предположению.

Предположим теперь, что $2 \mid \delta_F$. Мы должны иметь $d \equiv 2, 3\ (4)$. Если $d \equiv 2\ (4)$, то $(2) = (2, \sqrt{d})^2$, а если $d \equiv 3\ (4)$, то $(2) = (2, 1 + \sqrt{d})^2$. Простую проверку этого мы оставляем читателю. □

Заметим, что закон разложения для нечетных простых чисел можно сформулировать в сжатом виде, используя символ Лежандра. А именно, если $(\delta_F/p) = 1$, то p полностью разлагается, если $(\delta_F/p) = -1$, то p остается простым, и если $(\delta_F/p) = 0$, то p разветвляется. Кроме того, закон разложения для p, p нечетно, зависит лишь от класса вычетов числа p по модулю δ_F.

Ибо если $d \equiv 2$ или 3 по модулю 4, то $\delta_F = 4d$ и доказываемое утверждение следует из предложения 5.5.3 и упр. 37 гл. 5. Если $d \equiv 1$ (4), то мы можем доказать это следующим образом. При $d \equiv 1$ (4) имеет место равенство $\delta_F = d$. Таким образом,

$$\left(\frac{\delta_F}{p}\right) = (-1)^{((p-1)/2)((\delta_F-1)/2)}\left(\frac{p}{\delta_F}\right) = \left(\frac{p}{\delta_F}\right).$$

Значение (p/δ_F) зависит лишь от класса вычетов p по модулю δ_F.

Теперь мы определим структуру группы единиц в D. Нетрудно убедиться в том, что α является единицей тогда и только тогда, когда $N(\alpha) = \pm 1$. Рассмотрим сначала случай мнимого квадратичного поля, так что $d < 0$. Пусть U_d обозначает группу единиц в D.

Предложение 13.1.5. *Если d меньше 0 и свободно от квадратов, то*

(a) $U_{-1} = \{1, i, -1, -i\}$;

(b) $U_{-3} = \{\pm 1, \pm\omega, \pm\omega^2\}$, *где* $\omega = (-1 + \sqrt{-3})/2$;

(c) $U_d = \{1, -1\}$ *для* $d < -3$ *или* $d = -2$.

Доказательство. Если $d \equiv 2$ или 3 (4), то любая единица может быть записана в виде $x + y\sqrt{d}$, $x, y \in \mathbf{Z}$. Таким образом, $N(\alpha) = \pm 1$ эквивалентно равенству $x^2 + |d|y^2 = 1$. При $d = -1$ получаем случай (a). При $|d| > 1$ очевидно, что $U_d = \{+1, -1\}$.

При $d \equiv 1$ (4) запишем $\alpha = (x + y\sqrt{d})/2$, где $x \equiv y$ (2). Тогда $N(\alpha) = \pm 1$ эквивалентно равенству $x^2 + |d|y^2 = 4$. Если $d = -3$, то решение уравнения $x^2 + 3y^2 = 4$ приводит к случаю (b), в то время как при $|d| > 3$ уравнение $x^2 + |d|y^2 = 4$ приводит к тому, что $U_d = \{+1, -1\}$. Это завершает доказательство. □

Таким образом, нахождение группы единиц в случае мнимого поля — очень простая задача. Случай вещественного квадратичного поля значительно более трудный.

Если d больше 0 и свободно от квадратов, то уравнение $x^2 - dy^2 = 1$ называется уравнением Пелля. В гл. 17, § 5, показано, что это уравнение имеет решение в ненулевых целых числах x, y. Доказательство элементарно. Предполагая известным этот результат, мы опишем единицы в D для вещественного квадратичного поля.

Предложение 13.1.6. *Если D — кольцо целых чисел в $\mathbf{Q}(\sqrt{d})$, $d > 0$, то существует такая единица $u > 1$, что каждая единица имеет вид $\pm u^m$, $m \in \mathbf{Z}$.*

Доказательство. Согласно предложению 17.5.2, существуют положительные ненулевые целые числа x, y, для которых $x^2 - dy^2 = +1$. Таким образом, $x + \sqrt{d}y = u$ — единица в D, $u > 1$. Пусть M — некоторое фиксированное вещественное число, $M > u$. Согласно упр. 4 из гл. 12, существует лишь конечное число таких $\alpha \in D$, что $|\alpha| < M$, $|\alpha'| < M$, где α' — сопряженное к α. Если β — единица, причем $1 < \beta < M$, то $N(\beta) = \beta\beta' = \pm 1$. Если $\beta' = -1/\beta$, то $-M < -1/\beta < M$, а если $\beta' = 1/\beta$, то также $-M < 1/\beta < M$. Таким образом, существует лишь конечное число единиц β с $1 < \beta < M$, и имеется по крайней мере одна, и именно u. Пусть ε — наименьшая положительная единица, такая, что $\varepsilon > 1$. Если τ — какая-либо положительная единица, то существует единственное целое число s (не обязательно положительное), удовлетворяющее условию $\varepsilon^s \leqslant \tau < \varepsilon^{s+1}$. Тогда $1 \leqslant \tau\varepsilon^{-s} < \varepsilon$ и, так как $\tau\varepsilon^{-s}$ — единица, то $\tau\varepsilon^{-s} = 1$. Если τ отрицательна, то $-\tau$ положительна и $-\tau = \varepsilon^s$. Это завершает доказательство. □

Единственная единица ε, определенная в предложении 13.1.6, называется *фундаментальной единицей* поля $\mathbf{Q}(\sqrt{d})$. Множество $d > 0$, для которых норма единицы ε равна -1, до сих пор не найдено. Однако имеется много интересных результатов в этом направлении (см. [196], с. 124—126). Была высказана гипотеза, что если $d = p$, $p \equiv 1$ (4) и просто, и $\varepsilon = (u + v\sqrt{r})/2$, то $p \nmid v$ [86]. Вычислить фундаментальную единицу даже для малых дискриминантов может быть довольно трудно. Например, фундаментальная единица поля $\mathbf{Q}(\sqrt{94})$ равна $2143295 + 221064\sqrt{94}$.

Эти результаты о единицах являются частными случаями важной теоремы Дирихле о единицах, которая определяет структуру группы единиц в произвольном числовом поле. В этой теореме утверждается, что группа единиц по модулю подгруппы корней из единицы в поле будет конечно порожденной группой с $r + s - 1$ образующими, где r — число пар комплексно сопряженных корней, а s — число вещественных корней порождающего это поле многочлена. В случае квадратичных полей это число, очевидно, равно 0 или 1 в зависимости от того, будет поле мнимым или вещественным, что согласуется с приведенным выше результатом.

Что касается числа классов, то для квадратичных числовых полей имеется исключительно богатая теория. На самом деле существуют явные формулы, открытые Дирихле. Мы упомянем об одном особенно изящном частном случае. Предположим, что $q > 3$ — простое число и $q \equiv 3$ (4). Пусть $F = \mathbf{Q}(\sqrt{-q})$. Пусть V и R представляют суммы квадратичных невычетов и квадратич-

ных вычетов по модулю q соответственно среди чисел 1, 2, 3, ..., $q-1$. Тогда $h_F = (1/q)(V - R)$.

Например, пусть $q = 7$. Тогда $V = 3 + 5 + 6 = 14$ и $R = 1 + 2 + 4 = 7$. Поэтому $h_F = (14 - 7)/7 = 1$.

Для случая $d < 0$ Зигель доказал, что $\ln h_F / \ln |\delta_F|^{1/2} \to 1$ при $|\delta_F| \to \infty$. Отсюда следует, что существует лишь конечное число таких $d < 0$, для которых число классов поля $\mathbf{Q}(\sqrt{-d})$ меньше какой-либо фиксированной границы.

Гаусс высказал гипотезу о том, что единственными $d < 0$, для которых число классов поля $\mathbf{Q}(\sqrt{d})$ равно 1, являются $d = -1, -2, -3, -7, -11, -19, -43, -67$ и -163. Первое признанное всеми доказательство было получено Старком. По существу доказательство было дано ранее Хегнером, но из-за неясности изложения его доказательство считалось сначала неверным [1]).

Для положительных d Гаусс выдвинул гипотезу о том, что для бесконечно многих полей $\mathbf{Q}(\sqrt{d})$ число классов равно 1. Это, однако, остается открытой проблемой.

Красивая формула, определяющая число классов вещественного квадратичного поля с дискриминантом p, p — простое число сравнимое с 1 по модулю 4, такова: $\varepsilon^h = \prod (\sin(\pi j/p))^{-\chi(j)}$, где ε — фундаментальная единица, χ — символ Лежандра и произведение берется по числам $j = 1, \ldots, (p-1)/2$. Аналогичная формула имеет место для произвольного дискриминанта. Эти результаты и их доказательства см. в [9], гл. 5.

Мы закончим этот параграф упоминанием нескольких других результатов, доказательство которых лежит вне рамок элементарного подхода. Рассмотрим мнимое квадратичное поле с дискриминантом d. В таком случае число классов поля делится на 2^{t-1}, где t — число различных простых делителей d. Таким образом, число классов поля $\mathbf{Q}(\sqrt{-210})$ делится на 8. Оказывается, что это число классов в точности равно 8. Подобный результат имеет место и для вещественных квадратичных числовых полей.

Следующий, наиболее замечательный факт был открыт Хирцебрухом. Пусть p — какое-либо простое число, сравнимое с 3 по модулю 4, и предположим, что число классов поля $\mathbf{Q}(\sqrt{p})$

---

[1]) Другое доказательство было дано Бейкером (см. его обзор в [20*]). Он и Старк показали также, что из $h_F = 2$ вытекает, что $d < 10^{1030}$, $F = \mathbf{Q}(\sqrt{-d})$. Впоследствии эта оценка была усилена до $d \leqslant 427$. Наконец, в 1983 г. Гросс и Загир получили следующую оценку: $h_F \geqslant c(\varepsilon)(\log d)^{1-\varepsilon}$, где $c(\varepsilon) > 0$ — эффективно вычисляемая константа. В частности, из $h_F = 3$ следует, что $d < 10^{10^{600}}$ (предполагается, что на самом деле $d \leqslant 907$). Подробный обзор этих вопросов см. в [2*]. — *Прим. ред.*

равно единице. Тогда число классов мнимого квадратичного поля $\mathbf{Q}(\sqrt{-p})$ равно одной трети от знакочередующейся суммы $a_s - a_{s-1} + a_{s-2} - \cdots \pm a_1$, где в стандартных обозначениях $(a_0, \overline{a_1, a_2, \ldots, a_s})$ — разложение для $\sqrt{p}$ в непрерывную дробь (см. [73], гл. 7, и [22]). Например, число классов обоих полей $\mathbf{Q}(\sqrt{67})$ и $\mathbf{Q}(\sqrt{-67})$ равно единице, и

$$\sqrt{67} = (8, \overline{5, 2, 1, 1, 7, 1, 1, 2, 5, 16}).$$

§ 2. Круговые поля

Пусть m — положительное целое число и $\zeta_m = e^{2\pi i/m}$. Число ζ_m, как и все его степени, удовлетворяет уравнению $x^m - 1 = 0$. Таким образом, $x^m - 1 = (x-1)(x-\zeta_m)\ldots(x-\zeta_m^{m-1})$. Отсюда вытекает, что поле $F = \mathbf{Q}(\zeta_m)$ является полем разложения для многочлена $x^m - 1$. Следовательно, $F/\mathbf{Q}$ — нормальное расширение.

Мы называем $F = \mathbf{Q}(\zeta_m)$ *круговым полем корней степени m из единицы*. Первым начал его изучать Гаусс в связи с построением правильных многоугольников (см. гл. 9, § 11).

Предложение 13.2.1. *Пусть G — группа Галуа поля $F/\mathbf{Q}$. Существует такой мономорфизм $\theta : G \to U(\mathbf{Z}/m\mathbf{Z})$, что при любом $\sigma \in G$*

$$\sigma\zeta_m = \zeta_m^{\theta(\sigma)}.$$

Доказательство. Так как $\zeta_m^m = 1$, то $(\sigma\zeta_m)^m = 1$. Таким образом, $\sigma\zeta_m = \zeta_m^{\theta(\sigma)}$, где $\theta(\sigma)$ — некоторое целое число по модулю m. Если $\tau = \sigma^{-1}$, то $\zeta_m = \tau\sigma\zeta_m = \tau(\zeta_m^{\theta(\sigma)}) = \zeta_m^{\theta(\tau)\theta(\sigma)}$. Таким образом, $\theta(\tau)\theta(\sigma) = \overline{1}$ (где $\overline{1}$ — класс вычетов числа 1 в $\mathbf{Z}/m\mathbf{Z}$). Поэтому $\theta : G \to U(\mathbf{Z}/m\mathbf{Z})$. Нетрудно проверить, что θ — гомоморфизм. Наконец, если $\theta(\sigma) = \overline{1}$, то $\sigma\zeta_m = \zeta_m$, откуда следует что σ — единица в G, ибо ζ_m порождает F над $\mathbf{Q}$. □

Следствие. *$[\mathbf{Q}(\zeta_m) : \mathbf{Q}]$ делит $\varphi(m)$.*

Мы покажем далее, что на самом деле $[\mathbf{Q}(\zeta_m) : \mathbf{Q}] = \varphi(m)$.

Определение. Пусть $\Phi_m(x) = \prod_{(a,m)=1} (x - \zeta_m^a)$, где $1 \leqslant a < m$. Этот многочлен называется *m-м круговым многочленом*.

Его корнями будут в точности примитивные корни степени m из единицы, т. е. корни степени m из единицы, порядок которых равен m. Очевидно, что степень многочлена $\Phi_m(x)$ равна $\varphi(m)$.

Предложение 13.2.2. $x^m - 1 = \prod_{d \mid m} \Phi_d(x)$.

Доказательство. Имеем

$$x^m - 1 = \prod_{i=0}^{m-1} (x - \zeta_m^i) = \prod_{d \mid m} \prod_{(i,\, m) = d} (x - \zeta_m^i).$$

Мы утверждаем, что $\prod_{(i,\, m) = d} (x - \zeta_m^i) = \Phi_{m/d}(x)$. Отсюда будет следовать наше утверждение.

Если $(i, m) = d$, то положим $i = dj$. Имеем $\zeta_m^i = \zeta_m^{dj} = \zeta_{m/d}^j$. Кроме того, $(j, m/d) = 1$. Поэтому

$$\prod_{(i,\, m) = d} (x - \zeta_m^i) = \prod_{(j,\, m/d) = 1} (x - \zeta_{m/d}^j) = \Phi_{m/d}(x). \qquad \square$$

Следствие. $\Phi_m(x) \in \mathbf{Z}[x]$.

Доказательство. Мы применим индукцию по m. Имеем $\Phi_1(x) = x - 1$. Предположим, что следствие верно для целых чисел, меньших m. Согласно предложению 13.2.2, $\Phi_m(x) = (x^m - 1)/f(x)$, где $f(x)$ — приведенный многочлен, который по предположению индукции лежит в $\mathbf{Z}[x]$. Используя «деление столбиком», получаем, что $\Phi_m(x) \in \mathbf{Z}[x]$. $\square$

Независимое доказательство этого следствия получается так. Каждый элемент $\sigma \in G$ переставляет примитивные корни степени m из единицы. Таким образом, коэффициенты многочлена $\Phi_m(x)$ остаются на месте при действии элементов из G, а потому принадлежат $\mathbf{Q}$. Так как они, очевидно, являются целыми алгебраическими числами, то они должны лежать в $\mathbf{Z}$.

Начиная с этого места, мы введем следующие обозначения: $\zeta_m = \zeta$, $F = \mathbf{Q}(\zeta)$ и D — кольцо целых чисел в F.

Предложение 13.2.3. *Предположим, что p — рациональное простое число и $p \nmid m$. Пусть P — простой идеал в D, содержащий p. Тогда классы вычетов чисел $1, \zeta, \zeta^2, \ldots, \zeta^{m-1}$ в D/P все различны. Если f — степень идеала P, то $p^f \equiv 1\ (m)$.*

Доказательство. Пусть $\bar{w}$ обозначает класс вычетов числа $w \in D$ в D/P.

Разделим обе части равенства $x^m - 1 = \prod (x - \zeta^i)$ на $x - 1$. В результате получим

$$1 + x + \ldots + x^{m-1} = \prod_{i=1}^{m-1} (x - \zeta^i).$$

Положим в этом тождестве $x = 1$: $m = \prod (1 - \zeta^i)$, где $1 \leqslant i \leqslant m - 1$. Таким образом, $\overline{m} = \prod \overline{(1 - \zeta^i)}$. Так как $\overline{m} \neq \overline{0}$, отсюда следует, что $\bar{\zeta}^i \neq \overline{1}$ для $1 \leqslant i \leqslant m - 1$, а также $\bar{\zeta}^i \neq \bar{\zeta}^j$ для $0 \leqslant i < j \leqslant m - 1$.

Элементы $\{\bar{\zeta}^i \mid 0 \leqslant i \leqslant m - 1\}$ образуют подгруппу порядка m в мультипликативной группе поля D/P. Последняя группа имеет порядок $p^l - 1$. Поэтому $p^l \equiv 1 \ (m)$. □

Теорема 1. *m-й круговой многочлен $\Phi_m(x)$ неприводим в $\mathbf{Z}[x]$.*

Доказательство. Пусть $f(x) \in \mathbf{Z}[x]$ — приведенный неприводимый многочлен для ζ. Тот факт, что его коэффициенты лежат в $\mathbf{Z}$, следует из того, что ζ — целое алгебраическое число (упр. 16, гл. 6). При простом $p \nmid m$ мы покажем, что ζ^p также будет корнем многочлена $f(x)$. Если $a \in \mathbf{Z}$ и $(a, m) = 1$, то, разлагая a в произведение простых чисел, мы получим, что ζ^a будет корнем для $f(x)$. Таким образом, $\deg f(x) \geqslant \varphi(m)$. С другой стороны, так как $\Phi_m(\zeta) = 0$, $f(x)$ делит многочлен $\Phi_m(x)$, который имеет степень $\varphi(m)$. Отсюда будет следовать, что $f(x) = \Phi_m(x)$.

Пусть p — простое число, $p \nmid m$ и P — какой-либо простой идеал в D, содержащий p. Как обычно, $\bar{w}$ при $w \in D$ будет обозначать класс вычетов элемента w в D/P. Мы имеем $x^m - 1 = f(x)\, g(x)$ и $x^m - \overline{1} = \bar{f}(x)\, \bar{g}(x)$ в $\mathbf{Z}/p\mathbf{Z}[x]$. Согласно предыдущему предложению, $x^m - \overline{1}$ имеет различные корни в D/P. Отсюда следует, что $\bar{f}(x)$ и $\bar{g}(x)$ не имеют общих корней. Предположим, что $f(\zeta^p) \neq 0$. Тогда $g(\zeta^p) = 0$ и $\bar{g}(\bar{\zeta}^p) = \overline{0}$. Коэффициенты многочлена $\bar{g}(x)$ лежат в $\mathbf{Z}/p\mathbf{Z}$ и равны поэтому своим собственным p-м степеням. Отсюда получаем, что $\overline{0} = \bar{g}(\bar{\zeta}^p) = \bar{g}(\bar{\zeta})^p$, так что $\overline{0} = \bar{g}(\bar{\zeta})$. Отсюда вытекает, что $\bar{f}(\bar{\zeta}) \neq \overline{0}$, а это неверно, ибо $f(\zeta) = 0$. Следовательно, $f(\zeta^p) = 0$, как и утверждалось. □

Следствие 1. $[\mathbf{Q}(\zeta_m) : \mathbf{Q}] = \varphi(m)$.

Следствие 2. *Отображение θ из предложения 13.2.1 является изоморфизмом группы G на $U(\mathbf{Z}/m\mathbf{Z})$.*

Доказательство. Обе группы G и $U(\mathbf{Z}/m\mathbf{Z})$ имеют по $\varphi(m)$ элементов. Так как отображение θ взаимно однозначно, то оно должно быть эпиморфизмом. □

В силу следствия 2 для каждого $a \in \mathbf{Z}$, такого, что $(a, m) = 1$, существует такой элемент $\sigma_a \in G$, что $\sigma_a \zeta = \zeta^a$. Отображение $a \to \sigma_a$ индуцирует гомоморфизм из $U(\mathbf{Z}/m\mathbf{Z})$ в G, обратный к θ.

Для простого числа $p \nmid m$ мы хотим изучить более внимательно автоморфизм σ_p. Прежде чем приступить к этому, необходимо привести некоторые вспомогательные результаты.

Лемма 1. *Пусть $F/\mathbf{Q}$ — поле алгебраических чисел степени n. Пусть $D \subset F$ — кольцо целых чисел и $\alpha_1, \alpha_2, \ldots, \alpha_n \in D$ — базис поля $F/\mathbf{Q}$. Пусть $\Delta = \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ — дискриминант этого базиса. Тогда $\Delta D \subset \mathbf{Z}\alpha_1 + \mathbf{Z}\alpha_2 + \ldots + \mathbf{Z}\alpha_n$.*

Доказательство. Для $\omega \in D$ мы имеем $\omega = \sum r_i \alpha_i$ с $r_i \in \mathbf{Q}$. Умножим обе части этого равенства на α_j и возьмем след: $t(\omega\alpha_j) = \sum r_i t(\alpha_i\alpha_j)$. Элементы $t(\omega\alpha_j)$ и $t(\alpha_i\alpha_j)$ лежат в $\mathbf{Z}$, так как они являются следами целых алгебраических чисел. Используя правило Крамера для решения системы уравнений относительно r_i, мы видим, что каждое r_i есть целое число, деленное на Δ. Лемма доказана. □

Лемма 2. *Дискриминант $\Delta = \Delta(1, \zeta, \ldots, \zeta^{\varphi(m)-1})$ делит $m^{\varphi(m)}$.*

Доказательство. Продифференцировав обе части равенства $x^m - 1 = \Phi_m(x)\, g(x)$, получим

$$mx^{m-1} = \Phi_m'(x)\, g(x) + \Phi_m(x)\, g'(x).$$

Подставляя $x = \zeta$, получаем в результате $m\zeta^{m-1} = \Phi_m'(\zeta)\, g(\zeta)$. Возьмем теперь норму от обеих частей. Воспользовавшись предложением 12.1.4 и тем фактом, что $N(\zeta) = \pm 1$, получим $\pm m^{\varphi(m)} = \Delta N(g(\zeta))$. Заметим, что, согласно теореме 1, элементы $1, \zeta, \ldots, \zeta^{\varphi(m)-1}$ образуют базис для $\mathbf{Q}(\zeta)/\mathbf{Q}$, так что $\Delta(1, \zeta, \ldots, \zeta^{\varphi(m)-1}) \neq 0$.

Предложение 13.2.4. *Пусть $p \in \mathbf{Z}$ — такое простое число, что $p \nmid m$. Пусть w лежит в D, кольце целых чисел в $\mathbf{Q}(\zeta)$. Существует такой элемент $\sum a_i \zeta^i \in \mathbf{Z}[\zeta]$, что $w \equiv \sum a_i \zeta^i \ (p)$.*

Доказательство. Положим $\Delta = \Delta(1, \zeta, \ldots, \zeta^{\varphi(m)-1})$. В силу леммы 2 $p \nmid \Delta$. Таким образом, существует такое $\Delta' \in \mathbf{Z}$, что $\Delta'\Delta \equiv 1 \ (p)$. Следовательно, $w \equiv \Delta'\Delta w \ (p)$. В силу леммы 1 $\Delta w \in \mathbf{Z}[\zeta]$. Предложение доказано. □

Заметим, что на самом деле $D = \mathbf{Z}[\zeta]$, но это не так легко доказать для произвольного m. В случае когда m — степень простого числа, доказательство достаточно просто (см. предложение 13.2.10).

Следствие. *Пусть $p \nmid m$ и $n > 0$ таковы, что $p^n \equiv 1 \ (m)$. Тогда для $w \in D$ имеем $w^{p^n} \equiv w \ (p)$.*

Доказательство. Согласно предыдущему предложению, $w \equiv \sum a_i \zeta^i$ (p), где $a_i \in \mathbf{Z}$. Так как $a_i^p \equiv a_i$ (p), то должно выполняться сравнение $w^p \equiv \sum a_i \zeta^{pi}$ (p). Повторив это возведение в степень n раз и воспользовавшись тем, что из $p^n \equiv 1$ (m) следует $\zeta^{p^n} = \zeta$, получаем доказываемый результат. □

Предложение 13.2.5. *Если p, $p \nmid m$, — простое число, то каждый идеал P в D, содержащий p, неразветвлен.*

Доказательство. Предположим, что P разветвлен. Тогда $(p) \subset P^2$. Пусть w — какой-либо элемент из P, не принадлежащий P^2. Согласно предыдущему следствию, $w^{p^n} \equiv w$ (p), а потому $w^{p^n} \equiv w$ (P^2). Так как $p^n \geqslant 2$, отсюда следует, что $w \in P^2$, т. е. мы пришли к противоречию. □

Мы увидим далее, что «почти» верно обращение этого предложения. См. предложение 13.2.8.

Напомним, что если p, $p \nmid m$, — простое число, то автоморфизм σ_p переводит ζ в ζ^p.

Предложение 13.2.6. *Для всех $w \in D$ имеем $\sigma_p w \equiv w^p$ (p).*

Доказательство. Согласно предложению 13.2.4, $w \equiv \sum a_i \zeta^i$ (p). Применив σ_p к обеим частям этого сравнения, получим $\sigma_p w \equiv \sum a_i \zeta^{pi}$ (p). Так как $a_i \in \mathbf{Z}$, то $\sum a_i \zeta^{pi} \equiv \sum a_i^p \zeta^{pi}$ $(p) \equiv \left(\sum a_i \zeta^i\right)^p$ (p). Таким образом, $\sigma_p w \equiv w^p$ (p), что и утверждалось. □

Следствие. *Пусть P — какой-либо простой идеал, в D, содержащий p. Тогда $\sigma_p P = P$.*

Доказательство. Для $w \in P$ имеем $\sigma_p w \equiv w^p$ $(P) \equiv 0$ (P), а потому $\sigma_p P \subset P$. Так как $\sigma_p P$ — максимальный идеал, выполняется равенство. □

Теорема 2. *Пусть p — некоторое простое число, $p \nmid m$. Пусть f — наименьшее положительное целое число, для которого $p^f \equiv 1$ (m). Тогда в $D \subset \mathbf{Q}(\zeta)$*

$$(p) = P_1 P_2 \ldots P_g,$$

где каждый идеал P_i имеет степень f и $g = \varphi(m)/f$.

Доказательство. Заметим сначала, что, как следует непосредственно из определения, f равно порядку автоморфизма σ_p.

Далее, $p^{f_1} = |D/P_1|$, где f_1 — степень идеала P_1. Так как D/P_1 — конечное поле, то $w^{p^{f_1}} \equiv w\ (P_1)$ для всех $w \in D$ и f_1 — наименьшее положительное целое число с этим свойством.

Согласно последнему предложению, $w \equiv \sigma_p^f(w)\ (P_1) \equiv w^{p^f}\ (P_1)$ для всех $w \in D$. Отсюда получаем, что $f_1 \leqslant f$.

С другой стороны, из $\zeta^{p^{f_1}} \equiv \zeta\ (P_1)$ следует $\zeta^{p^{f_1}} = \zeta$ в силу предложения 13.2.3. Таким образом, $p^{f_1} \equiv 1\ (m)$, откуда вытекает, что $f \leqslant f_1$.

Мы убедились, что $f = f_1$ равно степени идеала P_1. Все идеалы P имеют степень f. В силу предложения 13.2.5 все идеалы P_i неразветвлены. Пользуясь соотношением $efg = \varphi(m)$, получаем, что $g = \varphi(m)/f$. □

Следствие. *В обозначениях теоремы 2 пусть P — один из идеалов P_i. Положим $G(P) = \{\sigma \in G \mid \sigma P = P\}$. Тогда $G(P)$ — циклическая группа, порожденная элементом σ_p.*

Доказательство. В силу следствия предложения 13.2.6 $\sigma_p \in G(P)$. Пусть $\langle\sigma_p\rangle$ — циклическая группа, порожденная элементом σ_p. Тогда $\langle\sigma_p\rangle \subset G(P)$. Согласно предложению 12.3.3, $g \mid G(P)\mid = \varphi(m)$. Таким образом, $|G(P)| = \varphi(m)/g = f = |\langle\sigma_p\rangle|$ и следствие доказано. □

Теорема 2 весьма удовлетворительно описывает разложение простых чисел, не делящих m. Можно получить также закон разложения для простых чисел, делящих m. Мы ограничимся рассмотрением следующего важного частного случая.

Предложение 13.2.7. *Пусть l — какое-либо простое число в $\mathbf{Z}$. Тогда l полностью разветвляется в $\mathbf{Q}(\zeta_l)$. Более точно, пусть $L = (1 - \zeta_l)$. Тогда L будет простым идеалом и $(l) = L^{l-1}$. Кроме того, L имеет степень 1.*

Доказательство. Как и в доказательстве предложения 13.2.3, $l = \prod(1 - \zeta_l^i)$, где произведение берется по $1 \leqslant i \leqslant l - 1$. Положим $u_i = (1 - \zeta^i)/(1 - \zeta) = 1 + \zeta + \ldots + \zeta^{i-1}$. Мы утверждаем, что u_i — единица. Так как $l \nmid i$, существует такое $j \in \mathbf{Z}$, что $ij \equiv 1\ (l)$. Таким образом, $u_i^{-1} = (1 - \zeta)/(1 - \zeta^i) = (1 - \zeta^{ij})/(1 - \zeta^i) = 1 + \zeta^i + \ldots + (\zeta^i)^{j-1}$ — целое алгебраическое число, что и доказывает утверждение.

Отсюда следует, что $l = \prod(1 - \zeta^i) = (1 - \zeta)^{l-1} \prod u_i$, а потому $(l) = L^{l-1}$. Используя соотношение $efg = \varphi(l) = l - 1$, мы видим, что L должно быть простым идеалом, $e = l - 1$, $g = 1$ и $f = 1$. □

Предложение 13.2.8. *Пусть P — какой-либо простой идеал в $\mathbf{Q}(\zeta_m)$, и положим $P \cap \mathbf{Z} = p\mathbf{Z}$. Если p нечетно, то P разветвлено в том и только том случае, когда $p \mid m$. Если $p = 2$, то P разветвлено тогда и только тогда, когда $4 \mid m$.*

Доказательство. В силу предложения 13.2.5 из $p \nmid m$ следует неразветвленность P.

Предположим, что p нечетно и $p \mid m$. Тогда $\mathbf{Q}(\zeta_p) \subset \mathbf{Q}(\zeta_m)$. Пусть D_p и D_m — кольца целых чисел в $\mathbf{Q}(\zeta_p)$ и $\mathbf{Q}(\zeta_m)$ соответственно. По предыдущему предложению $pD_p = (1 - \zeta_p)^{p-1}$. Запишем $(1 - \zeta_p) D_m = P_1 P_2 \ldots P_t$, где P_i суть не обязательно различные простые идеалы в D_m. Тогда $pD_m = (P_1 P_2 \ldots P_t)^{p-1}$. Так как $p - 1 > 1$, то все простые идеалы в D_m, содержащие p, будут разветвлены.

Предположим теперь, что $p = 2$. Если $2 \mid m$, но $4 \nmid m$, то $m = 2m_0$ с нечетным m_0. В этом случае $-\zeta_{m_0}$ — примитивный корень степени m из единицы, так что $\mathbf{Q}(\zeta_m) = \mathbf{Q}(\zeta_{m_0})$. Так как $2 \nmid m_0$, то P неразветвлено.

Предположим, наконец, что $p = 2$ и $4 \mid m$. Тогда $\zeta_4 = \sqrt{-1} = i \in \mathbf{Q}(\zeta_m)$. Так как $(1 - i)^2 = -2i$, то $2D_m = ((1 - i) D_m)^2$, откуда следует, как и прежде, что все простые идеалы в D_m, содержащие 2, разветвлены. □

Предположим, что p — какое-либо простое число и $p \nmid m$. Для дальнейшего использования (в следующей главе) нам нужно знать, как p разлагается на простые идеалы в поле $\mathbf{Q}(\zeta_p, \zeta_m)$.

Лемма 3. *Если $(m, n) = 1$, то $\mathbf{Q}(\zeta_m, \zeta_n) = \mathbf{Q}(\zeta_{mn})$.*

Доказательство. Так как $\zeta_{mn}^m = \zeta_n$ и $\zeta_{mn}^n = \zeta_m$, то $\mathbf{Q}(\zeta_m, \zeta_n) \subset \mathbf{Q}(\zeta_{mn})$.

С другой стороны, так как $(m, n) = 1$, то существуют такие целые числа u и v, что $um + vn = 1$. Следовательно,

$$\zeta_{mn} = \zeta_{mn}^{um} \zeta_{mn}^{vn} = \zeta_n^u \zeta_m^v \in \mathbf{Q}(\zeta_m, \zeta_n). \qquad \square$$

Предложение 13.2.9. *Пусть p — какое-либо простое число, $p \nmid m$, и D — кольцо целых чисел в $\mathbf{Q}(\zeta_p, \zeta_m)$. Тогда*

$$pD = (P_1 P_2 \ldots P_g)^{p-1},$$

где P_i — различные простые идеалы степени f и $g = \varphi(m)/f$. Целое число f — наименьшее положительное целое число, для которого $p^f \equiv 1 \ (m)$.

Доказательство. Так как $\mathbf{Q}(\zeta_p) \subset \mathbf{Q}(\zeta_p, \zeta_m)$, то мы видим, что, как и в доказательстве последнего предложения, все индексы ветвления простых идеалов в D, содержащих p, делятся на $p - 1$.

Таким образом,

$$pD = (P_1P_2 \dots P_g)^{e'(p-1)}, \qquad (*)$$

где P_i — различные простые идеалы степени, скажем, f' и $e' \geqslant 1$ — некоторое целое число.

Пусть D_m — кольцо целых чисел в $\mathbf{Q}(\zeta_m)$. В силу теоремы 2

$$pD_m = \tilde{P}_1\tilde{P}_2 \dots \tilde{P}_g,$$

где $\tilde{P}_i$ — простые идеалы в D_m степени f и $g = \varphi(m)/f$.

Рассматривая разложение на простые идеалы для $\tilde{P}_iD$ и сравнивая его с равенством (*), мы видим, что $f' \geqslant f$ и $g' \geqslant g$.

Из равенства (*) и леммы 3 получаем, что

$$(p-1)\varphi(m) = \varphi(pm) = e'(p-1)f'g' \geqslant e'(p-1)f\frac{\varphi(m)}{f}.$$

Отсюда следует, что $\varphi(m) \geqslant e'\varphi(m)$. Таким образом, $e' = 1$, и все неравенства превращаются в равенства, т. е. $f' = f$ и $g' = g = \varphi(m)/f$. Это завершает доказательство. □

Мы закончим этот параграф доказательством того, что $D = \mathbf{Z}[\zeta_l]$, где l — простое число. Этот результат верен и в случае, когда l не простое, но доказательство более трудное (см., например, с. 265—268 в [207]). Случай с простым l понадобится нам в гл. 17, где будет обсуждаться частный случай гипотезы Ферма.

Предложение 13.2.10. *Если l — простое число, то $D = \mathbf{Z}[\zeta_l]$.*

Доказательство. Ясно, что $\mathbf{Z}[\zeta_l] \subset D$. Если $\alpha \in D$, то существуют такие рациональные числа $a_0, a_1, \dots, a_{l-2}$, что $\alpha = a_0 + a_1\zeta + \dots + a_{l-2}\zeta^{l-2}$. Прежде всего мы покажем, что $la_i \in \mathbf{Z}$, $i = 0, \dots, l-2$. Действительно, если tr обозначает отображение следа из $\mathbf{Q}(\zeta)$ в $\mathbf{Q}$, то, как нетрудно вычислить, воспользовавшись, например, следствием 1 теоремы 1, $\operatorname{tr}\zeta^i = -1$ при $l \nmid j$. Таким образом, мы видим, что $\operatorname{tr}(\alpha\zeta^{-s}) = -a_0 - a_1 - \dots - a_{s-1} + (l-1)a_s - a_{s+1} - \dots - a_{l-2}$. Поэтому $\operatorname{tr}(\alpha\zeta^{-s} - \alpha\zeta) = la_s$, $s = 0, \dots, l-2$. Так как $\alpha\zeta^{-s} - \alpha\zeta \in D$, отсюда следует, что $la_s \in \mathbf{Z}$. Если $\lambda = 1 - \zeta$, то по предложению 13.2.7 имеем $(\lambda)^{l-1} = (l)$. В силу того, что было изложено выше, существуют такие $b_0, \dots, b_{l-2}$ в $\mathbf{Z}$, что $l\alpha = b_0 + b_1\lambda + \dots + b_{l-2}\lambda^{l-2}$. Таким образом, $\lambda \mid b_0$ и взятие норм показывает, что $l \mid b_0$. Значит, $\lambda^{l-1} \mid b_0$ и редукция по модулю λ^2 дает $\lambda^2 \mid b_1\lambda$, так что $\lambda \mid b_1$. Опять это означает, что $l \mid b_1$. Ясно, что последовательная редукция по модулю все более высоких степеней λ приводит к тому, что $l \mid b_j$, $j = 0, \dots, l-2$, и деление на l затем показывает, что $\alpha \in \mathbf{Z}[\zeta_l]$. □

§ 3. Снова квадратичный закон взаимности

В качестве приложения теории, развитой в этой главе, мы приведем еще одно доказательство квадратичного закона взаимности. Идея этого доказательства восходит по существу к Кронекеру.

Пусть p — какое-либо нечетное простое число. Рассмотрим поле $\mathbf{Q}(\zeta_p)$. Мы утверждаем, что это поле содержит квадратный корень из $(-1)^{(p-1)/2}p = p^*$. Это следует из предложения 6.3.2. Однако чтобы сделать наше теперешнее рассмотрение независимым от теории сумм Гаусса, мы дадим прямое доказательство, исходя из соотношения

$$p = \prod_{i=1}^{p-1}(1 - \zeta^i).$$

Скомбинируем члены, соответствующие i и $p - i$, следующим образом:

$$(1 - \zeta^i)(1 - \zeta^{p-i}) = (1 - \zeta^i)(1 - \zeta^{-i}) = -\zeta^{-i}(1 - \zeta^i)^2.$$

Итак,

$$p = (-1)^{(p-1)/2}\zeta^b \prod_{i=1}^{(p-1)/2}(1 - \zeta^i)^2, \text{ где } b = -1 - 2 - \ldots - \frac{(p-1)}{2}.$$

Пусть $c \in \mathbf{Z}$ таково, что $2c \equiv 1\ (p)$. Тогда $\zeta^b = (\zeta^{bc})^2$. Отсюда следует, что p^* является квадратом в $\mathbf{Q}(\zeta)$, как и утверждалось. Пусть $\tau^2 = p^*$.

Предположим теперь, что q — нечетное простое число и $q \neq p$. Рассмотрим автоморфизм σ_q. Тогда $\sigma_q\tau = \pm\tau$, причем знак плюс берется в том и только том случае, когда σ_q принадлежит группе Галуа поля $\mathbf{Q}(\zeta)/\mathbf{Q}(\tau)$. Так как группа Галуа G поля $\mathbf{Q}(\zeta)/\mathbf{Q}$ изоморфно отображается посредством φ на $U(\mathbf{Z}/p\mathbf{Z})$ и последняя группа циклическая порядка $p - 1$, то мы видим, что $\sigma_q\tau = \tau$ тогда и только тогда, когда σ_q — квадрат в G, а последнее имеет место, если и только если q — квадрат в $U(\mathbf{Z}/p\mathbf{Z})$. Другими словами,

$$\sigma_q\tau = \left(\frac{q}{p}\right)\tau.$$

Пусть Q — какой-либо простой идеал в $D \subset \mathbf{Q}(\zeta)$, содержащий q. По предложению 13.2.6

$$\sigma_q\tau \equiv \tau^q\ (Q).$$

Таким образом, $(q/p)\tau \equiv \tau^q\ (Q)$, откуда следует, что

$$(p^*/q) \equiv p^{*(q-1)/2}\ (Q) = \tau^{q-1} \equiv (q/p)\ (Q).$$

Последнее сравнение означает, что $(p^*/q) = (q/p)$, так как Q не содержит 2.

Можно было бы подумать, что это доказательство, каким бы приятным оно ни было, намного сложнее, чем прежние доказательства, а поэтому мало что добавляет к предыдущему. Но дело обстоит не так, потому что использованные при этом идеи дают ключ к изучению высших законов взаимности.

Замечания

Введение в арифметику квадратичных числовых полей имеется в книге «Введение в теорию алгебраических чисел» Зоммера (Sommer J. Introduction à la Théorie des Nombres Algebrique. — Paris: Hermann, 1911). Эта книга основана на лекциях Гильберта в 1897—1898 гг. См. также [111], [84] и [73] [1]).

Как упоминалось ранее, были найдены все мнимые квадратичные поля, кольца целых чисел которых являются областями с однозначным разложением на множители. Были также найдены мнимые квадратичные поля с числом классов два. Таких полей имеется 18, причем поле с наименьшим дискриминантом есть $\mathbf{Q}(\sqrt{-427})$ [2]).

В случае круговых полей Мэсли показал, что если m — положительное целое число, $m \not\equiv 2$ (4), то существует точно 29 значений m, для которых число классов поля $\mathbf{Q}(\zeta_m)$ равно 1. Кроме того, круговые поля $\mathbf{Q}(\zeta_p)$ с числом классов 1 задаются значениями $p = 3, 5, 7, 11, 13, 17, 19$; это результат Утиды и Монтгомери. Детали см. в обзорах [184], [185].

Для более полного знакомства с арифметикой квадратичных и круговых полей читателю следует обратиться к [9].

В § 3 мы видели, что $\mathbf{Q}(\sqrt{(-1)^{(p-1)/2}p})$ — подполе поля $\mathbf{Q}(\zeta_p)$. Более общим образом, согласно теореме Кронекера и Вебера, любое поле алгебраических чисел, которое нормально и имеет абелеву группу Галуа, будет подполем поля $\mathbf{Q}(\zeta_m)$ при некотором m. Доказательство этой трудной теоремы см. в [207], [13].

Упражнения

1. Показать, что поле алгебраических чисел нечетной степени не может содержать примитивный корень n-й степени из единицы при $n > 2$.

2. Пусть F — вещественное квадратичное поле. Показать, что если F содержит элемент с нормой -1, то любое простое число p, $p \equiv 3$ (4), неразветвлено.

3. Доказать, что если F — такое поле алгебраических чисел, что $e^{2\pi i/n} \in F$ при некотором $n \geqslant 3$, то норма любого ненулевого элемента из F положительна

---

[1]) На русском языке имеются изложения [9], [44] и [22*]. — *Прим. ред.*

[2]) См. примечание редактора к § 1. — *Прим. ред.*

4. Найти фундаментальные единицы для $\mathbf{Q}(\sqrt{5})$, $\mathbf{Q}(\sqrt{15})$, $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{3})$, $\mathbf{Q}(\sqrt{624})$.

5. Показать, что квадратичное числовое поле не может содержать $\sqrt{p}$ и $\sqrt{q}$ для двух различных простых чисел p и q.

6. Перечислить подполя поля $\mathbf{Q}(\zeta_8)$.

7. Пусть F — вещественное квадратичное поле. Показать, что в F существуют целые алгебраические числа, произвольно близкие к 1 и произвольно удаленные.

8. Показать, что число классов поля $\mathbf{Q}(\sqrt{10})$ не равно 1.

9. Пусть p — нечетное простое число, и рассмотрим $\mathbf{Q}(\zeta_p)$.

(a) Показать, что $N(1+\zeta) = 1$, где N обозначает норменное отображение из $\mathbf{Q}(\zeta_p)$ в $\mathbf{Q}$.

(b) Показать, что $\prod(1+\zeta^s) = A$, где произведение берется по квадратам по модулю p, лежит в $\mathbf{Q}(\sqrt{p})$.

(c) Если $p \equiv 1$ (4), то показать, что $A = (t + u\sqrt{p})/2$, где $t \equiv u$ (2).

(d) Из (a) сделать вывод, что $((t^2 - pu^2)/4)^{(p-1)/2} = +1$, так что

(e) $t^2 - pu^2 = \pm 4$.

(f) Показать, что $A \neq -1$, доказав, что $A > 0$ (ср. упр. 3).

Пусть теперь $p \equiv 5$ (8).

(g) Показать, что $A \neq 1$, рассматривая многочлен $\prod_S (1+x^s) - 1$, $s = 1^2, 2^2, \ldots, ((p-1)/2)^2$. (См. также упр. 9 гл. 16.) Это упражнение извлечено из [145].

10. Для какого d поле $\mathbf{Q}(\sqrt{d})$ имеет целый базис вида α, α', где α' — сопряженный элемент к α?

11. Показать, что $-(\zeta^3 + \zeta^2)$ — единица в $\mathbf{Q}(\zeta)$, $\zeta = e^{2\pi i/5}$. Какова связь между этой единицей и единицами в $\mathbf{Q}(\sqrt{5})$?

12. Показать, что $\sin(\pi j/p)/\sin(\pi/p)$ — единица в $\mathbf{Q}(\zeta_p)$, $1 \leqslant j \leqslant p-1$.

13. Показать, что если $p \equiv 1$ (4), p — простое число, то кольцо целых чисел в $\mathbf{Q}(\zeta_p)$ всегда содержит бесконечное число единиц.

14. Пусть p — какое-нибудь простое число. Показать, что дискриминант Δ поля $\mathbf{Q}(\zeta_p)$ равен $\prod_{i<j}(\zeta^i - \zeta^j)^2$, $1 \leqslant i,\ j \leqslant p-1$.

15. В обозначениях упр. 14 показать, что

(a) $p\zeta^{-j}/(1-\zeta^j) = \prod(\zeta^j - \zeta^i)$, причем произведение берется по всем $i \neq j$, $1 \leqslant i,\ j \leqslant p-1$.

(b) Перемножая по всем $j = 1, 2, \ldots, p-1$, получить, что $\Delta = (-1)^{(p-1)/2} p^{p-2}$.

16. Используя предложение 13.2.8, показать, что $i \notin \mathbf{Q}(\zeta_p)$, где p нечетно.

17. Воспользовавшись предложениями 13.2.7 и 13.2.8, показать, что $\zeta_q \notin \mathbf{Q}(\zeta_p)$, если p и q — нечетные простые числа и $p \neq q$.

18. Показать, что если p — простое число, сравнимое с 3 по модулю 4, то $\mathbf{Q}(\sqrt{p})$ содержится в круговом поле $\mathbf{Q}(\zeta_{4p})$.

19. Показать, что любое квадратичное поле содержится в некотором круговом поле.

20. Показать, что фундаментальной единицей вещественного квадратичного поля $\mathbf{Q}(\sqrt{10})$ будет $3 + \sqrt{10}$ и, воспользовавшись формулой из основного текста, определить число классов этого поля.

21. Пусть $a \in \mathbf{Z}$, a — не квадрат, $a \equiv 0$ (4) или $a \equiv 1$ (4). Определим символ Кронекера χ_a следующим образом. Если $p \mid a$, то $\chi_a(p) = 0$. Если $p \nmid a$ — нечетное простое число, то $\chi_a(p) = (a/p)$, символ Лежандра; $\chi_a(2) = 1$ при $a \equiv$

$\equiv 1$ (8); $\chi_a(2) = -1$ при $a \equiv 5$ (8). Наконец, $\chi_a(b) = \prod_{i=1}^{t} \chi_a(p_i)$ при $\pm b = p_1 \dots p_t$. Показать, что

(a) χ_a совпадает с символом Якоби при нечетном b;

(b) если $b > 0$, $(a, b) = 1$, $a = 2^t c$ с нечетным c, то $\chi_a(b) = \chi_2(b)^t \chi_b(c) \cdot (-1)^{((c-1)/2)((b-1)/2)}$;

(c) $\chi_a(x) = \chi_a(y)$ при $x \equiv y$ (a).

22. Пусть K — некоторое квадратичное поле с дискриминантом d и χ_d — символ Кронекера. Показать, что если p — *любое* простое число, то

(a) p полностью разлагается в K тогда и только тогда, когда $\chi_d(p) = 1$;

(b) p остается простым тогда и только тогда, когда $\chi_d(p) = -1$;

(c) p разветвляется тогда и только тогда, когда $\chi_d(p) = 0$.

23. Используя таблицу в [73], с. 340, вместе с таблицами из [9], с. 472—476, проверить формулу Хирцебруха, приведенную в конце § 1, для простых чисел 7, 19, 23, 31, 43, 47, 67, 83. Кроме того, использовать формулу Дирихле для вычисления числа классов некоторых мнимых квадратичных полей. Показать, что $\mathbf{Q}(\sqrt{91})$ не является областью главных идеалов, исходя из того что число классов поля $\mathbf{Q}(\sqrt{-91})$ равно 2.

24. Пусть K — поле корней степени p из единицы, p — нечетное простое число. Не используя сумм Гаусса, показать, что единственное квадратичное подполе поля K имеет дискриминант $(-1)^{(p-1)/2}p$.

25. В ситуации предыдущего упражнения пусть f — порядок числа q по модулю p, причем q — нечетное простое число, отличное от p. Если E обозначает квадратичное подполе поля K, то показать, что q полностью разлагается в E в том и только том случае, когда E содержится в подполе D степени $(p-1)/f$. Кроме того, показать, что это будет иметь место, если и только если q — квадрат по модулю p. Используя предыдущее упражнение, получить новое доказательство квадратичного закона взаимности.

26. Подсчитать число доказательств квадратичного закона взаимности, приведенных до сих пор в этой книге, и придумать еще одно.

27. Показать, что не существует простых чисел, которые оставались бы простыми в $\mathbf{Q}(\zeta_8)$. Можете ли Вы этот результат обобщить?

Глава 14

СООТНОШЕНИЕ ШТИКЕЛЬБЕРГЕРА И ЗАКОН ВЗАИМНОСТИ ЭЙЗЕНШТЕЙНА

Изложив основные свойства круговых полей, мы докажем теперь две красивые и важные теоремы, которые играют фундаментальную роль в дальнейшем развитии теории этих полей.

Закон взаимности Эйзенштейна обобщает некоторые наши прежние результаты по квадратичному и кубическому законам взаимности. Он лежит на полпути между этими частными случаями и более общими законами взаимности, которые исследовались Куммером и Гильбертом, были впервые доказаны Фуртвенглером и затем в полной общности Артином и Хассе. В последнем параграфе этой главы мы приведем два интересных приложения результата Эйзенштейна. Первое относится к последней теореме Ферма, а второе — к теории степенных вычетов.

Соотношение Штикельбергера является базисом для доказательства закона взаимности Эйзенштейна, которое мы приводим. В последние годы теория круговых полей значительно продвинулась вперед благодаря, главным образом, усилиям Ивасавы. В его работе соотношение Штикельбергера занимает центральное место. Оно оказалось важным также в арифметической алгебраической геометрии.

§ 1. Норма идеала

Нам понадобится несколько дополнительных результатов из общей теории полей алгебраических чисел.

Пусть $K/\mathbf{Q}$ — некоторое поле алгебраических чисел, D — кольцо целых чисел в K и A — какой-либо идеал. Определим $N(A)$, норму идеала A, как число элементов в D/A. Мы продолжаем предполагать, что рассматриваемые идеалы ненулевые.

Предложение 14.1.1. *Если A, $B \subset D$ — идеалы, то $N(AB) = N(A)\,N(B)$.*

Доказательство. Если A и B взаимно просты, то $D/AB \approx D/A \oplus D/B$, так что в этом случае утверждение очевидно.

Пусть $A = P_1^{a_1}P_2^{a_2} \ldots P_t^{a_t}$ — разложение идеала A на простые идеалы. Мы утверждаем, что $N(A) = (N(P_1))^{a_1}(N(P_2))^{a_2} \ldots$

$\ldots (N(P_t))^{a_t}$. Учитывая уже сказанное, достаточно доказать, что $N(P^a) = (N(P))^a$ для любого простого идеала P. Это, однако, простая переформулировка предложения 12.3.2.

Далее, разложим в общем случае A и B в произведение простых идеалов, перемножим эти разложения, применим сформулированный выше результат и перегруппируем члены. Это дает доказываемый результат. □

Предложение 14.1.2. *Предположим, что K $\mathbf{Q}$ — нормальное расширение с группой Галуа G. Тогда*

$$\prod_{\sigma \in G} \sigma(A) = (N(A)).$$

Доказательство. Так как обе части равенства мультипликативны по A, достаточно доказать результат для простого идеала P.

Пусть $P_1, P_2, \ldots, P_g$ — различные простые идеалы в множестве $\{\sigma(P) \mid \sigma \in G\}$. Тогда $|G| = g|G(P)|$, где $G(P) = \{\sigma \in G \mid \sigma(P) = P\}$. Так как $efg = n = |K : \mathbf{Q}| = |G|$, то $|G(P)| = ef$. Таким образом, воспользовавшись предложением 12.3.3 и теоремой 3′ из гл. 12, получаем

$$\prod_{\sigma \in G} \sigma(P) = (P_1 P_2 \ldots P_g)^{ef} = (p)^f = (p^f), \text{ где } P_i \cap \mathbf{Z} = p\mathbf{Z}.$$

Так как $N(P) = |D/P| = p^f$, это завершает доказательство. □

Предложение 14.1.3. *Пусть K $\mathbf{Q}$ — нормальное расширение с группой Галуа G. Пусть $\alpha \in D$ и $A = (\alpha)$ — главный идеал, порожденный элементом α. Пусть $N(\alpha)$ — норма элемента α. Тогда $N(A) = |N(\alpha)|$.*

Доказательство. Имеем $(N(A)) = \prod \sigma(A) \prod \sigma((\alpha)) = \prod(\sigma\alpha) = (\prod \sigma(\alpha)) = (N(\alpha))$. Таким образом, числа $N(A)$ и $N(\alpha)$ отличаются на единицу. Так как оба они лежат в $\mathbf{Z}$, они могут отличаться лишь знаком. Поскольку $N(A)$ по определению положительно, то $N(A) = |N(\alpha)|$, что и утверждалось. □

Заметим, что это предложение остается верным и в случае, когда $K/\mathbf{Q}$ не является нормальным расширением. Доказательство в общем случае несколько более сложное.

§ 2. Символ степенного вычета

Пусть m — некоторое положительное целое число и D_m обозначает кольцо целых чисел в $\mathbf{Q}(\zeta_m)$. Пусть P — какой-либо простой идеал в D_m, не содержащий m. Положим $q = N(P) = |D_m/P|$. В

силу предложения 13.2.3 мы знаем что классы смежности элементов $1, \zeta_m, \ldots, \zeta_m^{m-1}$ различны и что $q \equiv 1\ (m)$.

Предложение 14.2.1. *Пусть $\alpha \in D_m$, $\alpha \notin P$. Существует такое целое число i, единственное по модулю m, что*

$$\alpha^{(q-1)/m} \equiv \zeta_m^i\ (P).$$

Доказательство. Так как мультипликативная группа поля D_m/P имеет $q-1$ элементов, то $\alpha^{q-1} \equiv 1\ (P)$. Таким образом,

$$\prod_{i=0}^{m-1} (\alpha^{(q-1)/m} - \zeta_m^i) \equiv 0\ (P).$$

Поскольку P — простой идеал, существует такое целое число i, $0 \leqslant i < m$, что $\alpha^{(q-1)/m} \equiv \zeta_m^i\ (P)$. Если $i \not\equiv j\ (m)$, то $\zeta_m^i \not\equiv \zeta_m^j\ (P)$, так что i единственно по модулю m. □

Определение. Для $\alpha \in D_m$ и простого идеала P, не содержащего m, определим символ m-степенного вычета $(\alpha/P)_m$ следующим образом:

(a) $(\alpha/P)_m = 0$, если $\alpha \in P$;

(b) если $\alpha \notin P$, то $(\alpha/P)_m$ есть единственный корень степени m из единицы, для которого $\alpha^{(NP-1)/m} \equiv (\alpha/P)_m\ (P)$.

Предложение 14.2.2.

(a) $(\alpha/P)_m = 1$ *тогда и только тогда, когда* $x^m \equiv \alpha\ (P)$ *разрешимо в* D_m.

(b) $\alpha^{(NP-1)/m} \equiv (\alpha/P)_m\ (P)$ *для всех* $\alpha \in D_m$.

(c) $(\alpha\beta/P)_m = (\alpha/P)_m\,(\beta/P)_m$.

(d) *Если* $\alpha \equiv \beta\ (P)$, *то* $(\alpha/P)_m = (\beta/P)_m$.

Доказательство. Поскольку этот результат был ранее доказан для $m = 2$, 3, и 4, мы можем с уверенностью предоставить восстановление деталей читателю. □

Следствие. *Предположим, что P — какой-либо простой идеал, не содержащий m. Тогда*

$$\left(\frac{\zeta_m}{P}\right)_m = \zeta_m^{(NP-1)/m}.$$

Доказательство. Из п. (b) предложения 14.2.2 следует, что обе части выписанного равенства сравнимы по модулю P. Поскольку обе они — корни степени m из единицы и $m \notin P$, отсюда вытекает, что они равны. □

Имеет смысл расширить определение символа $(\alpha/P)_m$ так, чтобы $(\alpha/\beta)_m$ было определено при β, взаимно простом с m. Это делается следующим образом.

Определение. Предположим, что $A \subset D_m$ — идеал, взаимно простой с m. Пусть $A = P_1P_2 \dots P_n$ — разложение A на простые идеалы. Для $\alpha \in D_m$ полагаем

$$(\alpha/A)_m = \prod_i (\alpha/P_i)_m.$$

Если $\beta \in D_m$ и β взаимно просто с m, то положим $(\alpha/\beta)_m = (\alpha/(\beta))_m$.

Предложение 14.2.3. *Предположим, что A и B — взаимно простые с (m) идеалы. Тогда*
(a) $(\alpha\beta/A)_m = (\alpha/A)_m (\beta/A)_m$;
(b) $(\alpha/AB)_m = (\alpha/A)_m (\alpha/B)_m$;
(c) *если α взаимно просто с A и $x^m \equiv \alpha \ (A)$ разрешимо в D_m, то $(\alpha/A)_m = 1$.*

Доказательство. Все три утверждения доказываются непосредственно с использованием последнего предложения и данного выше определения. Заметим, что обращение п. (c) неверно. □

Нам следует посмотреть, как ведет себя символ $(\alpha/A)_m$ относительно автоморфизмов группы Галуа G поля $\mathbf{Q}(\zeta_m)/\mathbf{Q}$.

В дальнейшем мы будем использовать для автоморфизмов степенные обозначения. Если $\sigma \in G$ и $\alpha \in \mathbf{Q}(\zeta_m)$, то мы будем писать α^σ вместо $\sigma\alpha$. Аналогично если A — идеал, то мы будем писать A^σ вместо $\sigma(A)$. Это более общепринятая форма записи, которая имеет определенные преимущества.

Предложение 14.2.4. *Пусть A — некоторый идеал, взаимно простой с m, и $\sigma \in G$. Тогда*

$$\left(\frac{\alpha}{A}\right)_m^\sigma = \left(\frac{\alpha^\sigma}{A^\sigma}\right)_m.$$

Доказательство. Поскольку обе части написанного равенства мультипликативны по A, достаточно будет проверить его для случая, когда $A = P$ — простой идеал. По определению

$$\alpha^{(NP-1)/m} \equiv \left(\frac{\alpha}{P}\right)_m (P).$$

Применяя автоморфизм σ к этому сравнению, получаем

$$(\alpha^\sigma)^{(NP-1)/m} = \left(\frac{\alpha}{P}\right)_m^\sigma (P^\sigma).$$

Отсюда следует, что $(\alpha^\sigma/P^\sigma) \equiv (\alpha/P)_m^\sigma\ (P^\sigma)$, так что $(\alpha^\sigma/P^\sigma)_m = (\alpha/P)_m^\sigma$. Заметим, что мы воспользовались соотношением $N(P^\sigma) = N(P)$. □

Мы закончим этот параграф формулировкой закона взаимности Эйзенштейна. Но сначала нам понадобится одно важное определение.

Пусть l — некоторое нечетное простое число. Напомним, что в D_l выполняется равенство $(l) = (1 - \zeta_l)^{l-1}$ и $(1 - \zeta_l)$ — простой идеал степени 1.

Определение. Ненулевой элемент $\alpha \in D_l$ называется *примарным*, если он взаимно прост с l и сравним по модулю $(1 - \zeta_l)^2$ с некоторым рациональным целым числом.

Если бы l было равно 3, нужно было бы потребовать $\alpha \equiv 2\ (1 - \zeta_3)^2$, так что приведенное определение немного слабее в этом случае [1]). Но для наших целей оно достаточно. Примарных элементов довольно много, как показывает следующая лемма.

Лемма. *Предположим, что $\alpha \in D_l$ и α взаимно просто с l. Тогда существует такое целое число $c \in \mathbf{Z}$, единственное по модулю l, что $\zeta_l^c \alpha$ примарно.*

Доказательство. Пусть $\lambda = 1 - \zeta_l$. Так как простой идеал (λ) имеет степень 1, то существует такое целое число $a \in \mathbf{Z}$, что $\alpha \equiv a\ (\lambda)$. Далее, $(\alpha - a)/\lambda \in D_l$, так что существует такое $b \in \mathbf{Z}$, что $(\alpha - a)/\lambda \equiv b\ (\lambda)$. Следовательно, $\alpha \equiv a + b\lambda\ (\lambda^2)$.

Поскольку $\zeta_l = 1 - \lambda$, мы имеем $\zeta_l^c \equiv 1 - c\lambda\ (\lambda^2)$. Отсюда вытекает, что

$$\zeta_l^c \alpha \equiv a + (b - ac)\lambda\ (\lambda^2).$$

Целое число a не делится на l, так как в противном случае $\lambda \mid \alpha$, а мы предположили, что α взаимно просто с l. Выберем в качестве c решение сравнения $ax \equiv b\ (l)$. Тогда $\zeta_l^c \alpha \equiv a\ (\lambda^2)$, а потому $\zeta_l^c \alpha$ примарно. Единственность c по модулю l, очевидно, следует из доказательства.

Теорема 1. (Закон взаимности Эйзенштейна.) *Пусть l — некоторое нечетное простое число, $a \in \mathbf{Z}$ взаимно просто с l и $\alpha \in$*

---

[1]) См. определение примарного числа в гл. 9 § 3. — *Прим. ред.*

$\in D_l$ — примарный элемент. Предположим, кроме того, что α и a взаимно просты друг с другом. Тогда

$$\left(\frac{\alpha}{a}\right)_l = \left(\frac{a}{\alpha}\right)_l.$$

Доказательство этой изящной теоремы будет приведено в § 5. Она следует из соотношения Штикельбергера, которое будет сформулировано в следующем параграфе и доказано в § 4. Поскольку процесс этот длительный и достаточно сложный, у читателя может возникнуть желание перейти сразу к последней части этой главы, § 6, где приводятся три интересных приложения закона взаимности Эйзенштейна.

§ 3. Соотношение Штикельбергера

По самому способу определения суммы Гаусса являются элементами круговых полей. Мы будем исследовать разложение сумм Гаусса на простые идеалы в этих полях.

Пусть F — конечное поле из $p^f = q$ элементов, χ — мультипликативный характер порядка m и ψ — нетривиальный аддитивный характер (см. гл. 10, § 3). Тогда значениями χ будут корни из единицы степени m, а значениями ψ — корни из единицы степени p. Следовательно,

$$g(\chi, \psi) = \sum_{t \in F} \chi(t)\, \psi(t) \in \mathbf{Q}(\zeta_m, \zeta_p).$$

С арифметикой этого поля мы имели дело в последней главе.

Прежде всего необходимо конкретизировать обстановку, уточнив значения характеров χ и ψ. Это делается следующим образом.

Пусть P — некоторый простой идеал в $D_m \subset \mathbf{Q}(\zeta_m)$, и предположим, что $m \notin P$. Пусть $p\mathbf{Z} = P \cap \mathbf{Z}$ и $N(P) = q = p^f$. Наконец, положим $F = D_m/P$. Напомним, что $p^f \equiv 1\ (m)$.

Мультипликативный характер χ_P на F мы определим следующим образом. Пусть $0 \neq t \in F$ и $\gamma \in D_m$ таков, что $\bar{\gamma} = t$. Здесь $\bar{\gamma}$ — класс вычетов элемента γ по модулю P. Пусть

$$\chi_P(t) = \left(\frac{\gamma}{P}\right)_m^{-1}.$$

В силу предложения 14.2.2 $\chi_P(t)$ определен корректно и является мультипликативным характером. Причина взятия обратного к символу степенного вычета вместо него самого выявится позднее.

В качестве аддитивного характера мы выберем характер ψ, введенный в гл. 10, § 3. Напомним его определение. Сначала

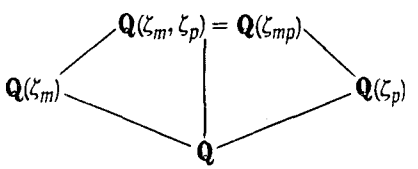
определяется $\mathrm{tr}\colon F \to \mathbf{Z}/p\mathbf{Z}$ посредством формулы $\mathrm{tr}(t) = t + t^p + t^{p^2} + \ldots + t^{p^{f-1}}$. Тогда $\psi(t) = \zeta_p^{\mathrm{tr}(t)}$.

При таком выборе характеров χ_P и ψ мы полагаем $g(P) = g(\chi_P, \psi)$, а также $\Phi(P) = g(P)^m$.

Предложение 14.3.1.
(a) $g(P) \in \mathbf{Q}(\zeta_m, \zeta_p)$.
(b) $|g(P)|^2 = q$.
(c) $\Phi(P) \in \mathbf{Q}(\zeta_m)$.

Доказательство. Пункт (a) уже обсуждался. Пункт (b) получается так же, как и в случае простого поля F. Пункт (c) следует из предложения 8.3.3, которое сформулировано для $\mathbf{Z}/p\mathbf{Z}$, но легко обобщается на F.

Мы приведем другое доказательство п. (c), основанное на теории Галуа. Рассмотрим диаграмму полей



Группа Галуа поля $\mathbf{Q}(\zeta_{mp})/\mathbf{Q}$ задается автоморфизмами σ_c с $(c, pm) = 1$. Заметим, что

(i) поле $\mathbf{Q}(\zeta_m)$ поэлементно инвариантно относительно σ_c в том и только том случае, когда $c \equiv 1\ (m)$;

(ii) поле $\mathbf{Q}(\zeta_p)$ поэлементно инвариантно относительно σ_c в том и только том случае, когда $c \equiv 1\ (p)$.

Для получения включения $\Phi(P) \in \mathbf{Q}(\zeta_m)$ будет достаточно показать, что $\Phi(P)^{\sigma_c} = \Phi(P)$ при $c \equiv 1\ (m)$.

Применим σ_c, где $c \equiv 1\ (m)$, к $g(P) = \sum \chi_P(t)\,\psi(t)$. Так как $\chi_P(t)^{\sigma_c} = \chi_P(t)$ и $\psi(t)^{\sigma_c} = \psi(t)^c$, мы получаем

$$g(P)^{\sigma_c} = \sum \chi_P(t)\,\psi(ct) = \chi_P(c)^{-1}\, g(P).$$

Возведение обеих частей этого равенства в степень m показывает, что $\Phi(P)$ инвариантен при действии σ_c, как и утверждалось. □

Прежде чем приступить к обсуждению разложения элементов $g(P)$ и $\Phi(P)$ на простые идеалы в общем случае, посмотрим, как обстоит дело при $m = 2$, 3 и 4.

При $m = 2$ имеем $\mathbf{Q}(\zeta_2) = \mathbf{Q}$. Если p — положительный образующий для P, то $g(P)^2 = (-1)^{(p-1)/2} p$.

При $m = 3$ имеем $\mathbf{Q}(\zeta_3) = \mathbf{Q}(\sqrt{-3})$. Предположим, что P имеет степень 1 и $P = (\pi)$, где π примарно. Из результатов

гл. 9, § 4, можно получить, что $g(P)^3 = \Phi(P) = p\bar{\pi} = \pi\bar{\pi}^2$ (черта обозначает комплексное сопряжение).

Для $m = 4$ имеем $\mathbf{Q}(\zeta_4) = \mathbf{Q}(\sqrt{-1})$. Предположим, что P — простой идеал степени 1 и $P = (\pi)$, где π примарно. Из § 7 гл. 9 можно получить, что $g(P)^4 = \Phi(P) = p\bar{\pi}^2 = \pi\bar{\pi}^3$ (черта опять обозначает комплексное сопряжение).

Чтобы вывести общее правило и сформулировать обобщение, будет очень полезно ввести одно условное обозначение, известное как «символические степени». Предположим, что $K/\mathbf{Q}$ — некоторое числовое поле, нормальное над $\mathbf{Q}$, с группой Галуа G. Групповое кольцо $\mathbf{Z}(G)$ определяется как множество формальных выражений

$$\sum_{\sigma \in G} a(\sigma)\,\sigma,$$

где коэффициенты $a(\sigma)$ лежат в $\mathbf{Z}$. Позже мы покажем, как это множество превратить в кольцо. Для $\alpha \in K$ полагаем

$$\alpha^{\sum a(\sigma)\sigma} = \prod_{\sigma} \sigma(\alpha)^{a(\sigma)}.$$

Для идеала A его символическая степень относительно элемента группового кольца определяется точно так же.

Пусть σ — нетривиальный автоморфизм поля $\mathbf{Q}(\sqrt{-3})/\mathbf{Q}$. Наш результат при $m = 3$ принимает такой вид: $\Phi(P) = \pi^{1+2\sigma}$.

Аналогично если τ обозначает нетривиальный автоморфизм поля $\mathbf{Q}(\sqrt{-1})/\mathbf{Q}$, то $\Phi(P) = \pi^{1+3\tau}$.

В общем случае мы не можем ожидать разложения $\Phi(P)$ на неприводимые элементы, так как D_m не всегда будет областью с однозначным разложением на простые множители. Однако эти частные случаи красиво обобщаются следующим образом.

Теорема 2. (Соотношение Штикельбергера.) *Пусть P — некоторый простой идеал в D_m, не содержащий m. Тогда*

$$(\Phi(P)) = P^{\sum t\sigma_t^{-1}}.$$

Сумма берется по всем t, $1 \leqslant t < m$, взаимно простым с m.

Длинное доказательство теоремы 2 занимает весь следующий параграф.

§ 4. Доказательство соотношения Штикельбергера

Мы начнем с трех элементарных результатов, которые понадобятся нам в дальнейшем.

Лемма 1. *Пусть* $p > 1$ *— некоторое положительное целое число. Каждое положительное целое число может быть единственным образом записано в виде* $\sum_{i=0}^{n} a_i p^i$, *где* $0 \leqslant a_i < p$.

Доказательство. Пусть a — положительное целое число. Существует единственное неотрицательное целое число n, для которого $p^n \leqslant a < p^{n+1}$. Деление с остатком приводит к равенству $a = a_n p^n + r$, где $0 \leqslant r < p^n$. Число a_n меньше p, ибо в противном случае $a \geqslant p^{n+1}$. Применим тот же прием к r и т. д. За конечное число шагов мы получим для a выражение требуемого вида.

Единственность представления может быть доказана следующим образом. Предположим, что $\sum a_i p^i = \sum b_i p^i$, где $0 \leqslant a_i, b_i < p$. Тогда p делит $a_0 - b_0$. Так как $|a_0 - b_0| < p$, то $a_0 = b_0$. Вычитая a_0 из обеих частей равенства и деля результат на p, повторяем рассуждение. Это приводит к равенству $a_1 = b_1$. За конечное число шагов мы получаем, что $a_i = b_i$ при всех i. □

Определение. Пусть $q = p^f$. Если $0 \leqslant a < q - 1$, запишем $a = \sum_{i=0}^{f-1} a_i p^i$, где $0 \leqslant a_i < p$, и положим

$$S(a) = \sum_{i=0}^{f-1} a_i.$$

Для произвольного положительного целого числа a пусть $S(a) = S(r)$, где $a \equiv r \ (q-1)$ и $0 \leqslant r < q - 1$.

Определение. Для вещественного числа u определим $\langle u \rangle$ как $u - [u]$, где $[u]$ — наибольшее целое число, меньшее или равное u. Число $\langle u \rangle$, лежащее в интервале $[0, 1)$, называется *дробной частью* числа u.

Лемма 2. $S(a) = (p-1) \sum_{i=0}^{f-1} \langle p^i a/(q-1) \rangle$.

Доказательство. Обе части написанного равенства не изменятся, если к a будет добавлено некоторое кратное числа $q - 1$. Таким образом, можно считать, что $1 \leqslant a < q - 1$.

Запишем $a = a_0 + a_1 p + \ldots + a_{f-1} p^{f-1}$, где $0 \leqslant a_i < p$. Так как $p^f = q \equiv 1 \ (q-1)$, то

$$\begin{aligned} a &= a_0 + a_1 p + \ldots + a_{f-1} p^{f-1}, \\ pa &\equiv a_{f-1} + a_0 p + \ldots + a_{f-2} p^{f-1} \ (q-1), \\ p^2 a &\equiv a_{f-2} + a_{f-1} p + \ldots + a_{f-3} p^{f-1} \ (q-1), \text{ и т. д.} \end{aligned}$$

Правые части всех этих сравнений меньше, чем $q-1$, так что $\langle p^i a/(q-1)\rangle$ равно правой части i-го сравнения, деленной на $q-1$. Таким образом,

$$\sum_{i=0}^{f-1}\left\langle\frac{p^i a}{q-1}\right\rangle=\frac{1}{q-1}S(a)(1+p+\ldots+p^{f-1}).$$

Лемма доказана. □

Лемма 3. $\sum_{a=1}^{q-2} S(a)=(f(p-1)(q-2))/2.$

Доказательство. Запишем $a=a_0+a_1p+\ldots+a_{f-1}p^{f-1}$, где $0\leqslant a_i<p$. Заметим, что $q-1=(p-1)+(p-1)p+\ldots+(p-1)p^{f-1}$. Отсюда следует, что $q-1-a=(p-1-a_0)+(p-1-a_1)p+\ldots+(p-1-a_{f-1})p^{f-1}$, так что

$$S(a)+S(q-1-a)=f(p-1).$$

Суммируя обе части этого равенства от $a=1$ до $a=q-2$, в результате получаем

$$2\sum_{a=1}^{q-2}S(a)=f(p-1)(q-2).$$ □

Сумма Гаусса $g(P)$, рассмотренная в предыдущем параграфе, является элементом поля $\mathbf{Q}(\zeta_m, \zeta_p)$. Приводимое нами доказательство теоремы 2 требует, чтобы мы работали в большем поле $\mathbf{Q}(\zeta_{q-1}, \zeta_p)$. Это дает то преимущество, что свободно могут использоваться все корни степени $q-1$ из единицы. С другой стороны, больше полей — больше путаницы. Мы постараемся свести к минимуму эту путаницу, внимательно следя за тем, в каком поле мы в каждый момент времени работаем.

При последующих рассуждениях будет полезно иметь перед глазами следующую диаграмму:

$$\begin{array}{ccc}
\mathfrak{P}\subset D_{(q-1)p} & \to & D_{(q-1)p}/\mathfrak{P} \\
\downarrow\quad\downarrow & & \downarrow \\
\mathfrak{P}\subset D_{q-1} & \to & D_{q-1}/\mathfrak{P} \\
\downarrow\quad\downarrow & & \downarrow \\
P\subset D_m & \to & D_m/P \\
\downarrow\quad\downarrow & & \downarrow \\
p\subset \mathbf{Z} & \to & \mathbf{Z}/p\mathbf{Z}
\end{array}\Bigg\} f$$

В этой диаграмме P, $\mathfrak{P}$ и $\mathfrak{P}$ — простые идеалы в указанных кольцах целых чисел. Вспомним (см. § 3), что $p\nmid m$, f — поря-

док p по модулю m, так что $p^f \equiv 1\ (m)$, и $q = p^f$. До конца этого параграфа $\lambda_p = 1 - \zeta_p$.

Лемма 4.
(1) $\mathrm{ord}_{\mathscr{P}}(pD_{(q-1),p}) = p - 1$.
(2) $\mathrm{ord}_{\mathscr{P}}(\lambda_p) = 1$.
(3) $\mathrm{ord}_{\mathscr{P}}(P) = p - 1$.

Доказательство. Для доказательства (1) применим предложение 13.2.9 с m (в обозначении этого предложения), замененным на $q - 1$. Так как $\mathscr{P}$ лежит над p, он входит в разложение идеала pD, и $\mathrm{ord}_{\mathscr{P}} pD_{(q-1)\,p} = p - 1$. Опять по тому же самому предложению и предложению 13.2.7 имеют место равенства

$$pD_{p\,(q-1)} = (pD_p)\,D_{p\,(q-1)} = \lambda_p^{p-1} D_{p\,(q-1)} = (\mathscr{P}_1 \ldots \mathscr{P}_h)^{p-1},$$

где, скажем, $\mathscr{P}_1 = \mathscr{P}$. Следовательно, $\lambda_p D_{p\,(q-1)} = \mathscr{P}_1 \ldots \mathscr{P}_h$ и (2) доказано. Для доказательства (3), используя теорему 2 гл. 13 и предложение 13.2.9, получаем, что $PP_2 \ldots P_h \cdot D_{(q-1)\,p} = (\mathscr{P}\mathscr{P}_2 \ldots \mathscr{P}_h)^{p-1}$, где все простые идеалы различны и P, P_2, ..., P_h попарно взаимно просты. Таким образом, $PD_{(q-1)\,p} = \mathscr{P}^{p-1}$, откуда и следует доказываемый результат. □

Лемма 5. $D_m/P \approx D_{q-1}/\mathfrak{P}$.

Доказательство Имеется естественный мономорфизм из D_m/P в $D_{q-1}/\mathfrak{P}$. Чтобы убедиться в том, что это изоморфизм, достаточно показать, что оба поля имеют одно и то же число элементов. По теореме 2 гл. 13 $|D_{q-1}/\mathfrak{P}| = p^{f'}$, где f' — наименьшее положительное целое число, для которого $p^{f'} \equiv 1\ (q-1)$. Так как $q = p^f$, ясно, что $f' = f$, а потому $|D_{q-1}/\mathfrak{P}| = p^f = |D_m/P|$. □

В силу предложения 13.2.3 элементы 1, ζ_{q-1}, ..., ζ_{q-1}^{q-2} имеют разные образы в $D_{q-1}/\mathfrak{P}$. Следующее определение аналогично определению символа m-степенного вычета.

Определение. Для $\alpha \in D_{q-1}$ положим
(a) $(\alpha/\mathfrak{P}) = 0$, если $\alpha \in \mathfrak{P}$;
(b) если $\alpha \notin \mathfrak{P}$, то $(\alpha/\mathfrak{P})$ — единственный корень степени $q-1$ из единицы, для которого $\alpha \equiv (\alpha/\mathfrak{P})\ (\mathfrak{P})$.

Нетрудно убедиться в том, что $(\alpha\beta/\mathfrak{P}) = (\alpha/\mathfrak{P})\,(\beta/\mathfrak{P})$ и что из $\alpha \equiv \beta\ (\mathfrak{P})$ вытекает равенство $(\alpha/\mathfrak{P}) = (\beta/\mathfrak{P})$. Следующая лемма тоже легко получается из определений.

Лемма 6. *Если* $\alpha \in D_m$, *то* $(\alpha/\mathfrak{P})^{(q-1)/m} = (\alpha/P)_m$.

Мы теперь следующим образом определим мультипликативный характер на $\mathbf{F} \approx D_{q-1}/\mathfrak{P}$:

$$\omega(t) = \left(\frac{\gamma}{\mathfrak{P}}\right),$$

где $\gamma \in D_{q-1}$ таков, что $\bar{\gamma} = t$. Доказательство того, что ω определен корректно и является мультипликативным характером, получается сразу же из предыдущих замечаний.

Лемма 7. $\omega(\bar{\zeta}_{q-1}^{i}) = \zeta_{q-1}^{i}$.

Доказательство следует из определения. □

Значит, ω имеет порядок $q-1$ и, таким образом, порождает группу мультипликативных характеров на $\mathbf{F}$.

Определение. Пусть a — некоторое неотрицательное целое число. Положим $g_a = g(\omega^{-a}, \psi)$.

Заметим, что $g(P)$, определенное в предыдущем параграфе, равно g_a при $a = (q-1)/m$.

Теорема 2 является следствием такого результата:

Теорема 3. $\operatorname{ord}_{\mathscr{P}}(g_a) = S(a)$, *где* $1 \leqslant a < q$.

Доказательство. Для начала мы покажем, что $\operatorname{ord}_{\mathscr{P}}(g_1) = 1$. Напомним, что

$$g_1 = \sum_{t \in \mathbf{F}} \omega(t)^{-1} \zeta_p^{\operatorname{tr}(t)}.$$

Используя лемму 7, мы превратим это выражение в сумму по степеням ζ_{q-1}. Пусть m_i — такое положительное целое число, что $m_i \equiv \operatorname{tr}(\bar{\zeta}_{q-1}^{i})\ (p)$. Напомним также, что $\zeta_p = 1 - \lambda_p$. В таком случае

$$g_1 = \sum_{i=0}^{q-2} \zeta_{q-1}^{-i} (1-\lambda_p)^{m_i}.$$

Используя формулу бинома, убеждаемся в том, что $(1-\lambda_p)^{m_i} \equiv 1 - m_i\lambda_p\ (\mathscr{P}^2)$, а потому

$$g_1 \equiv -\left(\sum_{i=0}^{q-2} m_i \zeta_{q-1}^{-i}\right) \lambda_p\ (\mathscr{P}^2).$$

Далее,

$$m_i\lambda_p \equiv (\zeta_{q-1}^{i} + \zeta_{q-1}^{pi} + \ldots + \zeta_{q-1}^{p^{f-1}i})\lambda_p\ (\mathscr{P}^2).$$

Производя подстановку, получаем

$$g_1 = -\sum_{i=0}^{q-2} \zeta_{q-1}^{-i} \left(\zeta_{q-1}^{i} + \zeta_{q-1}^{pi} + \ldots + \zeta_{q-1}^{p^{f-1}i}\right) \lambda_p \ (\mathscr{P}^2).$$

Все суммы

$$\sum_{i=0}^{q-2} \zeta_{q-1}^{(p^j-1)\,i}, \quad j = 1, 2, \ldots, f-1,$$

равны нулю, в то время как при $j = 0$ получается значение $q - 1$. Так как $q = p^f \equiv 0 \ (\mathscr{P}^2)$, то

$$g_1 \equiv \lambda_p \ (\mathscr{P}^2).$$

В силу п. (2) леммы 4 мы получаем, что $\lambda_p \in \mathscr{P}$, но $\lambda_p \notin \mathscr{P}^2$. Таким образом, $\operatorname{ord}_{\mathscr{P}} g_1 = 1$.

Пусть $\tilde{s}(a) = \operatorname{ord}_{\mathscr{P}} g_a$. Мы выведем ряд свойств функции $\tilde{s}(a)$.

(i) $\tilde{s}(a+b) \leqslant \tilde{s}(a) + \tilde{s}(b)$ при условии, что

$$1 \leqslant a,\ b,\ a+b < q-1.$$

По теореме 1 гл. 8 $g_a g_b = J(\omega^{-a}, \omega^{-b})\, g_{a+b}$. Беря $\operatorname{ord}_{\mathscr{P}}$ от обеих частей этого равенства, получаем доказываемый результат.

(ii) $\tilde{s}(a+b) \equiv \tilde{s}(a) + \tilde{s}(b) \ (p-1)$.

Заметим, что сумма Якоби $J(\omega^{-a}, \omega^{-b})$ лежит в $\mathbf{Q}(\zeta_{q-1})$. Из равенства $\mathfrak{P} D_{(q-1)p} = \mathscr{P}^{(p-1)}$ тогда выводим, что $p-1$ делит $\operatorname{ord}_{\mathscr{P}}(J(\omega^{-a}, \omega^{-b}))$. Таким образом, доказываемый результат опять сразу же следует из соотношения $g_a g_b = J(\omega^{-a}, \omega^{-b})\, g_{a+b}$.

(iii) $\tilde{s}(pa) = \tilde{s}(a)$.

Чтобы убедиться в этом, заметим, что

$$g_{pa} = \sum \omega(t)^{-pa} \psi(t) = \sum \omega(t^p)^{-a} \psi(t^p).$$

Мы воспользовались тем фактом, что $\operatorname{tr}(t) = \operatorname{tr}(t^p)$, а это очевидно в силу определения следа. Но $t \to t^p$ — автоморфизм поля $\mathbf{F}$. В результате получаем, что $g_{pa} = g_a$, а потому $\tilde{s}(pa) = \tilde{s}(a)$.

В первой части доказательства мы нашли, что $\tilde{s}(1) = 1$. Используя (i) и (ii), убеждаемся, что $\tilde{s}(a) = a$ для $1 \leqslant a < p$.

Для любого a между 1 и $q-1$ запишем $a = a_0 + a_1 p + \ldots + a_{f-1} p^{f-1}$, $0 \leqslant a_i < p$. Используя (i) и (iii), приходим к соотношениям

$$\tilde{s}(a) \leqslant \sum_{j=0}^{f-1} \tilde{s}(a_j p^j) = \sum_j \tilde{s}(a_j) = \sum_j a_j = S(a).$$

Теперь $\tilde{s}(a) \leqslant S(a)$ для всех a в рассматриваемых пределах. Для доказательства теоремы будет достаточно, в свете леммы 3, показать, что

$$\text{(iv)} \qquad \sum_{a=1}^{q-2} \tilde{s}(a) = \frac{f(p-1)(q-2)}{2}.$$

Вообще, для сумм Гаусса мы имеем соотношение $g(\chi^{-1}) = \chi(-1)\,\overline{g(\chi)}$ (здесь черта обозначает комплексное сопряжение). Таким образом, $g_a g_{q-1-a} = \omega(-1)^a q = \omega(-1)^a p^f$. Из леммы 4 мы знаем, что $\mathrm{ord}_{\mathscr{P}}(p) = p - 1$. Отсюда следует, что

$$\tilde{s}(a) + \tilde{s}(q-1-a) = f(p-1).$$

Просуммировав обе части этого равенства по a от 1 до $q-2$, получим

$$2\sum_{a=0}^{q-2} \tilde{s}(a) = f(p-1)(q-2).$$

Это завершает доказательство теоремы 3. □

Следствие. $\mathrm{ord}_P(\Phi(P)) = (m/(p-1))\,S((q-1)/m)$.

Доказательство. Воспользовавшись леммой 4, п. (3), получаем

$$(p-1)\,\mathrm{ord}_{\mathfrak{p}}(\Phi(P)) = \mathrm{ord}_{\mathscr{P}}(\Phi(P)).$$

Далее,

$$\mathrm{ord}_{\mathscr{P}}(\Phi(P)) = m\,\mathrm{ord}_{\mathscr{P}}(g(P)) = mS((q-1)/m),$$

где последнее равенство следует из теоремы 3, ибо $g(P) = g_a$, где $a = (q-1)/m$. □

Это следствие является первым шагом в получении полного разложения на простые множители для $\Phi(P)$. Чтобы продвинуться дальше, мы заметим сначала, что единственными простыми идеалами в D_m, содержащими $\Phi(P)$, будут те, которые содержат p. Это следует из пп. (b) и (c) предложения 14.3.1, которые показывают, что

$$|\Phi(P)|^2 = q^m = p^{fm}.$$

Если P' — какой-либо другой простой идеал кольца D_m, содержащий p, то по предложению 12.3.3 существует такой автоморфизм σ_t поля $\mathbf{Q}(\zeta_m)/\mathbf{Q}$, что $P' = P^{\sigma_t^{-1}}$. Для $1 \leqslant t < m$ и $(t, m) = 1$ положим $P_t = P^{\sigma_t^{-1}}$.

Лемма 8. $\operatorname{ord}_{P_t}(\Phi(P)) = (m/(p-1))\, S(t((q-1)/m))$.

Доказательство. Из определений легко получается, что

$$\operatorname{ord}_{P_t}(\Phi(P)) = \operatorname{ord}_P(\Phi(P)^{\sigma_t}).$$

Выберем такое целое число t', что $t' \equiv t\,(m)$ и $t' \equiv 1\,(p)$. Тогда

$$g(P)^{\sigma_{t'}} = \Big(\sum_{r \in F} \chi_P(r)\,\psi(r)\Big)^{\sigma_{t'}} = \sum_{r \in F} \chi_P(r)^t\,\psi(r).$$

Таким образом,

$$\Phi(P)^{\sigma_t} = \Big(\sum_{r \in F} \chi_P^t(r)\,\psi(r)\Big)^m.$$

Второй член в этом соотношении равен g_a^m, где $a \equiv t\ ((q-1)/m)$. Доказательство леммы завершается теперь при помощи того же самого рассуждения, что и в следствии теоремы 3. □

Мы можем теперь, наконец, закончить доказательство теоремы 2.

В силу следствия теоремы 2 из гл. 13 группа

$$G(P) = \{\sigma \in G(\mathbf{Q}(\zeta_m)/\mathbf{Q}) \mid P^\sigma = P\}$$

циклическая и порождается элементом σ_p.

Пусть $t_1, t_2, \ldots, t_g$ — множество целых чисел, представляющих классы смежности в $U(\mathbf{Z}/m\mathbf{Z})$ по модулю циклической подгруппы, порожденной образом p. Другими словами, если $1 \leqslant t < m$, $(t, m) = 1$, то $t \equiv t_i p^j\ (m)$ для единственной пары (i, j), $0 \leqslant j \leqslant f$, $1 \leqslant i \leqslant g$. В силу леммы 8, простое разложение для $\Phi(P)$ задается идеалами

$$P^{\gamma'}, \text{ где } \gamma' = \frac{m}{p-1} \sum_{i=1}^{g} S\left(t_i \frac{q-1}{m}\right) \sigma_{t_i}^{-1}.$$

Воспользовавшись леммой 2, мы можем записать γ' следующим образом:

$$\gamma' = m \sum_i \left(\sum_j \left\langle \frac{p^j t_i}{m} \right\rangle \right) \sigma_{t_i}^{-1}.$$

Индекс i меняется от 1 до g и индекс j меняется от 0 до $f-1$. Так как σ_p оставляет P на месте, действие γ' на P совпадает с действием

$$\gamma = m \sum_i \sum_j \left\langle \frac{p^j t_i}{m} \right\rangle \sigma_{t_i}^{-1} \sigma_{p^j}^{-1} = m \sum_{t \bmod m} \left\langle \frac{t}{m} \right\rangle \sigma_t^{-1} =$$

$$= \sum t \sigma_t^{-1}, \text{ где } 1 \leqslant t < m \text{ и } (t, m) = 1.$$

Это завершает доказательство. □

Для дальнейших ссылок мы заметим, что

$$(\Phi(P)) = P^{m\theta},$$

где $\theta = \sum_{t \bmod m} \langle t/m \rangle \sigma_t^{-1}$, $(t, m) = 1$. Элемент $\theta \in \mathbf{Q}[G]$ называется элементом Штикельбергера.

§ 5. Доказательство закона взаимности Эйзенштейна

Нам понадобятся два результата о корнях из единицы.

Лемма 1. *Единственными корнями из единицы в поле* $\mathbf{Q}(\zeta_m)$ *будут* $\pm\zeta_m^i$, $i = 1, 2, \ldots, m$.

Доказательство. В доказательстве теоремы 1 этот результат будет нужен нам лишь в случае, когда m — нечетное простое число. Доказательство для общего m переносится в упражнения, а здесь мы предполагаем, что $m = l$ — нечетное простое число.

Пусть $\zeta_n \in \mathbf{Q}(\zeta_l)$. Если $4 \mid n$, то $\sqrt{-1} \in \mathbf{Q}(\zeta_l)$. Но 2 разветвляется в $\mathbf{Q}(\sqrt{-1})$ и не разветвляется в $\mathbf{Q}(\zeta_l)$. Таким образом, $4 \nmid n$. Если $n = 2n_0$, n_0 нечетно, то $\{\zeta_n^i\} = \{\pm\zeta_{n_0}^i\}$, а потому мы можем считать, что n нечетно. Если l' — нечетное простое число, делящее n, то $\zeta_{l'} \in \mathbf{Q}(\zeta_l)$. Но l' разветвлено в $\mathbf{Q}(\zeta_{l'})$ и l — единственное простое число, разветвленное в $\mathbf{Q}(\zeta_l)$. Таким образом, $l = l'$ и n должно быть степенью l, скажем l^a. Так как $\varphi(l^a) = l^{a-1}(l-1)$ — степень поля $\mathbf{Q}(\zeta_{l^a})$ над $\mathbf{Q}$ и $l - 1$ — степень поля $\mathbf{Q}(\zeta_l)$ над $\mathbf{Q}$, то $a = 1$. Отсюда и следует доказываемый результат. □

Лемма 2. *Пусть* $K/\mathbf{Q}$ *— поле алгебраических чисел и* $\sigma_1, \sigma_2, \ldots, \sigma_n$ *суть* $n = [K: \mathbf{Q}]$ *изоморфизмов поля* K *в* $\mathbf{C}$. *Если* $\alpha \neq K$ *— такой целый элемент, что* $|\alpha^{\sigma_i}| \leqslant 1$ *при всех* $i = 1, 2, \ldots, n$, *то* α *есть корень из единицы.*

Доказательство. α — корень многочлена

$$f(x) = \prod_{i=1}^{n} (x - \alpha^{\sigma_i}) \in \mathbf{Z}[x].$$

Предположения леммы означают, что коэффициент при x^m в $f(x)$ — целое рациональное число, ограниченное по модулю биномиальным коэффициентом $\binom{n}{m}$. Таким образом, лишь конечное число многочленов степени n в $\mathbf{Z}[x]$ может получиться таким способом.

Если α удовлетворяет предположениям леммы, то им удовлетворяют и все степени α. Так как конечное число многочленов может иметь лишь конечное число корней, отсюда следует, что какие-нибудь две различные степени α должны быть равны. Поэтому α есть корень из единицы. □

Следующий шаг состоит в определении $\Phi(A)$ для произвольного идеала в D_m, A взаимно просто с m, и исследовании свойства этой функции. В частности, будет важно найти значения Φ на главных идеалах.

Определение. Пусть $A \subset D_m$ — некоторый идеал, взаимно простой с m. Пусть $A = P_1 P_2 \ldots P_n$ — разложение A на простые идеалы. Положим

$$\Phi(A) = \Phi(P_1)\,\Phi(P_2) \ldots \Phi(P_n).$$

Предложение 14.5.1. *Пусть A, $B \subset D_m$ — идеалы, взаимно простые с m, и $\alpha \in D_m$ — некоторый элемент, взаимно простой с m; напомним, что $\gamma = \sum t\sigma_t^{-1}$, $1 \leqslant t < m$ и $(t, m) = 1$. Тогда*

(a) $\Phi(A)\,\Phi(B) = \Phi(AB)$;
(b) $|\Phi(A)|^2 = (NA)^m$;
(c) $(\Phi(A))^{\gamma} = A^{\gamma}$;
(d) $\Phi((\alpha)) = \varepsilon(\alpha)\,\alpha^{\gamma}$, *где* $\varepsilon(\alpha)$ — *единица в* D_m.

Доказательство. Пункт (a) ясен из определения. Так как обе части в п. (b) мультипликативны по A, мы можем предполагать, что A — простой идеал P. В этом случае $|\Phi(P)|^2 = |g(P)|^{2m} = (NP)^m$ в силу предложения 14.3.1, п. (b).

Обе части в (c) мультипликативны по A, так что мы опять можем предполагать, что A — простой идеал P. В этом случае доказываемый результат совпадает с теоремой 2.

Для п. (d) заметим, что

$$(\Phi((\alpha)))^{\gamma} = (\alpha)^{\gamma} = (\alpha^{\gamma})$$

в силу п. (c). Таким образом, $\Phi((\alpha))$ и α^{γ} порождают один и тот же главный идеал. □

В дальнейшем мы будем писать $\Phi(\alpha)$ вместо $\Phi((\alpha))$.

Будет важно определить обратимый элемент $\varepsilon(\alpha)$ более точно. В действительности мы покажем, что он есть корень из единицы.

Лемма 3. *Предположим, что $A \subset D_m$ — идеал, взаимно простой с m, и σ — автоморфизм поля $\mathbf{Q}(\zeta_m)/\mathbf{Q}$. Тогда*

$$\Phi(A)^{\sigma} = \Phi(A^{\sigma}).$$

Доказательство. Чтобы убедиться в этом, удобно записать $g(P)$ в следующем виде:

$$g(P) = \sum \left(\frac{\alpha}{P}\right)_m^{-1} \zeta_p^{\mathrm{tr}(\bar{\alpha})},$$

где сумма берется по множеству представителей классов смежности D_m/P.

Пусть $\tilde{\sigma}$ — некоторый автоморфизм поля $\mathbf{Q}(\zeta_m, \zeta_p)/\mathbf{Q}$, который при ограничении на $\mathbf{Q}(\zeta_m)$ превращается в σ, а при ограничении на $\mathbf{Q}(\zeta_p)$ тривиален (см. доказательство леммы 8). В силу предложения 14.2.4

$$g(P)^{\tilde{\sigma}} = \sum \left(\frac{\alpha^\sigma}{P^\sigma}\right)_m^{-1} \zeta_p^{\mathrm{tr}(\bar{\alpha})}.$$

Так как $\mathrm{tr}(\bar{\alpha}) \in \mathbf{Z}/p\mathbf{Z}$, то $\mathrm{tr}(\bar{\alpha}^\sigma) = \mathrm{tr}(\bar{\alpha})$. Отсюда следует, что $g(P)^{\tilde{\sigma}} = g(P^\sigma)$. Возведение обеих частей этого равенства в степень m приводит к нужному результату в случае, когда A — простой идеал. Общий случай следует из мультипликативности. □

Лемма 4. *Для* $\alpha \in D_m$ *имеем* $|\alpha^\gamma|^2 = |N\alpha|^m$.

Доказательство. Автоморфизм σ_{-1} совпадает с комплексным сопряжением на $\mathbf{Q}(\zeta_m)$, так как он переводит ζ_m в $\zeta_m^{-1} = \bar{\zeta}_m$. Таким образом,

$$|\alpha^\gamma|^2 = \alpha^\gamma \alpha^{\gamma\sigma_{-1}} = \alpha^{\gamma(1+\sigma_{-1})}.$$

Далее, $\sigma_{-1}\gamma = \sigma_{-1} \sum t\sigma_t^{-1} = \sum t\sigma_{-t}^{-1}$. Очевидно, что $\sigma_{m-t} = \sigma_{-t}$ и $\gamma = \sum (m-t)\,\sigma_{m-t}^{-1}$. Таким образом, используя равенство $t = m - (m-t)$, приходим к равенству

$$(1 + \sigma_{-1})\,\gamma = m \sum \sigma_t^{-1}.$$

Лемма вытекает из того факта, что $N\alpha = \prod \alpha^{\sigma_t^{-1}} = \alpha^{\sum \sigma_t^{-1}}$. □

Предложение 14.5.2. *Пусть* $\alpha \in D_m$ *взаимно просто с* m. *Тогда* $\Phi(\alpha) = \varepsilon(\alpha)\,\alpha^\gamma$, *где* $\varepsilon(\alpha) = \pm\zeta_m^i$ *при некотором* i.

Доказательство. Ввиду п. (d) последнего предложения достаточно доказать лишь утверждение относительно $\varepsilon(\alpha)$. В силу предложения 14.5.1 $|\Phi(\alpha)|^2 = (N(\alpha))^m$ и $|\alpha^\gamma|^2 = |N\alpha|^m$, согласно лемме 4. Ввиду предложения 14.1.3 $N(\alpha) = |N\alpha|$.

Собирая все это вместе, получаем, что $|\varepsilon(\alpha)| = 1$. Используя лемму 3, тем же способом устанавливаем, что $|\varepsilon(\alpha)^\sigma| = 1$ при всех $\sigma \in G$. Из леммы 2 теперь следует, что $\varepsilon(\alpha)$ — корень из единицы. Наконец, так как $\varepsilon(\alpha) \in \mathbf{Q}(\zeta_m)$, то $\varepsilon(\alpha) = \pm\zeta_m^i$, в силу леммы 1. □

Мы теперь в состоянии приступить к доказательству закона взаимности Эйзенштейна. Способ доказательства следующего предложения уже знаком нам по доказательствам квадратичного, кубического и биквадратичного законов взаимности. Оно само есть некоторое утверждение «взаимности».

Предложение 14.5.3. *Предположим, что* P, $P' \subset \boldsymbol{D}_m$ — *простые идеалы, взаимно простые с* m. *Пусть, кроме того, числа* NP *и* NP' *взаимно просты. Тогда*

$$\left(\frac{\Phi(P)}{P'}\right)_m = \left(\frac{NP'}{P}\right)_m.$$

Доказательство. Пусть $q' = p'^{f'} = NP'$. Напомним, что $q' \equiv 1\ (m)$. Следующие сравнения берутся в D_m по модулю p':

$$g(P)^{q'} \equiv \sum \chi_P(t)^{q'} \psi(t)^{q'} \equiv \sum \chi_P(t) \psi(q't) \equiv \left(\frac{q'}{P}\right)_m g(P).$$

С другой стороны,

$$g(P)^{q'-1} = \Phi(P)^{(q'-1)/m} \equiv \left(\frac{\Phi(P)}{P'}\right)_m (P').$$

Отсюда следует, что

$$\left(\frac{\Phi(P)}{P'}\right)_m \equiv \left(\frac{NP'}{P}\right)_m (P').$$

Так как $m \notin P'$, то обе части этого сравнения должны быть равны. □

Следствие 1. *Предположим, что* A, $B \subset D_m$ — *взаимно простые с* m *идеалы и что* NA *и* NB *взаимно просты друг с другом. Тогда*

$$\left(\frac{NB}{A}\right)_m = \left(\frac{\Phi(A)}{B}\right)_m.$$

Доказательство. Как обычно, это следствие получается из предложения 14.5.3 по мультипликативности. □

Следствие 2. *Предположим, что* A *и* B *такие же, как в следствии* 1, *и что, кроме того, идеал* $A = (\alpha)$ *главный. Тогда*

$$\left(\frac{\varepsilon(\alpha)}{B}\right)_m \left(\frac{\alpha}{NB}\right)_m = \left(\frac{NB}{\alpha}\right)_m.$$

Доказательство. Начнем с равенства

$$\left(\frac{\Phi(\alpha)}{B}\right)_m = \left(\frac{\varepsilon(\alpha)}{B}\right)_m \left(\frac{\alpha^{\nu}}{B}\right)_m.$$

Заметим, что

$$\left(\alpha^{t\sigma_t^{-1}} / B\right)_m = \left(\alpha^{\sigma_t^{-1}} / B\right)_m^t = \left(\alpha^{\sigma_t^{-1}} / B\right)_m^{\sigma_t} = (\alpha / B^{\sigma_t})_m$$

в силу предложения 14.2.4. Таким образом,

$$\left(\frac{\alpha^\nu}{B}\right)_m = \prod_t \left(\frac{\alpha^{t\sigma_t^{-1}}}{B}\right)_m = \prod_t \left(\frac{\alpha}{B^{\sigma_t}}\right)_m = \left(\frac{\alpha}{NB}\right)_m.$$

Для получения окончательного равенства следует воспользоваться предложением 14.1.2. □

В дальнейшем мы будем предполагать, что $m = l$ — нечетное простое число.

Лемма 5. *Если $A \subset D_l$ — взаимно простой с l идеал, то* $\Phi(A) \equiv \pm 1\ (l)$.

Доказательство. Достаточно показать, что $\Phi(P) \equiv -1\ (l)$ где $P \subset D_l$ — некоторый простой идеал, взаимно простой с l. Имеем

$$\Phi(P) = g(P)^l \equiv \sum_t \chi_P(t)^l \psi(t)^l\ (l) \equiv$$

$$\equiv \sum_{t \neq 0} \psi(lt)\ (l) \equiv -1\ (l).$$

Последнее сравнение следует из того факта, что $l \to \psi(lt)$ является нетривиальным аддитивным характером на D_l/P, так что сумма его значений по всем t равна нулю. Нужный результат вытекает из того, что $\psi(0) = 1$. □

Напомним, что $\alpha \in D_l$ называется примарным, если он взаимно прост с l и выполняется сравнение $\alpha \equiv x\ ((1 - \zeta_l)^2)$ при некотором $x \in \mathbf{Z}$.

Лемма 6. *Если $\alpha \in D_l$ примарен, то* $\varepsilon(\alpha) = \pm 1$.

Доказательство. Так как $(1 - \zeta_l)$ — единственный простой идеал над l в D_l, то $(1 - \zeta_l)^\sigma = (1 - \zeta_l)$ при всех $\sigma \in G$. Отсюда следует, что $(1 - \zeta_l)^\nu \subset (1 - \zeta_l)$.

Так как $\Phi(\alpha) = \varepsilon(\alpha)\,\alpha^\nu$, то по лемме 5 $\varepsilon(\alpha)\,\alpha^\nu \equiv \pm 1\ (l)$. Поскольку $\alpha \equiv x\ ((1 - \zeta_l)^2)$ с $x \in \mathbf{Z}$, то

$$\alpha^\nu \equiv x^\nu\ ((1 - \zeta_l)^2) \equiv x^{1+2+\cdots+l-1}\ ((1 - \zeta_l)^2).$$

Далее, $x^{(l-1)/2} \equiv \pm 1\ (l)$, так что

$$\alpha^\nu \equiv (\pm 1)^l\ ((1 - \zeta_l)^2) \equiv \pm 1\ ((1 - \zeta_l)^2).$$

Отсюда следует, что $\varepsilon(\alpha) \equiv \pm 1 \ ((1-\zeta_l)^2)$. Из предложения 14.5.2 мы знаем, что $\varepsilon(\alpha) = \pm\zeta_l^i$. Чтобы закончить доказательство, мы должны показать, что l делит i. Это следует из утверждения о единственности в лемме из § 2, но имеет смысл убедиться в этом и непосредственно.

Имеем $\zeta_l^i \equiv \pm 1 \ ((1-\zeta_l)^2)$. Записывая $\zeta_l = 1 - (1-\zeta_l)$, получаем

$$1 - i(1-\zeta_l) \equiv \pm 1 \ ((1-\zeta_l)^2).$$

Здесь должен стоять знак плюс, ибо в противном случае $1-\zeta_l$ делило бы 2. Но тогда, вычитая 1 из обеих частей, убеждаемся в том, что $1-\zeta_l$ делит i, а это означает $l \mid i$. □

Предложение 14.5.4. *Если $\alpha \in D_l$ примарен, B — некоторый взаимно простой с l идеал и число NB взаимно просто с α, то*

$$\left(\frac{\alpha}{NB}\right)_l = \left(\frac{NB}{\alpha}\right)_l.$$

Доказательство. Согласно следствию 2 предложения 14.5.3, нам надо лишь показать, что $(\varepsilon(\alpha)/B)_l = 1$.

Так как α примарно, то $\varepsilon(\alpha) = \pm 1$ по только что доказанной лемме. Поскольку l нечетно, $(\pm 1)^l = \pm 1$ и предложение доказано. □

Теперь мы можем закончить доказательство теоремы 1.

Пусть $p \in \mathbf{Z}$ — некоторое простое число, $p \neq l$ и p взаимно просто с α в D_l. Пусть P — простой идеал в D_l, содержащий p. Тогда $NP = p^f$. В только что доказанном предложении подставим P вместо B. В результате получим

$$\left(\frac{\alpha}{p}\right)_l^f = \left(\frac{p}{\alpha}\right)_l^f.$$

Так как $f \mid l-1 = [\mathbf{Q}(\zeta_l) : \mathbf{Q}]$, то $(f, l) = 1$. Таким образом,

$$\left(\frac{\alpha}{p}\right)_l = \left(\frac{p}{\alpha}\right)_l.$$

Отсюда и (в последний раз) из мультипликативности получаем, что $(\alpha/a)_l = (a/\alpha)_l$ при всех $a \in \mathbf{Z}$, взаимно простых с l и α, если α примарно. □

§ 6. Три приложения

В гл. 5 мы доказали, что если a — целое число, для которого сравнение $x^2 \equiv a \ (p)$ разрешимо для всех, кроме конечного числа, простых чисел, то a будет квадратом. Этот результат был обобщен на n-е степени Тростом. Позднее он был переоткрыт Анкени и

Роджерсом. Формулировка его такова: если сравнение $x^n \equiv a\ (p)$ разрешимо для почти всех простых чисел p, то $a = b^n$ при $8 \nmid n$ и $a = b^n$ или $a = 2^{n/2}b^n$ при $8 \mid n$. При помощи закона взаимности Эйзенштейна мы докажем часть этого результата, когда $n = l$ — нечетное простое число. См. также [211], [134] и замечания к гл. 5.

Теорема 4. *Предположим, что $a \in \mathbf{Z}$ и что $l \nmid a$, где l — нечетное простое число. Если сравнение $x^l \equiv a\ (p)$ разрешимо для всех, кроме конечного числа, простых чисел, то $a = b^l$.*

Доказательство. Эту теорему можно переформулировать следующим образом. Если a не является l-й степенью, то существует бесконечно много простых чисел p, для которых сравнение $x^l \equiv a\ (p)$ неразрешимо.

Предположим, что a не равно l-й степени в $\mathbf{Z}$. Пусть $aD_l = P_1^{a_1}P_2^{a_2} \dots P_n^{a_n}$ — разложение на простые идеалы для a в D_l. Мы утверждаем, что $l \nmid a_i$ по крайней мере для одного a_i. Чтобы убедиться в этом, положим $p_i\mathbf{Z} = P_i \cap \mathbf{Z}$. Так как $l \nmid a$, то $l \neq p_i$, так что p_i неразветвлено в D_l. Следовательно, $\operatorname{ord}_{P_i} a = \operatorname{ord}_{P_i} a = a_i$. Если бы $l \mid a_i$ при всех i, отсюда вытекало бы, что a есть l-я степень в $\mathbf{Z}$. Таким образом, можно считать, что $l \nmid a_n$.

Пусть $\{Q_1, Q_2, \dots, Q_k\}$ — какое-либо конечное множество простых идеалов Q_i, отличных от P_i и от $(1 - \zeta_l)$.

При помощи китайской теоремы об остатках мы можем найти такой элемент $\tau \in D_l$, что $\tau \equiv 1\ (Q_i)$ при $i = 1, 2, \dots, k$, $\tau \equiv 1\ (l)$, $\tau \equiv 1\ (P_j)$ для $j = 1, 2, \dots, n-1$ и $\tau \equiv \alpha\ (P_n)$, где α выбран так, что $(\alpha/P_n)_l = \zeta_l$.

Так как $\tau \equiv 1\ (l)$, то τ примарен. Таким образом, с одной стороны,

$$\left(\frac{a}{\tau}\right)_l = \left(\frac{\tau}{a}\right)_l = \prod \left(\frac{\tau}{P_i}\right)^{a_i} = \zeta_l^{a_n} \neq 1.$$

С другой стороны, пусть $(\tau) = R_1R_2 \dots R_m$ — разложение τ на простые идеалы. Тогда

$$\left(\frac{a}{\tau}\right)_l = \prod_j \left(\frac{a}{R_j}\right)_l.$$

Отсюда вытекает, что $(a/R_j)_l \neq 1$ при некотором j.

Из сравнений, которым удовлетворяет τ, непосредственно следует, что $R_j \notin \{Q_1, Q_2, \dots, Q_k\} \cup \{(1 - \zeta_l)\} \cup \{P_1, \dots, P_n\}$.

Мы показали, что существует бесконечно много простых идеалов Q, для которых сравнение $x^l \equiv a\ (Q)$ неразрешимо. Пусть $q\mathbf{Z} = Q \cap \mathbf{Z}$. Тогда $x^l \equiv a\ (q)$ неразрешимо и таких q существует

бесконечно много, ибо каждое рациональное простое число содержится лишь в конечном числе простых идеалов в D_l. □

Второе приложение закона взаимности Эйзенштейна, которое мы хотим изложить, относится к гипотезе Ферма. Эта гипотеза состоит в том, что если $n > 2$ — целое число, то не существует решения уравнения $x^n + y^n + z^n = 0$ в ненулевых целых числах. Захватывающая история этой гипотезы будет кратко изложена в следующей главе.

Легко видеть, что если гипотеза Ферма верна для n, то она верна и для любого кратного n. Так как любое целое число, большее чем 2, делится либо на 4, либо на нечетное простое число, мы можем ограничиться рассмотрением случаев $n = 4$ или $n = l$— нечетное простое число. Случай $n = 4$ был решен Эйлером [1]).

Если l — нечетное простое число, стало традиционным рассматривать два случая. Говорят, что рассматривается первый случай, если $x^l + y^l + z^l = 0$ и $l \nmid xyz$. Второй случай является отрицанием первого. В 1909 г. Виферих опубликовал следующий важный результат ([1166], т. 3).

Теорема 5. *Если уравнение $x^l + y^l + z^l = 0$ разрешимо в ненулевых целых числах с $l \nmid xyz$, то $2^{l-1} \equiv 1 \ (l^2)$.*

Было показано, что единственными двумя простыми числами, меньшими 3×10^9 и удовлетворяющими сравнению $2^{l-1} \equiv 1 \ (l)^2$, являются 1093 и 3511. Неизвестно, бесконечно ли много простых чисел такого типа.

В 1912 г. Фуртвенглер доказал теорему, которая содержит теорему 5 в виде следствия. А именно,

Теорема 6. *Пусть x, y и z — ненулевые попарно взаимно простые целые числа, для которых $x^l + y^l + z^l = 0$. Предположим, что $l \nmid xyz$. Пусть p — какой-либо простой делитель y. Тогда $p^{l-1} \equiv 1 \ (l^2)$.*

Как нетрудно убедиться, предположение о попарной взаимной простоте чисел x, y и z не приводит к потере общности.

Чтобы увидеть, как теорема 5 следует из теоремы 6, предположим, что $l \nmid xyz$. Поскольку $x^l + y^l + z^l = 0$, не все три числа x, y и z нечетные. По симметрии можно считать, что $2 \mid y$. В силу теоремы 6 $2^{l-1} \equiv 1 \ (l^2)$.

---

[1]) Для $n = 4$ уравнение следует, конечно, записать в виде $x^4 + y^4 - z^4 = 0$. — *Прим. перев.*

Мы приступаем к доказательству теоремы Фуртвенглера. Пусть $\zeta = \zeta_l$ — примитивный корень степени l из единицы. Тогда

$$(x + y)(x + \zeta y) \ldots (x + \zeta^{l-1} y) = (-z)^l. \qquad (*)$$

Лемма 1. *Предположим, что* $i \neq j$ *и* $0 \leqslant i, j < l$. *Тогда* $x + \zeta^i y$ *и* $x + \zeta^j y$ *взаимно просты в* D_l.

Доказательство. Предположим, что $A \subset D_l$ — некоторый идеал, содержащий $x + \zeta^i y$ и $x + \zeta^j y$. Тогда $(\zeta^j - \zeta^i)\, x$ и $(\zeta^j - \zeta^i)\, y$ принадлежат A. Так как x и y взаимно просты, отсюда следует, что $\zeta^j - \zeta^i$ лежит в A. Значит, $\lambda = 1 - \zeta \in A$. Так как (λ) — максимальный идеал, то либо $(\lambda) = A$, либо $A = D_l$. Если $(\lambda) = A$, то из равенства $(*)$ мы видим, что $(-z) \in (\lambda)$, откуда следует, что $z \in (\lambda)$ и $l \mid z$, вопреки предположению. Таким образом, $A = D_l$, и лемма доказана. □

Следствие. *Идеалы* $(x + \zeta^i y)$ *являются в точности* l*-ми степенями.*

Рассмотрим элемент $\alpha = (x + y)^{l-2}(x + \zeta y)$. Мы утверждаем, что

(i) Идеал (α) является точной l-й степенью.

(ii) $\alpha \equiv 1 - u\lambda\ (\lambda^2)$, где $u = (x + y)^{l-2} y$.

Свойство (i) получается из следствия леммы 1.

Для доказательства свойства (ii) заметим, что $x + \zeta y = x + y - y\lambda$. Таким образом,

$$\alpha = (x + y)^{l-1} - \lambda u.$$

Далее, $x^l + y^l + z^l \equiv x + y + z\ (l)$. Если $l \mid (x + y)$, то мы имели бы $l \mid z$, вопреки предположению. Поэтому $l \nmid (x + y)$ и $(x + y)^{l-1} \equiv 1\ (l)$. Отсюда и следует свойство (ii).

Рассмотрим $\zeta^{-u}\alpha$. Мы имеем

$$\zeta^{-u}\alpha = (1 - \lambda)^{-u}\alpha \equiv (1 + u\lambda)(1 - u\lambda)\ (\lambda^2) \equiv 1\ (\lambda^2).$$

Отсюда следует, что $\zeta^{-u}\alpha$ примарно. По закону взаимности Эйзенштейна

$$\left(\frac{p}{\zeta^{-u}\alpha}\right)_l = \left(\frac{\zeta^{-u}\alpha}{p}\right)_l = \left(\frac{\zeta}{p}\right)_l^{-u} \left(\frac{\alpha}{p}\right)_l. \qquad (**)$$

Поскольку идеал $(\zeta^{-u}\alpha) = (\alpha)$ равен l-й степени, левая часть в $(**)$ равна 1.

Так как $p \mid y$, то $\alpha \equiv (x + y)^{l-1}\ (p)$. Таким образом,

$$\left(\frac{\alpha}{p}\right)_l = \left(\frac{(x+y)^{l-1}}{p}\right)_l = \left(\frac{p}{(x+y)^{l-1}}\right)_l = 1,$$

ибо идеал $(x + y)$ равен l-й степени.

Из (**) теперь следует, что $(\zeta/p)_l^u = 1$. Для завершения доказательства мы должны вычислить $(\zeta/p)_l$.

Пусть $pD_l = P_1P_2 \dots P_g$ — разложение на простые идеалы для p в D_l. Мы знаем, что $NP_i = p^f$ и, так как $p \neq l$, то $e = 1$, а потому $gf = l - 1$.

По следствию предложения 14.2.2

$$\left(\frac{\zeta}{p}\right)_l = \prod_i \left(\frac{\zeta}{P_i}\right)_l = \prod_i \zeta^{(p^f-1)/l} = \zeta^{g[(p^f-1)/l]}.$$

Соотношение $(\zeta/p)_l^u = 1$ приводит теперь к сравнению

$$ug\frac{p^f-1}{l} \equiv 0 \ (l).$$

Поскольку $g \mid l-1$, то $l \nmid g$. Так как $u = (x+y)^{l-2}y$, то $l \nmid u$. Таким образом,

$$\frac{p^f-1}{l} \equiv 0 \ (l), \text{ или } p^f \equiv 1 \ (l^2).$$

Теорема 6 следует отсюда, ибо $f \mid l-1$. □

Мы закончим приложением теоремы 2, которое относится к структуре группы классов идеалов поля $\mathbf{Q}(\sqrt{-l})$, где $l > 3$ — простое число, $l \equiv 3 \ (4)$. Пусть p — некоторое нечетное простое число, $p \equiv 1 \ (l)$. Тогда, поскольку p полностью разлагается в $\mathbf{Q}(\zeta_l)$, оно полностью разлагается в $\mathbf{Q}(\sqrt{-l})$ (почему?). В этом можно убедиться также, заметив, что

$$(-l/p) = (-1)^{(p-1)/2}(p/l)(-1)^{((p-1)/2)((l-1)/2)} = (p/l) = 1,$$

и применив предложение 13.1.3. В кольце целых чисел D поля $\mathbf{Q}(\sqrt{-l})$ запишем $p = \mathfrak{P}\overline{\mathfrak{P}}$. Если $\tilde{D}$ обозначает кольцо целых чисел в $\mathbf{Q}(\zeta_l)$, то справедлива

Лемма 2. $\mathfrak{P}\tilde{D} = \prod P^{\sigma_s}$, *где* P — *простой идеал кольца* $\tilde{D}$, $P \cap D = \mathfrak{P}$ *и* s *пробегает ненулевые квадраты по модулю* l.

Доказательство. Множество элементов σ_s в утверждении леммы образует группу Галуа поля $\mathbf{Q}(\zeta_l)$ над $\mathbf{Q}(\sqrt{-l})$. Так как $p\tilde{D} = P^{\sum_{t=1}^{l-1}\sigma_t}$ и $\sigma_n(\mathfrak{P}) = \overline{\mathfrak{P}}$ для неквадрата n по модулю l, то $\mathfrak{P}\tilde{D}$ делится точно на $\sigma_s(P)$, с показателем степени 1. □

По теореме 2 $(g(P)^l) = P^{\sum t\sigma_t^{-1}}$, $t = 1, 2, \ldots, l-1$. Возведение в символическую степень $\sum\sigma_s$, s — квадрат по модулю l, приводит к равенствам

$$(\alpha)\,\tilde{D} = \mathfrak{P}^{\sum t\sigma_t^{-1}}\cdot\tilde{D} = \mathfrak{P}^{\sum s}\cdot\bar{\mathfrak{P}}^{\sum n}\cdot\tilde{D},$$

где $\alpha \in D$ и n пробегает неквадраты по модулю l в интервале $[1, l-1]$. Положим $R = \sum s$, $N = \sum n$. Из упр. 34 гл. 12 следует, что $\alpha D = \mathfrak{P}^R\bar{\mathfrak{P}}^N$. Если $[\mathfrak{A}]$ обозначает класс эквивалентности идеала $\mathfrak{A}$ и 1 — единичный класс, то $[\mathfrak{P}]^{-1} = [\bar{\mathfrak{P}}]$. Таким образом, $[\mathfrak{P}]^{N-R} = 1$. С другой стороны, если $1 \leqslant r \leqslant l-1$, то из упр. 7 (или леммы 3 § 3 гл. 15) получаем $g(P)^{\sigma_r - r} = \beta$ при некотором $\beta \in \tilde{D}$. Возведение в степень l, использование теоремы 2 и применение $\sum\sigma_s$ приводят, когда r — квадрат, к равенству $(\mathfrak{P}^R\bar{\mathfrak{P}}^N)^{r-1}\,\tilde{D} = (\gamma)^l\,\tilde{D}$ для некоторого $\gamma \in D$. Отсюда следует, что $([\mathfrak{P}]^{(N-R)/l})^{r-1} = 1$ (нетрудно показать, что $l \mid N$ и $l \mid R$). Но из предыдущих рассмотрений вытекало, что $([\mathfrak{P}]^{(N-R)/l})^l = 1$. Так как $(r-1, l) = 1$, мы доказали следующий результат.

Предложение 14.6.1. *Пусть $\mathfrak{P}$ — какой-либо простой идеал степени 1 в $\mathbf{Q}(\sqrt{-l})$ для простого числа $l > 3$, $l \equiv 3\ (4)$. Тогда $[\mathfrak{P}]^{(N-R)/l} = 1$.*

Если тот факт, что $(N-R)/l$ — целое число, элементарен, то отнюдь не очевидно, что это число положительно. Все известные доказательства положительности используют математический анализ [1]). Мы приведем короткое доказательство, принадлежащее Мозеру, в упражнениях к гл. 16. Другие доказательства положительности, как и многие иные интересные результаты этого типа, см. в статье [94]. Как упомянуто в гл. 13, оказывается, что $(N-R)/l$ на самом деле есть число классов поля $\mathbf{Q}(\sqrt{-l})$, но доказательство опять аналитическое. В случае когда при прямом вычислении $N - R = l$, $\mathfrak{P}$ будет главным идеалом. Если предположить (что можно доказать), что каждый класс идеалов содержит некоторый простой идеал степени 1, то отсюда можно заключить, что для таких l кольцо целых поля $\mathbf{Q}(\sqrt{-l})$ является областью с однозначным разложением на множители. Таким способом проверяется, что у мнимых квадратичных полей с дискриминантом -7, -11, -19, -43, -67, -163 число классов равно 1. Опять ссылаясь на предложение 14.6.1, получаем $\mathfrak{P}^{(N-R)/l} = (\alpha)$, где $(\alpha) = (x + \sqrt{-l}y)/2$; $x, y \in \mathbf{Z}$. Взятие норм приводит к следующему интересному следствию.

[1]) Чисто арифметическое доказательство для $l \not\equiv 7\ (8)$ было дано в 1927 г. Б. А. Венковым (см. [10*], гл. VI, § 4). — *Прим. ред.*

Следствие. *Если* $p \equiv 1\ (l)$, $l \equiv 3\ (4)$, $l > 3$, *то* $4p^{(N-R)/l} = x^2 + ly^2$ *с* $x, y \in \mathbf{Z}$.

Замечания

В своей статье (1890 г.) [224] шведский математик Людвиг Штикельбергер (1850—1936) (см. [148]) нашел разложение на простые идеалы гауссовой суммы, соответствующей произвольному мультипликативному характеру, определенному над конечным полем (теорема 2 этой главы). На самом деле он доказал более точный результат, а именно, если воспользоваться обозначением этой главы,

$$g_a \equiv \frac{-(-\lambda)^{S(a)}}{a_0!\, a_1! \ldots a_{f-1}!}\ (\mathfrak{P}^{S(a)+1}).$$

Из этого, конечно, следует теорема 2. Частный случай этой теоремы, когда m — простое число и $p \equiv 1\ (m)$, был уже доказан Куммером в 1847 г. Интересно отметить, что Куммер получил свой результат при помощи разложения в $\mathbf{Q}(\zeta_m)$ определенных сумм Якоби, что стало возможно, в свою очередь, благодаря сравнению $J(\bar{\omega}^m, \bar{\omega}^n) \equiv -[(m+n)!/n!m!]\ (P)$, известному Якоби, Эйзенштейну и Коши. (См. [164], т. 1, с. 361—364, 448—453 и упр. 1 и 2.) Изящное доказательство результата Куммера можно найти также в работе Гильберта [151] (теорема 135), где суммы Якоби не используются, но применяются рассуждения, использующие ветвления. Этот частный случай теоремы Штикельбергера был недостающим звеном в программе получения высших законов взаимности, начатой Гауссом, Эйзенштейном и Якоби. В самом деле, в 1850 г. Эйзенштейн [132] опубликовал свое доказательство закона взаимности, носящего его имя (теорема 1), в котором использовался относительно новый тогда язык идеальных чисел, введенный в рассмотрение Куммером. Полное доказательство можно также найти в [166] (т. 3), а также у Гильберта в [151] (теорема 140), где для преодоления ограничения $p \equiv 1\ (l)$ последний использует конечность числа классов в $\mathbf{Q}(\zeta_l)$! Гильберт рассматривает закон Эйзенштейна в качестве необходимой леммы для закона взаимности Куммера. Приводимое нами доказательство теоремы 2 следует доказательству из важной статьи [23] (см. также гл. 7 в [160]), в то время как получение закона Эйзенштейна из теоремы Куммера тесно примыкает к трактовке Вейля в его первоклассном историческом очерке [238]. Эта статья Вейля вместе с его рецензией [239] на «Mathematische Werke» Эйзенштейна и его введением к собранию статей Куммера [164] детально и с проникновением в суть дела освещает историю усилий Якоби, Эйзенштейна и Куммера по доказательству законов взаимности высших степеней при помощи сумм Гаусса. В данной книге мы проследили

это развитие событий вплоть до работы Эйзенштейна. Последующее развитие приводит к исследованиям Куммера, Гильберта, Фуртвенглера и Такаги и в конечном счете к знаменитому закону взаимности Артина. Историю этих событий см. в [158] и [110]. Интересное и, пожалуй, более элементарное обсуждение природы законов взаимности см. в [246].

Использование теоремы 2 для того, чтобы показать, что группа классов идеалов поля $\mathbf{Q}(\sqrt{-l})$, $l \equiv 3$ (4), аннулируется $(1/l)\sum_{x=1}^{l-1} x(x/l)$, восходит к Куммеру и появляется как теорема 145 в [151] Гильберта. Следствие предложения 14.6.1 было первоначально отмечено Якоби, который на его основе высказал гипотезу о формуле для числа классов поля $\mathbf{Q}(\sqrt{-l})$. (См. также замечание Вейля в [238], с. 252—253.) В упомянутой выше статье Штикельбергер возвращается к этому приложению круговых полей к арифметике квадратичных форм и получает аналогичные результаты для $\mathbf{Q}(\sqrt{-m})$ при произвольном m.

Имеются и другие приложения теоремы 1 к последней теореме Ферма. Например, в широко известном результате Мириманова утверждается, что если x, y и z — целые числа, для которых $x^p + y^p + z^p = 0$, $p \nmid xyz$, то $3^{p-1} \equiv 1\ (p^2)$ (см. теорему 1041 из [166]). Вандивер также показал, используя аналогичные методы, что если $x^p + y^p + z^p = 0$, $(x, y, z) = 1$, $p > 3$, то $x^p \equiv x\ (p^3)$, $y^p \equiv y\ (p^3)$, $z^p \equiv z\ (p^3)$ ([166], теорема 1046). Дальнейшие результаты по последней теореме Ферма, которые используют закон взаимности Эйзенштейна, см. в лекции 9 прекрасной книги [206].

Упражнения

Во всех упражнениях обозначения такие же, как и в этой главе.

1. Показать, что если $1 \leqslant n < q-1$, $1 \leqslant m < q-1$, то

(a) $J(\omega^{-n}, \omega^{-m}) \equiv -[(m+n)!/n!\,m!]\ (P)$;

(b) если $1 < a < q-1$, $a = a_0 + a_1 p + \cdots + a_{f-1}p^{f-1}$, то $J(\omega^{-1}, \omega^{-(a-1)}) \equiv a_0\ (P)$.

2. В доказательстве теоремы 2 мы показали, что $g_1 \equiv \lambda_p\ (\mathfrak{P}^2)$.

(a) Если $1 \leqslant a < p-1$, то показать, что $g_a \equiv (-1)^{a+1}\lambda_p^a/a!\ (\mathfrak{P}^{a+1})$, где $\alpha \equiv \beta\ (\mathfrak{P}^n)$ означает, что $\operatorname{ord}_{\mathfrak{P}}(\alpha - \beta) \geqslant n$.

(b) Если сравнение Штикельбергера $g_a \equiv (-1)^{a+S(a)}\lambda_p^{S(a)}/a_0!\ a_1! \ldots a_{f-1}!\ (\mathfrak{P}^{1+S(a)})$ выполняется для некоторого a, $1 \leqslant a < q-1$ и $pa < q-1$, то показать, что оно выполняется также для g_{pa}.

(c) Получить общее сравнение Штикельбергера.

3. Показать, что если $m > 2$, то $g(P)\,p^{-1/2}$ — не целое алгебраическое число (см. также [113]).

4. Пусть r и s — положительные целые числа и $m \nmid r+s$. Показать, что $\left(J(\chi_p^r, \chi_p^s)\right) = P^{\alpha}$, где $\alpha = \sum (\langle rt/m\rangle + \langle st/m\rangle - \langle [(r+s)\,t]/m\rangle)\,\sigma_t^{-1}$, причем сумма берется по t, $1 \leqslant t < m$, $(t, m) = 1$.

5. Проверить, что рассуждение в § 4, показывающее, что $g_1 \equiv \lambda_p \ (\mathcal{P}^2)$, проходит для $p = 2$, m нечетное.

6. Если $(r, pm) = 1$, $1 \leqslant r < pm$, то $g(P)^{\sigma_r - r} \in \mathbf{Q}(\zeta_m)$.

7. Проверить лемму 1 из § 5.

8. Пусть $p \equiv 1 \ (m)$, где m — простое число. Не используя упр. 4, показать, что $J(\chi, \chi^k)$, $1 \leqslant k \leqslant p-2$, является произведением различных простых идеалов с показателями степени 1. Используя упр. 1, найти разложение $J(\chi, \chi^k)$ и воспользоваться предложением 8.3.3 для получения прямого доказательства теоремы 2 в этом случае (Куммер).

9. Пусть K/F — нормальное расширение с циклической группой Галуа порядка p и образующим элементом σ. Для $x \in K$ положим $f(x) = 1 + x + x\sigma(x) + \cdots + x\sigma(x) \ldots \sigma^{p-3}(x)$. Пусть p — простое число, $F = \mathbf{Q}(\zeta_{p-1})$, $K = \mathbf{Q}(\zeta_p, \zeta_{p-1})$. Показать, что

$$g(\chi) = \sum_{x=1}^{p-1} \chi(x)\, \zeta_p^x = \zeta_p f\left(\zeta_{p-1}\zeta_p^{t-1}\right),$$

где t — примитивный корень по модулю p, $\chi(t) = \zeta_{p-1}$ и σ — автоморфизм поля K/F, для которого $\sigma(\zeta_{p-1}) = \zeta_{p-1}$ и $\sigma(\zeta_p) = \zeta_p^t$. Сделать отсюда вывод о том, что сумма Гаусса — прадедушка теории когомологий (Куммер [164], с. 10).

10. С помощью теоремы 2 показать, что $\mathbf{Q}(g(P)^m)$ — инвариантное подполе для группы разложения p, известное также как поле разложения для p.

11. Для простого числа l и положительных целых чисел r, s и t, удовлетворяющих равенству $r + s + t = l$, положим $H_{r,s,t} = \{h \mid h \in F_l^*,\ \widetilde{hr} + \widetilde{hs} + \widetilde{ht} = l\}$, где $\widetilde{a}$ *обозначает наименьший неотрицательный вычет для* a по модулю l. Показать, что $H_{r,s,t}$ есть множество представителей классов по подгруппе порядка 2 в F_l^*.

12. Рассмотрим кривую Γ над F_p, определенную уравнением $y^l = x^r(1-x)^s$ (обозначения те же, что и в упр. 11).

(a) Показать, что дзета-функция кривой Γ может быть записана в виде

$$z(u) = g(u)/(1-u)(1-pu),$$

где

$$g(u) = \prod_P \left(1 + J\left(\bar{\chi}_P^r, \bar{\chi}_P^s\right) u^f\right),$$

причем P пробегает простые идеалы в $\mathbf{Q}(\zeta_l)$ над p и обозначения те же, что и в основном тексте, т. е. $\bar{\chi}_P$ — символ вычета степени l.

(b) Показать, что $\left(J\left(\bar{\chi}_P^r, \bar{\chi}_P^s\right)\right) = P^{\sum \sigma_k^{-1}}$, где $k \in H_{r,s,t}$.

(c) Показать, то если порядок p по модулю l (т. е. f) четен, то комплексное сопряжение лежит в группе разложения идеала P.

(d) Если f четно, то $\left(J\left(\bar{\chi}_P^r, \bar{\chi}_P^s\right)\right) = (p^{f/2})$.

(e) $J\left(\bar{\chi}_P^r, \bar{\chi}_P^s\right) = up^{f/2}$, где u — корень степени l из единицы.

(f) Показать, что $u = 1$.

(Упражнения 11 и 12 взяты из статьи [142].)

13. Пусть l — простое число и $\chi \neq \varepsilon$ — мультипликативный характер поля F_l. Положим

$$B_\chi = (1/l) \sum_{a=1}^{l-1} a\chi(a).$$

Рассмотрим элементы группового кольца группы Галуа G поля $\mathbf{Q}(\zeta_l)/\mathbf{Q}$ с коэффициентами в $\mathbf{Q}(\zeta_l)$, определенные равенствами

$$\varepsilon_\chi = (1/(l-1)) \sum_{a=1}^{l-1} \chi(a)^{-1}\sigma_a,$$

$$\theta = (1/l) \sum_{t=1}^{l-1} t\sigma_t^{-1},$$

где $\sigma_a(\zeta_l) = \zeta_l^a$. Показать, что

(a) $\varepsilon_\chi(\zeta_l)\,\varepsilon_{\chi^{-1}}(\zeta_l) = \chi(-1)\,(l-1)^{-2}l$;

(b) $-l = (1-\zeta_l)\left(\zeta_l + 2\zeta_l^2 + \cdots + (l-1)\,\zeta_l^{l-1}\right)$;

(c) $\varepsilon_\chi(-\zeta_l/(1-\zeta_l)) = B_\chi \varepsilon_\chi(\zeta_l)$;

(d) $\theta\varepsilon_\chi = -B_{\chi^{-1}}\varepsilon_\chi$, где мы полагаем

$$\left(\sum_{t=1}^{l-1} a_t\sigma_t\right)\left(\sum_{t=1}^{l-1} b_t\sigma_t\right) = \sum_{t=1}^{l-1} c_t\sigma_t,$$

причем $c_t = \sum_{uv \equiv t\ (l)} a_u b_v$, $1 \leqslant u, v < l$.

(Это упражнение взято из [157], с. 115—117.)

14. Пусть p и l — простые числа, $l > 3$. Если $p \neq l$ и $\alpha \in \mathbf{Z}[\zeta_l]$ вещественно, $(\alpha, l) = 1$, то показать, что $(\alpha/p)_l = 1$.

15. Пусть $p \neq l$ — простые числа, $l > 3$. Показать, что

(a) $(\zeta_l/p)_l = \zeta_l^{((l-1)/f)\,(p^f-1)/l)}$, где f — порядок p по модулю l;

(b) $(\zeta_l/p)_l = 1$ означает, что $p^{l-1} \equiv 1\ (l^2)$.

16. Прочитать теоремы 1039 и 1041 в [166], т. 3.

17. Пусть $m = l$ — нечетное простое число и $\mathscr{L}$ — простой идеал в $\mathbf{Q}(\zeta_p)$, содержащий $(1-\zeta_l)$. Показать, что

(a) $g(P) = -1\ (1-\zeta_l)$;

(b) $g(P) = -1 + c(1-\zeta_l)\ (\mathscr{L}^2)$ с $c \in \mathbf{Z}[\zeta_p]$;

(c) $(-g(P))^{\sigma_t} = (-g(P))^t\ (\mathscr{L}^2)$ для $(t, l) = 1$ и такого автоморфизма σ_t поля $\mathbf{Q}(\zeta_{pl})$, что $\sigma_t(\zeta_p) = \zeta_p$ и $\sigma_t(\zeta_l) = \zeta_l^t$;

(d) $g(P)^{\sigma_t - t} = (-1)^{t+1}\left((1-\zeta_l)^2\right)$;

(e) если $1 \leqslant a, b < l$, $l \nmid a+b$, то $J(\chi_P^a, \chi_P^b) = -1\ \left((1-\zeta_l)^2\right)$.

(Это упражнение взято из [156].)

Глава 15

ЧИСЛА БЕРНУЛЛИ

В этой главе мы введем важную последовательность рациональных чисел, открытую Якобом Бернулли (1654—1705) и обсуждаемую им в его посмертно изданной работе «Ars Conjectandi» (1713 г.). *Эти числа, называемые теперь числами Бернулли, появляются во многих областях математики. В первом параграфе мы приводим их определение и обсуждаем связи с тремя классическими проблемами. В следующем параграфе рассматриваются различные арифметические свойства чисел Бернулли, включая теорему Клауссена — фон Штаудта и сравнения Куммера. Первый из этих результатов определяет знаменатели чисел Бернулли, в то время как второй дает информацию об их числителях. В последнем параграфе мы доказываем теорему Хербранда, которая связывает числа Бернулли со структурой группы классов идеалов поля* $\mathbf{Q}(\zeta_p)$. *Материал этого параграфа довольно сложен, но мы его все же включили ввиду того, что он позволяет получить красивое и важное приложение соотношения Штикельбергера, которое доказано в последней главе.*

§ 1. Числа Бернулли; определения и приложения

Мы начнем с обсуждения трех проблем, каждая из которых представляет исторический интерес.

Первая проблема относится к нахождению формул для суммирования k-х степеней первых n чисел. Якоб Бернулли знал о следующих фактах:

$$1 + 2 + 3 + \cdots + (n-1) = \frac{n(n-1)}{2},$$

$$1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 = \frac{n(n-1)(2n-1)}{6},$$

$$1^3 + 2^3 + 3^3 + \cdots + (n-1)^3 = \frac{n^2(n-1)^2}{4},$$

а также и о соответствующих (менее известных) формулах для показателей степеней вплоть до 10. Для каждого показателя степени k сумма $1^k + 2^k + \ldots + (n-1)^k$ оказывается многочленом от n степени $k+1$. Для нахождения коэффициентов этих много-

членов при произвольном k Бернулли и потребовалось определить числа, которые носят его имя. Ему удалось полностью решить первоначальную проблему и он гордо замечает (в своей книге «Ars Conjectandi»), что менее чем за половину четверти часа он смог просуммировать десятые степени первой тысячи целых чисел [220].

Другая знаменитая проблема этого времени состояла в вычислении суммы

$$\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \cdots$$

и вообще $\zeta(2m)$, где

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

— дзета-функция Римана. После долгих усилий Эйлер показал в 1734 г., что $\zeta(2) = \pi^2/6$. Впоследствии он определил $\zeta(2m)$ при всех положительных целых числах m.

Третья проблема — это знаменитая последняя теорема Ферма. Ферма утверждал, что уравнение $x^n + y^n = z^n$ не имеет решений в положительных целых числах при целом $n > 2$. В общем виде это утверждение никогда не было доказано. Нетрудно убедиться в том, что его достаточно доказать в случаях, когда $n = p$ — нечетное простое число и $n = 4$. В 1847 г. Куммер доказал теорему Ферма для некоторого множества простых чисел, называемых регулярными. Простое число p называется *регулярным*, если оно не делит число классов поля $\mathbf{Q}(\zeta_p)$. Кроме того, Куммер открыл красивый и элементарный критерий регулярности, в котором используются свойства делимости первых $(p-3)/2$ ненулевых чисел Бернулли.

Мы по очереди обсудим эти три проблемы.

Положим $S_m(n) = 1^m + 2^m + \ldots + (n-1)^m$. Приведем сначала простой индуктивный способ вычисления этих сумм. Из формулы бинома следует, что

$$(k+1)^{m+1} - k^{m+1} = 1 + \binom{m+1}{1} k + \binom{m+1}{2} k^2 + \cdots + \binom{m+1}{m} k^m.$$

Подставляем в это равенство $k = 0, 1, 2, \ldots, n-1$ и складываем. В результате получим

$$n^{m+1} = n + \binom{m+1}{1} S_1(n) + \binom{m+1}{2} S_2(n) + \cdots + \binom{m+1}{m} S_m(n). \quad (1)$$

Если имеются формулы для $S_1(n)$, $S_2(n)$, ..., $S_{m-1}(n)$, то равенство (1) позволяет найти формулу для $S_m(n)$. Бернулли заметил, что $S_m(n)$ — многочлен степени $m+1$ от n со старшим членом $n^{m+1}/(m+1)$. Это нетрудно получить по индукции из равенства (1). Кроме того, свободный член всегда равен нулю. Значе-

ния других коэффициентов менее очевидны. Прямым вычислением находим, что коэффициент при n равен $-1/2$, $1/6$, 0, $-1/30$, 0, $1/42$, 0, $-1/30$, 0, $5/66$ для $m = 1, 2, \ldots, 10$. Дальнейшие наблюдения вида этих формул привели Бернулли к следующему определению и теореме.

Определение. Последовательность чисел B_0, B_1, B_2, ..., чисел *Бернулли*, определяется по индукции следующим образом. $B_0 = 1$; если B_0, B_1, ..., B_{m-1} уже определены, то B_m определяется формулой

$$(m+1)B_m = -\sum_{k=0}^{m-1} \binom{m+1}{k} B_k. \tag{2}$$

Выписывая эти равенства, получаем последовательность линейных уравнений

$$\begin{aligned} &1 + 2B_1 = 0,\\ &1 + 3B_1 + 3B_2 = 0,\\ &1 + 4B_1 + 6B_2 + 4B_3 = 0,\\ &1 + 5B_1 + 10B_2 + 10B_3 + 5B_4 = 0. \end{aligned}$$

Отсюда находим $B_1 = -1/2$, $B_2 = 1/6$, $B_3 = 0$, $B_4 = -1/30$, $B_5 = 0$, $B_6 = 1/42$, ... и т. д. Мы докажем позже, что знаки ненулевых чисел Бернулли чередуются. Кроме того, мы убедимся, что числа Бернулли с нечетным индексом, большим 1, равны нулю.

Лемма 1. *Разложим функцию $t/(e^t - 1)$ в степенной ряд около начала координат следующим образом:*

$$t/(e^t - 1) = \sum_{m=0}^{\infty} b_m (t^m/m!).$$

Тогда $b_m = B_m$ для всех m.

Доказательство. Умножим обе части рассматриваемого равенства на $e^t - 1$:

$$t = \sum_{n=1}^{\infty} \frac{t^n}{n!} \sum_{m=0}^{\infty} b_m \frac{t^m}{m!}.$$

Приравнивание коэффициентов при t^{m+1} дает $1 = b_0$ для $m = 0$ и

$$\sum_{k=0}^{m} \binom{m+1}{k} b_k = 0$$

в общем случае. Это совпадает с системой равенств (2), определяющих числа Бернулли. Так как $B_0 = b_0 = 1$, отсюда следует, что $B_m = b_m$ при всех m. □

Мы дадим теперь ответ, полученный Бернулли, на вопрос о вычислении сумм $S_m(n)$.

Теорема 1. *Для $m \geqslant 1$ суммы $S_m(n)$ удовлетворяют равенству*

$$(m+1)\,S_m(n) = \sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m+1-k}.$$

Доказательство. Подставляя в равенство

$$e^{kt} = \sum_{m=0}^{\infty} k^m (t^m/m!)$$

значения $k = 0, 1, 2, \ldots, n-1$ и складывая, получаем

$$1 + e^t + e^{2t} + \cdots + e^{(n-1)t} = \sum_{m=0}^{\infty} S_m(n) \frac{t^m}{m!}. \tag{3}$$

Левая часть равна

$$\frac{e^{nt}-1}{e^t-1} = \frac{e^{nt}-1}{t} \frac{t}{e^t-1} = \sum_{k=1}^{\infty} n^k \frac{t^{k-1}}{k!} \sum_{j=0}^{\infty} B_j \frac{t^j}{j!}.$$

Приравнивая коэффициенты при t^m в правых частях равенства (3) и последнего равенства и умножая на $(m+1)!$, получаем доказываемый результат. □

Утверждение теоремы 1 можно переформулировать, введя важный класс многочленов, называемых *многочленами Бернулли*. По определению

$$B_m(x) = \sum_{k=0}^{m} \binom{m}{k} B_k x^{m-k}.$$

Таким образом, $B_1(x) = x - 1/2$, $B_2(x) = x^2 - x + 1/6$ и т. д. Тогда теорема 1 формулируется в таком виде:

$$S_m(n) = \frac{1}{m+1}(B_{m+1}(n) - B_{m+1}).$$

Заметим, между прочим, что лемма 1 приводит к простому доказательству того факта, что $B_{2k+1} = 0$ для $k \geqslant 1$. Так как $B_1 = -1/2$, то

$$\frac{t}{e^t-1} + \frac{t}{2} = 1 + \sum_{k=2}^{\infty} B_k \frac{t^k}{k!}.$$

Левая часть этого равенства совпадает с $(t/2)\,((e^t+1)/(e^t-1))$, а это выражение не меняется при замене t на $-t$, т. е. оно есть четная функция от t. Значит, коэффициенты при нечетных степенях t в правой части равны нулю.

Мы переходим теперь к рассмотрению связи между числами Бернулли и числами $\zeta(2m)$ при $m = 1, 2, 3, \ldots$. Следующий результат принадлежит Эйлеру и является одним из его самых замечательных вычислений. По поводу истории этого результата и его связи с функциональным уравнением для дзета-функции Римана читателю следует посмотреть статью [88].

Теорема 2. *Для положительного целого числа m*

$$2\zeta(2m) = (-1)^{m+1}\frac{(2\pi)^{2m}}{(2m)!}B_{2m}.$$

Доказательство. При доказательстве этого результата нам понадобится один факт из классического анализа. А именно, мы воспользуемся разложением на простейшие дроби функции $\operatorname{ctg} x$:

$$\operatorname{ctg} x = \frac{1}{x} - 2\sum_{n=1}^{\infty}\frac{x}{n^2\pi^2 - x^2}. \tag{4}$$

Имеется несколько способов получения этого разложения. Пожалуй, простейший путь — подставить $t = 1$ в разложение Фурье для $\cos \alpha t$. Оно получается также взятием логарифмической производной от разложения в бесконечное произведение функции $\sin x$:

$$\sin x = x\prod_{n=1}^{\infty}\left(1 - \frac{x^2}{n^2\pi^2}\right).$$

Это стандартный результат из курса теории функций комплексной переменной, но можно дать и совершенно элементарное его доказательство (см. гл. 2 из [162]).

Воспользовавшись формулой для геометрической прогрессии, можно разложить правую часть равенства (4) в степенной ряд около 0:

$$x\operatorname{ctg} x = 1 - 2\sum_{m=1}^{\infty}\zeta(2m)\frac{x^m}{\pi^{2m}}. \tag{5}$$

Левую же часть в (5) мы разложим в ряд другим способом. Напомним, что

$$\cos x = \frac{e^{ix}+e^{-ix}}{2} \quad \text{и} \quad \sin x = \frac{e^{ix}-e^{-ix}}{2i}.$$

Из этих выражений получаем

$$x \operatorname{ctg} x = ix + \frac{2ix}{e^{2ix} - 1} = 1 + \sum_{n=2}^{\infty} B_n \frac{(2ix)^n}{n!}. \tag{6}$$

Сравнение коэффициентов при x^{2m} в правых частях равенств (5) и (6) приводит к соотношению

$$-\frac{2}{\pi^{2m}} \zeta(2m) = (-1)^m \frac{2^{2m}}{(2m)!} B_{2m}.$$

Это и есть результат Эйлера. □

В качестве примеров рассмотрим $m = 1$, 2 и 3. Так как $B_2 = 1/6$, $B_4 = -1/30$ и $B_6 = 1/42$, то $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90$ и $\zeta(6) = \pi^6/945$.

Следствием теоремы 2 является тот факт, что $(-1)^{m+1} B_{2m} > 0$ при $m \geqslant 1$, ибо $\zeta(2m)$ — положительное вещественное число при таких m. Таким образом, числа Бернулли с четными индексами не равны нулю и последовательно меняют свой знак.

Теорема 2 дает возможность также оценить рост B_{2m}. А именно,

$$|B_{2m}| > \frac{2(2m)!}{(2\pi)^{2m}}. \tag{7}$$

Здесь мы воспользовались простым наблюдением, что $\zeta(2m) \geqslant 1$. Из очевидного неравенства $e^n > n^n/n!$ (см. разложение в ряд для e^n) получаем

$$|B_{2m}| > 2\left(\frac{m}{\pi e}\right)^{2m}. \tag{8}$$

Это показывает, что числа Бернулли с четными индексами растут очень быстро. Следствие, которое нам понадобится позже, состоит в том, что $|B_{2n}/2n| \to \infty$ при $n \to \infty$.

Мы объединяем полученные выше свойства чисел Бернулли в следующем предложении.

Предложение 15.1.1.
(a) *Для нечетного* $k > 1$ *имеем* $B_k = 0$.
(b) $(-1)^{m+1} B_{2m} > 0$ *при* $m = 1, 2, \ldots$.
(c) $|B_{2m}/2m| \to \infty$ *при* $m \to \infty$.

Третья проблема, обсуждаемая в этом параграфе, относится к связи между числами Бернулли и уравнением Ферма $x^p + y^p = z^p$. Это обсуждение будет чисто обзорным, ибо результат Куммера очень глубокий и требует знакомства с аналитической техникой, которой мы не развивали. Несмотря на это, мы введем важное понятие регулярного простого числа и выпишем сравнение

Клаусcена — фон Штаудта, которое будет доказано в следующем параграфе. Мы начнем с введения понятия p-целого числа.

Пусть p — некоторое простое число. Рациональное число $r \in \mathbf{Q}$ называется *p-целым*, если $\operatorname{ord}_p(r) \geqslant 0$. Другими словами, r будет p-целым, если $r = a/b$, $a, b \in \mathbf{Z}$ и $p \nmid b$. Говорят также, допуская небольшую нестрогость, что *p не делит знаменатель в r*. Важное замечание состоит в том, что множество p-целых чисел образует кольцо. Обозначим это кольцо через $\mathbf{Z}_p$. Если r и s принадлежит $\mathbf{Z}_p$ то будем писать $r \equiv s\ (p^n)$, если $\operatorname{ord}_p(r - s) \geqslant n$, или, что эквивалентно, если $r - s = a/b$, $p \nmid b$ и $p^n \nmid a$, $a, b \in \mathbf{Z}$. Следующая теорема, доказанная независимо Клаусcеном и фон Штаудтом, описывает знаменатель числа B_{2m}. Столь же полное описание простых делителей числителя неизвестно.

Теорема 3. *Для $m \geqslant 1$*

$$B_{2m} = A_{2m} - \sum_{p-1 \mid 2m} \frac{1}{p},$$

где $A_{2m} \in \mathbf{Z}$ и сумма берется по всем простым числам p, таким, что $p - 1 \mid 2m$.

Следствие. *Если $p - 1 \nmid 2m$, то B_{2m} будет p-целым. Если $p - 1 \mid 2m$, то $pB_{2m} + 1$ будет p-целым. Более точно, если $p - 1 \mid 2m$, то*

$$\operatorname{ord}(pB_{2m} + 1) = \operatorname{ord} p\left(B_{2m} + \frac{1}{p}\right) = 1 + \operatorname{ord}\left(B_{2m} + \frac{1}{p}\right) \geqslant 1,$$

так что $pB_{2m} \equiv -1\ (p)$. Наконец, заметим, что 6 всегда делит знаменатели чисел B_{2m}, $m \geqslant 1$, так как $2 - 1$ и $3 - 1$ делят 2.

Куммер ввел понятие простого регулярного числа следующим образом.

Определение. Нечетное простое число $p \in \mathbf{Z}$ называется *регулярным*, если p не делит числитель ни одного из чисел $B_2, B_4, \ldots, B_{p-3}$. В противном случае p называется *иррегулярным*. Простое число 3 регулярно.

Согласно следствию теоремы 3, $B_2, B_4, \ldots, B_{p-3}$ суть p-целые числа. Поэтому p регулярно, если $\operatorname{ord}_p B_{2i} = 0$ для $i = 1, \ldots, (p - 3)/2$. Как нетрудно видеть, единицами в $\mathbf{Z}_p$ являются в точности элементы x с $\operatorname{ord}_p x = 0$. Таким образом, p регулярно, если $B_2, B_4, \ldots, B_{p-3}$ — единицы в $\mathbf{Z}_p$. Эквивалентным образом, p иррегулярно, если некоторое число B_{2i}, $1 \leqslant i \leqslant (p - 3)/2$, будет неединицей в $\mathbf{Z}_p$. Первые иррегулярные простые числа — это 37

59, так как известно, что $\mathrm{ord}_{37}(B_{32}) = 1$ и $\mathrm{ord}_{59}(B_{44}) = 1$ [234]. Вот несколько первых иррегулярных простых чисел: 37, 59, 67, 101, 103, 149 и 157. Йенсен в 1915 г. доказал, что существует бесконечно много иррегулярных простых чисел вида $4n + 3$. В следующем параграфе мы приведем короткое доказательство, принадлежащее Карлитцу (1953 г.), того, что существует бесконечно много иррегулярных простых чисел. Не доказано, что регулярных простых чисел бесконечно много. Очень жаль, что таково положение дел ввиду следующего замечательного результата Куммера (1850 г.).

Теорема 4. *Пусть p — регулярное простое число. Тогда уравнение $x^p + y^p = z^p$ не имеет решений в положительных целых числах* [1]).

На самом деле Куммер доказал, что теорема Ферма верна, если p не делит число классов поля $\mathbf{Q}(\zeta_p)$. Другими словами, критерий состоит в том, что для любого неглавного идеала A в $\mathbf{Z}[\zeta_p]$ идеал A^p неглавный. Это условие эквивалентно регулярности числа p. Мы не доказываем этот результат, но материал третьего параграфа этой главы тесно к нему примыкает.

Зигель привел вполне убедительные доводы в пользу того, что плотность иррегулярных простых чисел равна $1 - e^{-1/2} = 0{,}3935\ldots$. Это было проверено Джонсоном для простых чисел, меньших 30 000, с хорошими результатами [159]. Вагстаф доказал верность теоремы Ферма для всех простых чисел, меньших 125 000 [234]. Кроме того, полученная Джонсоном информация была им подтверждена для всех простых чисел, меньших 125 000 [234].

Если простое число p иррегулярно, можно спросить, сколько ненулевых чисел Бернулли в множестве $\{B_2, B_4, \ldots, B_{p-3}\}$ делятся на p. Это число называется *индексом иррегулярности* числа p. Первое простое число индекса 2 — это 157. Одно из наиболее замечательных открытий, сделанных с помощью ЭВМ, — доказательство существования двух простых чисел индекса 5 [234]. Наконец, отметим, что до сих пор не найдено никакой пары p, B_{2i}, $1 \leqslant i \leqslant (p-3)/2$, для которой $\mathrm{ord}_p B_{2i} > 1$. Приведенные выше факты и их связь со знаменитыми инвариантами Ивасавы более подробно рассматриваются в статье Джонсона [159] (а также в [167], [171], [31*]. — *Ред.*)

---

[1]) Недавно было доказано [26*], что для бесконечного числа простых чисел p решение уравнения Ферма $x^p + y^p = z^p$ удовлетворяет сравнению $xyz \equiv 0\ (p)$ (это так называемый первый случай теоремы Ферма, см. гл. 14 § 6).— *Прим. ред.*

§ 2. Сравнения для чисел Бернулли

Мы докажем теперь ряд арифметических свойств чисел Бернулли.

Для начала мы обратимся к доказательству теоремы 3 предыдущего параграфа. Заметим, что при $m \geqslant k$

$$\binom{m+1}{k} = \frac{m+1}{m-k+1}\binom{m}{k};$$

это непосредственно следует из определения биномиальных коэффициентов. Следовательно, теорема 1 предыдущего параграфа превращается в

$$S_m(n) = \sum_{k=0}^{m} \binom{m}{k} B_k \frac{n^{m+1-k}}{m+1-k}. \tag{9}$$

Далее, воспользовавшись тем, что $\binom{m}{k} = \binom{m}{m-k}$, убеждаемся в том, что

$$S_m(n) = \sum_{k=0}^{m} \binom{m}{k} B_{m-k} \frac{n^{k+1}}{k+1} =$$

$$= B_m n + \binom{m}{1} B_{m-1} \frac{n^2}{2} + \ldots + \frac{n^{m+1}}{m+1}. \tag{10}$$

В дополнение к равенству (10) нам понадобится следующая простая лемма.

Лемма 1. *Пусть p — простое число и $k \geqslant 1$ — целое число. Тогда*

(a) $p^k/(k+1)$ *есть p-целое число;*

(b) $p^k/(k+1) \equiv 0\ (p)$, *если* $k \geqslant 2$;

(c) $p^{k-2}/(k+1)$ *есть p-целое число, если* $k \geqslant 3$ *и* $p \geqslant 5$.

Доказательство. Для доказательства п. (a) мы покажем, что $k+1 \leqslant p^k$ для $k \geqslant 1$. Если $k = 1$, то результат верен. Если $k+1 \leqslant p^k$, то $k+2 \leqslant p^k + 1 \leqslant 2p^k \leqslant p^{k+1}$. Далее, запишем $k+1 = p^a q$, где $(q, p) = 1$. Тогда $p^k/(k+1) = p^{k-a}/q$. Так как $p^k/(k+1) \geqslant 1$, получаем, что $k \geqslant a$, т. е. п. (a) доказан. Для доказательства п. (b) заметим, что $k+1 < p^k$ для $k \geqslant 2$. Рассуждение то же самое, что и для п. (a). Поэтому $k > a$, что доказывает п. (b).

Что касается п. (c), то по индукции можно доказать неравенство $k+1 < p^{k-2}$ для $k \geqslant 3$ и $p \geqslant 5$. На этот раз делаем вывод о том, что $k-2 > a$, так что $p^{k-2}/(k+1) = p^{k-2-a}/q$ будет p-целым (и на самом деле делящимся на p). □

Предложение 15.2.1. *Пусть p — простое число и $m \geqslant 1$ — целое число. Тогда pB_m будет p-целым. Если $m \geqslant 2$ четное, то $pB_m \equiv S_m(p)\ (p)$.*

Доказательство. В первом утверждении говорится, что если p делит знаменатель числа B_m, то p^2 его не делит. Прежде всего $pB_1 = -p/2$, а это в самом деле p-целое число для всех p. Мы продолжим рассуждение по индукции.

Пусть $m > 1$. Воспользовавшись равенством (10) при $n = p$, убеждаемся в том, что так как $S_m(p) \in \mathbf{Z}$, достаточно доказать, что

$$\binom{m}{k} B_{m-k} \frac{n^{k+1}}{k+1} = \binom{m}{k} nB_{m-k} \frac{p^k}{k+1} \tag{11}$$

— p-целое число для $k = 1, 2, \ldots, m$. По предположению индукции pB_{m-k} p-целое для $k \geqslant 1$. Кроме того, в силу леммы 1, п. (a), $p^k/(k+1)$ будет p-целым. Отсюда следует, что pB_m — тоже p-целое число.

Для получения нужного сравнения достаточно показать, что

$$\operatorname{ord}_p\left(\binom{m}{k}\left(pB_{m-k}\frac{p^k}{k+1}\right)\right) \geqslant 1 \text{ для } k \geqslant 1.$$

В силу леммы 1, п. (b), это верно для $k \geqslant 2$. Для $k = 1$ нам следует показать, что

$$\operatorname{ord}_p\left(\frac{m}{2}(pB_{m-1})\,p\right) \geqslant 1,$$

а это вытекает из четности m. Действительно, $B_{m-1} = 0$ для четного m при $m \geqslant 4$, так что необходимо проверить лишь неравенство для $m = 2$, которое очевидно. □

Лемма 2. *Пусть p — некоторое простое число. Тогда при $p - 1 \nmid m$ имеем $S_m(p) \equiv 0\ (p)$. Если $p - 1 \mid m$, то $S_m(p) \equiv -1\ (p)$.*

Доказательство. Пусть g — какой-либо примитивный корень по модулю p. Тогда

$$S_m(p) = 1^m + 2^m + \ldots + (p-1)^m \equiv$$
$$\equiv 1^m + g^m + g^{2m} + \ldots + g^{(p-2)m}\ (p).$$

Таким образом, $(g^m - 1)\, S_m(p) \equiv g^{m(p-1)} - 1\ (p) \equiv 0\ (p)$. Если $p - 1 \nmid m$, то $g^m \not\equiv 1\ (p)$ и $S_m(p) \equiv 0\ (p)$. С другой стороны, если $p - 1 \mid m$, то $S_m(p) \equiv 1 + 1 + \ldots + 1\ (p) \equiv p - 1\ (p) \equiv -1\ (p)$. □

Теперь мы в состоянии доказать теорему 3. Предположим, что m четно. Тогда в силу предложения 15.2.1 мы знаем, что pB_m будет

p-целым и $pB_m \equiv S_m(p)$ (p). Согласно только что доказанной лемме, отсюда следует, что B_m будет p-целым при $p-1 \nmid m$ и $pB_m \equiv -1$ (p) при $p-1 \mid m$. Таким образом, число

$$A_m = B_m + \sum_{p-1 \mid m} \frac{1}{p}$$

p-целое для всех простых p Поэтому $A_m \in \mathbf{Z}$, и доказательство закончено. □

Если на этом этапе читатель сочтет, что не все следствия равенства (10) исчерпаны, он будет прав. В следующем предложении сформулировано еще одно важное следствие этого равенства. Запишем m-е число Бернулли в виде $B_m = U_m/V_m$, где $(U_m, V_m) = 1$. Мы предполагаем, что m четно.

Предложение 15.2.2. *Если m четно, $m \geqslant 2$, то при всех $n \geqslant 1$*

$$V_m S_m(n) \equiv U_m n \ (n^2).$$

Доказательство. Рассмотрим в равенстве (10) члены с $k \geqslant 1$ и фиксируем n:

$$\binom{m}{k}\left(B_{m-k}\frac{n^{k-1}}{k+1}\right)n^2 = A_k^m n^2. \tag{12}$$

Мы покажем, что $\operatorname{ord}_p\left(A_k^m\right) \geqslant 0$ при $p \mid n$ и $p \neq 2, 3$. Кроме того, если $2 \mid n$, то $\operatorname{ord}_2\left(A_k^m\right) \geqslant -1$, а если $3 \mid n$, то $\operatorname{ord}_3\left(A_k^m\right) \geqslant -1$. Это будет означать, что наибольший общий делитель числа n и знаменателя числа A_k^m является делителем 6 и, таким образом, это будет верно также и для суммы чисел A_k^m. Другими словами, можно записать

$$S_m(n) = B_m n + \frac{An^2}{lB},$$

где $(B, n) = 1$ и $l \mid 6$. Умножая это равенство на BV_m и вспоминая, что $6 \mid V_m$ в силу следствия 2 теоремы 3, сразу же получаем нужный результат.

Для доказательства оценок с ord_p мы воспользуемся следствием теоремы 3, согласно которому $\operatorname{ord}_p(B_{m-k}) \geqslant -1$ для всех $m-k \geqslant 0$ и всех p. Предположим прежде всего, что $p \neq 2, 3$, $p \mid n$. Случаи $k = 1, 2$ вытекают просто из того, что $B_t = 0$ при нечетном $t > 1$, $B_1 = -1/2$ и $\operatorname{ord}_p 3 = 0$. Если $k \geqslant 3$, то

$$\operatorname{ord}_p\left(B_{m-k}\frac{n^{k-1}}{k+1}\right) \geqslant -1 + (k-1)\operatorname{ord}_p n - \operatorname{ord}_p(k+1) \geqslant$$
$$\geqslant k - 2 - \operatorname{ord}_p(k+1) \geqslant 0, \tag{13}$$

согласно п. (c) леммы 1.

Рассмотрим теперь случай $p = 2$. Если $k = 1$, то $B_{m-1} = 0$ для $m > 2$ (m четно), в то время как для $m = 2$ число A_k^m превращается в число $2 \cdot B_1 \cdot 1/2 = -1/2$, имеющее порядок -1. Заметим, что $B_{m-k} = 0$ при $k > 1$, если k не является четным или $k \neq m - 1$. Но если k четно, то $\operatorname{ord}_2 (k + 1) = 0$, в то время как при $k = m - 1$ $A_{m-1}^m = -1/2n^{m-2}$, а последнее имеет порядок ord_2, больший или равный -1.

Наконец, рассмотрим случай $p = 3$, $3 \mid n$. Тогда, как легко проверить, $\operatorname{ord}_3 (A_2^m) \geqslant -1$ и $\operatorname{ord}_3 (A_3^m) \geqslant 1$. Но при $k \geqslant 4$ точно так же, как в лемме, показывается, что $\operatorname{ord}_3 (3^{k-2}/(k + 1)) \geqslant 0$, так что $\operatorname{ord}_3 (A_k^m) \geqslant 0$. Это завершает доказательство. □

В качестве простой числовой иллюстрации этого предложения рассмотрим $B_2 = 1/6$, $U_2 = 1$, $V_2 = 6$ и положим $n = 6$. Сравнение из формулировки предложения 15.2.2 превращается в

$$6 (1^2 + 2^2 + 3^2 + 4^2 + 5^2) \equiv 6 \ (36),$$

или, в более общем виде,

$$6 (1^2 + 2^2 + \ldots + (n - 1)^2) \equiv n \ (n^2).$$

Следствие. *Пусть m четно и p — такое простое число, что $p - 1 \nmid m$. Тогда*

$$S_m (p) \equiv B_m p \ (p^2).$$

Доказательство. В силу теоремы 3 $p \nmid V_m$. Положим в предложении 15.2.2 $n = p$ и разделим обе части получающегося сравнения на V_m, что допустимо, так как $p \nmid V_m$. Следствие доказано. □

Мы теперь в состоянии доказать весьма полезные сравнения Вороного. Согласно [230], Г. Ф. Вороной открыл эти сравнения в 1889 г., будучи еще студентом.

Предложение 15.2.3. *Пусть $m \geqslant 2$ четно, и определим U_m и V_m, как в последнем предложении. Предположим, что a и n — некоторые положительные целые числа с $(a, n) = 1$. Тогда*

$$(a^m - 1) U_m \equiv m a^{m-1} V_m \sum_{j=1}^{n-1} j^{m-1} \left[\frac{ja}{n} \right] \ (n), \tag{14}$$

где $[\alpha]$ — единственное целое число k, для которого $k \leqslant \alpha < k + 1$.

Доказательство. Для $1 \leqslant j < n$ запишем $ja = q_j n + r_j$, где $0 \leqslant r_j < n$. Тогда $[ja/n] = q_j$ и, так как $(a, n) = 1$, два множе-

ства $\{1, 2, 3, \ldots, n-1\}$ и $\{r_1, r_2, \ldots, r_{n-1}\}$ совпадают. По формуле бинома

$$j^m a^m \equiv r_j^m + mq_j n r_j^{m-1} \ (n^2).$$

Так как $r_j \equiv ja \ (n)$,

$$j^m a^m \equiv r_j^m + ma^{m-1} n \left[\frac{ja}{n}\right] j^{m-1} \ (n^2).$$

Суммирование по $j = 1, 2, \ldots, n-1$ приводит к сравнению

$$S_m(n)\, a^m \equiv S_m(n) + ma^{m-1} n \sum_{j=1}^{n-1} j^{m-1} \left[\frac{ja}{n}\right] \ (n^2).$$

Доказываемый результат следует теперь из сравнения, фигурирующего в предложении 15.2.2. □

Следствие. *Пусть p — простое число, $p \equiv 3 \ (4)$. Положим $m = (p+1)/2$. Тогда при $p > 3$.*

$$2\left(2 - \left(\frac{2}{p}\right)\right) B_m \equiv -\sum_{j=1}^{m-1} \left(\frac{j}{p}\right) \ (p),$$

где (x/p) обозначает символ Лежандра.

Доказательство. Заметим, что $m - 1 = (p-1)/2$, так что по критерию Эйлера $a^{m-1} \equiv (a/p) \ (p)$ для всех целых чисел a.

Положим в сравнении Вороного $a = 2$ и $n = p$. Учитывая только что сделанное замечание, получаем

$$\left(2\left(\frac{2}{p}\right) - 1\right) U_m \equiv m\left(\frac{2}{p}\right) V_m \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \left[\frac{2j}{p}\right] \ (p).$$

Далее, $[2j/p] = 0$ для $1 \leqslant j < m-1$ и $[2j/p] = 1$ для $m \leqslant j < p$. Кроме того, $2m \equiv 1 \ (p)$ и $p \nmid V_m$ в силу теоремы 3. Таким образом,

$$2\left(2 - \left(\frac{2}{p}\right)\right) B_m \equiv \sum_{j=m}^{p-1} \left(\frac{j}{p}\right) \ (p).$$

Так как $\sum_{j=1}^{p-1} (j/p) = 0$, доказательство завершено. □

Это следствие может быть использовано для доказательства интересного результата, связывающего числа классов с числами

Бернулли. Пусть p — некоторое простое число, $p \equiv 3\ (4)$, и рассмотрим мнимое квадратичное числовое поле $\mathbf{Q}(\sqrt{-p})$. Пусть h обозначает его число классов. Можно показать, что при $p > 3$

$$\left(2 - \left(\frac{2}{p}\right)\right) h = \sum_{1 \leqslant x < p/2} \left(\frac{x}{p}\right).$$

Доказательство см. в гл. 5, § 4, книги [9]. Объединение доказанного выше следствия с этой формулой для h дает следующее замечательное сравнение:

$$h \equiv -2B_{(p+1)/2}\ (p).$$

Сравнения Вороного приводят и к многим другим свойствам чисел Бернулли. Следующее предложение часто приписывается Адамсу. Оно дает некоторую информацию о числителе числа B_m.

Предложение 15.2.4. *Если $p - 1 \nmid m$, то B_m/m будет p-целым.*

Доказательство. В силу теоремы 3 B_m является p-целым. Запишем $m = p^t m_0$, где $p \nmid m_0$. В сравнении Вороного (14) положим $n = p^t$. Тогда $(a^m - 1)\, U_m \equiv 0\ (p^t)$. Пусть a — примитивный корень по модулю p. Так как $p - 1 \nmid m$, то $p \nmid (a^m - 1)$. Таким образом, $U_m \equiv 0\ (p^t)$ и $B_m/m = U_m/mV_m$ будет p-целым. □

В качестве численного примера возьмем $m = 22$ и $p = 11$. Тогда $B_{22} = 11 \cdot 131 \cdot 593/2 \cdot 3 \cdot 23$, так что $B_{22}/22$ цело в 11. В самом деле, это число есть единица в 11. В качестве следующего примера возьмем $m = 50$ и $p = 5$. B_{50} можно разложить на множители следующим образом:

$$B_{50} = \frac{5 \cdot 5 \cdot 417202699 \cdot 47464429777438199}{2 \cdot 3 \cdot 11}.$$

Очевидно, что $B_{50}/50$ — единица в 5. Менее очевидно, что 17-значное число в числителе является простым!

Следующая теорема в случае $e = 1$ принадлежит Куммеру. На эти сравнения теперь ссылаются как на сравнения Куммера.

Теорема 5. *Предположим, что $m \geqslant 2$ четно, p — простое число и $p - 1 \nmid m$. Положим $C_m = (1 - p^{m-1})\, B_m/m$. Если $m' \equiv m\ (\varphi(p^e))$, то $C_{m'} \equiv C_m\ (p^e)$.*

Доказательство. Запишем, как обычно, $B_m = U_m/V_m$. Пусть $t = \mathrm{ord}_p m$. Предложение 15.2.4 показывает, что $p^t \mid U_m$. В сравнении (14) положим $n = p^{e+t}$. Так как p^t делит оба числа m и U_m,

мы можем разделить получившееся сравнение на p^t. Поскольку $(m/p^t)\,V_m$ взаимно просто с p, получаем следующее сравнение:

$$\frac{(a^m-1)\,B_m}{m} \equiv a^{m-1}\sum_{j=1}^{p^{e+t-1}} j^{m-1}\left[\frac{ja}{p^{e+t}}\right] (p^e). \tag{15}$$

Это сравнение намечает путь к полному доказательству теоремы. Мы дадим сначала доказательство в случае $e=1$. В этом случае полностью проявляется очень простая идея доказательства и вычисления не столь громоздки, как при $e>1$.

В написанном выше сравнении предположим, что $e=1$. В правой части мы можем опустить те j, которые делятся на p. Если $p\nmid j$, то $j^{p-1}\equiv 1\,(p)$. Кроме того, так как $p\nmid a$, то $a^{p-1}\equiv 1\,(p)$. Таким образом, правая часть не изменится по модулю p, если заменить m на m', такое, что $m'\equiv m\,(p-1)$. В результате получаем

$$\frac{(a^{m'}-1)\,B_{m'}}{m'} \equiv \frac{(a^m-1)\,B_m}{m}\,(p).$$

Выберем в качестве a примитивный корень по модулю p. Так как $p-1\nmid m$, то $a^{m'}-1\equiv a^m-1\,(p)\not\equiv 0\,(p)$. Следовательно,

$$\frac{B_{m'}}{m'} \equiv \frac{B_m}{m}\,(p).$$

В случае $e>1$ эта процедура должна быть изменена, поскольку с членами, содержащими $j\equiv 0\,(p)$, не так легко разделаться. Мы выделим эти члены и перепишем соответствующую сумму. Более точно:

$$\sum_{j=1}^{p^{e+t-1}} j^{m-1}\left[\frac{ja}{p^{e+t}}\right] = \sum_{\substack{j=1\\(p,\,j)=1}}^{p^{e+t-1}} j^{m-1}\left[\frac{ja}{p^{e+t}}\right] + p^{m-1}\sum_{i=1}^{p^{e+t-1-1}} i^{m-1}\left[\frac{ia}{p^{e+t-1}}\right].$$

Рассмотрим сравнение (15) с e, замененным на $e-1$, и напомним, что $m-1\geqslant 1$. Имеем

$$\frac{p^{m-1}(a^m-1)\,B_m}{m} \equiv p^{m-1}a^{m-1}\sum_{i=1}^{p^{e+t-1-1}} i^{m-1}\left[\frac{ia}{p^{e+t-1}}\right] (p^e).$$

Собирая все это вместе, получаем

$$\frac{(1-p^{m-1})(a^m-1)B_m}{m} \equiv a^{m-1} \sum_{\substack{j=1 \\ (p,\,j)=1}}^{p^{e+t}-1} j^{m-1}\left[\frac{ja}{p^{e+t}}\right] (p^e). \quad (16)$$

Если $p \nmid j$ и $m' \equiv m\,(\varphi(p^e))$, то $j^{m'-1} \equiv j^{m-1}\,(p^e)$. Таким образом, правая часть в (16) не меняется по модулю p^e, если m заменяется на m', где $m' \equiv m\,(\varphi(p^e))$. Доказательство теперь продолжается точно так же, как в случае $e = 1$, и получается полный результат. □

Мы сделаем небольшое отступление, чтобы указать на современную интерпретацию сравнений Куммера.

Вспомним дзета-функцию Римана

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}.$$

В упр. 25 гл. 2 мы упоминали, что $\zeta(s)$ может быть продолжена до функции, голоморфной на всей комплексной плоскости, за исключением $s = 1$, где она имеет простой полюс с вычетом 1. Более того, можно показать [1]), что $\zeta(s)$ удовлетворяет функциональному уравнению

$$\zeta(1-s) = 2(2\pi)^{-s}\cos\left(\frac{\pi s}{2}\right)\Gamma(s)\,\zeta(s).$$

Г-функция определяется и обсуждается в гл. 16, § 6. Здесь нам лишь требуется тот факт, что $\Gamma(m) = (m-1)!$, когда m — положительное целое число.

Предположим, что $m \geqslant 2$ — четное целое число. Объединяя приведенное выше функциональное уравнение с теоремой 2, получаем

$$\zeta(1-m) = \frac{-B_m}{m}.$$

Положим $\zeta^*(s) = (1-p^{-s})\,\zeta(s)$. Тогда $\zeta^*(1-m) = -(1-p^{m-1})\,B_m/m$ и в силу теоремы 5 при $m' \equiv m\,(\varphi(p^e))$

$$\zeta^*(1-m') \equiv \zeta^*(1-m)\,(p^e). \quad (17)$$

Для фиксированного простого числа p функция $d(n, m) = p^{-\mathrm{ord}_p(n-m)}$ определяет метрику на $\mathbf{Z}$, p-адическую метрику. В этой метрике два целых числа близки, если их разность делится

[1]) См. простое доказательство в [169], гл. 20, § 2. — *Прим. ред.*

на высокую степень p. Сравнение (17) можно неформально переформулировать следующим образом: если m' и m p-адически близки и $m' \equiv m\ (p-1)$, то $\zeta^*(1-m')$ и $\zeta^*(1-m)$ p-адически близки. Это дает возможность продолжить ζ^* на метрическое пополнение кольца $\mathbf{Z}$, кольцо p-адических целых чисел. Эти идеи были реализованы Леопольдом и Куботой, которые первыми построили p-адические функции и исследовали их свойства. С тех пор были придуманы многие другие подходы. В методе Мазура числа Бернулли выражаются в виде некоторого p-адического интеграла от функций x^m. В этом контексте сравнения Куммера имеют очень естественное доказательство. С деталями читатель может познакомиться в гл. 2 из [162]. Ивасаве принадлежит поистине замечательный результат о том, что свойства p-адических дзета-функций (и p-адических L-функций) тесно связаны со структурой группы классов идеалов круговых полей. Ивасава дает довольно сжатое и строгое изложение своей теории в монографии [155]. Еще одно изложение этого материала можно найти в [167] (см. также [24*], [31*]. — *Ред.*).

Закончим этот параграф одним приложением теоремы 5. А именно, докажем, что существует бесконечно много иррегулярных простых чисел. Это доказательство принадлежит Карлитцу [105].

Теорема 6. *Множество иррегулярных простых чисел бесконечно.*

Доказательство. Пусть $\{p_1, \ldots, p_s\}$ — некоторое множество иррегулярных простых чисел. Мы найдем иррегулярное простое число, не принадлежащее этому множеству.

Пусть $k \geqslant 2$ четно и $n = k(p_1 - 1) \ldots (p_s - 1)$. Если рассматриваемое множество пусто, положим $n = k$. Воспользовавшись предложением 15.1.1, п. (c), выберем k настолько большим, чтобы $|B_n/n| > 1$. Выберем простое число p с $\operatorname{ord}_p(B_n/n) > 0$. По теореме Клауссена—фон Штаудта $p - 1 \nmid n$. Таким образом, $p \neq p_i$, $i = 1, \ldots, s$. Кроме того, $p \neq 2$. Мы покажем, что p иррегулярно.

Пусть $n \equiv m\ (p-1)$, где $0 \leqslant m < p - 1$. Тогда m четно и $m \neq 0$. Таким образом, $2 \leqslant m \leqslant p - 3$. В силу сравнения Куммера

$$\frac{B_n}{n} \equiv \frac{B_m}{m}\ (p).$$

Так как $\operatorname{ord}_p(B_n/n) > 0$ и $\operatorname{ord}_p(B_n/n - B_m/m) > 0$, отсюда следует, что

$$\operatorname{ord}_p\left(\frac{B_m}{m}\right) = \operatorname{ord}_p B_m > 0.$$

Это показывает, что p иррегулярно. □

§ 3. Теорема Хербранда

Пусть D_m — кольцо целых алгебраических чисел в круговом числовом поле $\mathbf{Q}(\zeta_m)$ и P — некоторый простой идеал в D_m, не содержащий m. Таким образом, если p — рациональное простое число в P, то $p \nmid m$. В § 3 гл. 14 мы поставили в соответствие P сумму Гаусса $g(P)$ и показали, что $g(P)^m = \Phi(P) \in D_m$. Соотношение Штикельбергера, доказанное в теореме 2 этого параграфа, задает разложение на простые идеалы $\Phi(P)$ в D_m, а именно,

$$(\Phi(P)) = P^{\sum t\sigma_t^{-1}}.$$

Здесь показатель степени есть элемент целочисленного группового кольца $\mathbf{Z}[G]$ группы Галуа G поля $\mathbf{Q}(\zeta_m)$ и t пробегает целые числа между 1 и m, которые взаимно просты с m. Автоморфизм σ_t переводит ζ_m в ζ_m^t. Напомним, что написанное выше выражение с показателем степени из $\mathbf{Z}[G]$ является сокращенной записью равенства

$$(\Phi(P)) = \sum_{\substack{(t,\,m)=1\\ 1\leqslant t<m}} (\sigma_t^{-1}(P))^t.$$

Если A — взаимно простой с m идеал, то он будет произведением простых идеалов, не содержащих m. Отсюда следует, что $A^{\sum t\sigma_t^{-1}}$ будет главным идеалом. Нам понадобится следующее предложение. Его доказательство будет приведено немного позже.

Предложение 15.3.1. *Пусть K — поле алгебраических чисел и M — некоторый фиксированный идеал в кольце целых чисел поля K. Тогда каждый класс идеалов K содержит идеал, взаимно простой с M.*

Если α принадлежит групповому кольцу $\mathbf{Z}[G]$, где G — группа Галуа поля $\mathbf{Q}(\zeta_m)$, то α очевидным способом действует на группе классов идеалов поля $\mathbf{Q}(\zeta_m)$. Сформулированное выше предложение означает, что если $\alpha = \sum t\sigma_t^{-1}$, то α переводит каждый класс идеалов в единичный класс. Говорят, что α *аннулирует* группу классов. Естественно спросить, существуют ли другие такие элементы группового кольца. Ниже приводятся такие аннулирующие элементы. Но сначала дадим нужное нам определение.

Определение. Элемент $\theta = \sum \langle t/m\rangle \sigma_t^{-1}$, где t пробегает множество представителей классов вычетов, взаимно простых с m, называется *элементом Штикельбергера*. Здесь $\langle t/m\rangle$ обозначает дробную часть числа t/m, которая зависит лишь от вычета t по модулю m. Элемент θ лежит в рациональном групповом кольце $\mathbf{Q}[G]$. Если b — целое число, взаимно простое с m, то пусть $r_b = (\sigma_b - b)\,\theta$.

Следующее предложение, доказательство которого будет приведено позже, имеет очень большое значение.

Предложение 15.3.2. *Элементы r_b принадлежат* $\mathbf{Z}[G]$ *и аннулируют группу классов.*

Мы убедимся вскоре, что это предложение без особого труда получается из соотношения Штикельбергера.

Предполагая известными приведенные предложения, мы приступаем к главной цели этого параграфа, к формулировке и доказательству теоремы Хербранда.

Пусть $m = l$ — нечетное простое число. Грубо говоря, в теореме Хербранда утверждается, что если l не делит определенного числа Бернулли, то некоторая часть группы классов поля $\mathbf{Q}(\zeta_l)$ тривиальна. Чтобы сделать это утверждение точным, нужно ввести еще несколько определений.

Пусть $\mathscr{A}$ — подгруппа группы классов идеалов поля $\mathbf{Q}(\zeta_l)$, состоящая из элементов, порядок которых делит l. Другими словами, некоторый класс идеалов принадлежит $\mathscr{A}$, если он содержит идеал, l-я степень которого является главным идеалом.

Определение. Пусть $1 \leqslant i \leqslant l-1$. Положим

$$\mathscr{A}_i = \{A \in \mathscr{A} \mid A^{\sigma_t} = A^{t^i},\ 1 \leqslant t < l\}.$$

Нетрудно убедиться в том, что каждое множество $\mathscr{A}_i$ будет подгруппой в $\mathscr{A}$. Кроме того, так как каждый элемент из $\mathscr{A}$ имеет порядок, делящий l, показатели степени можно вычислять по модулю l, т. е. на $\mathscr{A}$ действует групповое кольцо $\mathbf{Z}/l\mathbf{Z}[G]$. Если $t \in \mathbf{Z}$, будем обозначать через $\bar{t}$ его класс вычетов по модулю l.

Лемма 1. *$\mathscr{A}$ является прямым произведением подгрупп $\mathscr{A}_i$. Другими словами, $\mathscr{A} = \mathscr{A}_1\mathscr{A}_2 \ldots \mathscr{A}_{l-1}$ и $\mathscr{A}_i \cap \mathscr{A}_j = e$ (единичный класс), если $i \neq j$.*

Доказательство. Для каждого i, такого, что $1 \leqslant i \leqslant l-1$, определим элементы $\varepsilon_i \in \mathbf{Z}/l\mathbf{Z}[G]$ формулой

$$\varepsilon_i = -\sum_{t=1}^{l-1} \bar{t}^{-i}\sigma_t.$$

Замена t на ts в этой формуле приводит к соотношению $\sigma_s\varepsilon_i = \bar{s}^i\varepsilon_i$, если $l \nmid s$. Отсюда следует, что $\mathscr{A}^{\varepsilon_i} \subseteq \mathscr{A}_i$. С другой стороны, если $A \in \mathscr{A}_i$, то

$$A^{\varepsilon_i} = A^{-\sum \bar{t}^{-i}\sigma_t} = A^{-(l-1)} = A.$$

Значит, $\mathscr{A}^{\varepsilon_i} = \mathscr{A}_i$.

В силу леммы 2 § 2 $\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_{l-1}$ равняется σ_1, единичному автоморфизму. Таким образом,

$$\mathscr{A} = \mathscr{A}^{\varepsilon_1+\ldots+\varepsilon_{l-1}} =$$

$$= \mathscr{A}^{\varepsilon_1}\mathscr{A}^{\varepsilon_2}\ldots\mathscr{A}^{\varepsilon_{l-1}} = \mathscr{A}_1\mathscr{A}_2\ldots\mathscr{A}_{l-1}.$$

Предположим, что $i \neq j$ и $A \in \mathscr{A}_i \cap \mathscr{A}_j$. Тогда $A^{\sigma_t} = A^{t^i} = A^{t^j}$. Мы можем выбрать t равным примитивному корню по модулю l. Тогда $t^i \not\equiv t^j$ (l). Так как $A^{t^i - t^j} = e$ и A имеет порядок, делящийся на l, отсюда следует, что $A = e$. □

Следующая теорема Хербранда [149] дает с помощью чисел Бернулли критерий тривиальности подгрупп $\mathscr{A}_i$.

Теорема 7 (Хербранд). *Пусть i — нечетное целое число, $1 \leqslant i < l$. Определим j равенством $i + j = l$.*
Тогда $\mathscr{A}_1 = (e)$. Если $i \geqslant 3$ и $l \nmid B_j$, то $\mathscr{A}_i = (e)$.

Доказательство. Пусть $A \in \mathscr{A}_1$. Тогда в силу соотношения Штикельбергера

$$e = A^{\sum \sigma_t^{-1}} = A^{\sum t^{l-1}} = A^{l-1} = A^{-1}.$$

Это показывает, что $\mathscr{A}_1 = (e)$, как и утверждалось.

Предположим теперь, что i нечетно и $3 \leqslant i \leqslant l-2$. Пусть $A \in \mathscr{A}_i$. В силу предложения 15.3.2 $A^{r_b} = e$, где b — произвольное целое число, взаимно простое с l. Мы проанализируем это соотношение более внимательно.

По определению $r_b = (\sigma_b - b)\,\theta$. Далее,

$$\sigma_b\theta = \sum \langle t/l\rangle\, \sigma_b\sigma_t^{-1} = \sum \langle t/l\rangle\, \sigma_{b^{-1}t}^{-1} = \sum \langle bt/l\rangle\, \sigma_t^{-1}.$$

Таким образом,

$$r_b = (\sigma_b - b)\,\theta = \sum_{t=1}^{l-1} \left(\left\langle \frac{bt}{l}\right\rangle - b\left\langle \frac{t}{l}\right\rangle\right)\sigma_t^{-1}.$$

Запишем $bt = q_t l + s_t$, где $0 \leqslant s_t < l$. Тогда $\langle bt/l\rangle - b\,\langle t/l\rangle = s_t/l - bt/l = -q_t = -[bt/l]$. Это показывает, что $r_b = -\sum [bt/l]\,\sigma_t^{-1} \in \mathbf{Z}[G]$.

Предположим, что $A \in \mathscr{A}_i$. Применение σ_t^{-1} к A сводится к возведению A в степень $t^{l-1-i} = t^{j-1}$. Таким образом, применение r_b к A сводится к возведению A в степень $-\sum [bt/l]\, t^{j-1}$.

Запишем $B_j = U_j/V_j$ с $(U_j, V_j) = 1$. Сравнение Вороного (предложение 15.2.3) показывает, что (после некоторых переобозначений)

$$(b^j - 1)\,U_j \equiv jb^{j-1}V_j \sum_{t=1}^{l-1} \left[\frac{bt}{l}\right] t^{j-1}\ (l).$$

Согласно предыдущим рассмотрениям, правая часть этого сравнения аннулирует любой элемент $A \in \mathscr{A}_i$. Таким образом, для такого элемента $A^{(b^j-1)\,U_j} = e$. Выбирая в качестве b примитивный корень по модулю l, видим, что $l \nmid b^j - 1$, так что $A^{U_j} = e$. Если $l \nmid B_j$, то $l \nmid U_j$, а потому $A = e$. Таким образом, из $l \nmid B_j$ следует, что $\mathscr{A}_i = (e)$, как и утверждалось. □

Заметим, что в 1976 г. Рибе [208] получил обращение теоремы Хербранда. А именно, он показал, что если j четно и $2 \leqslant j \leqslant l-3$, то из $l \mid B_j$ следует, что $\mathscr{A}_i \neq (e)$ для $i = l - j$. Эта красивая теорема существования основана на тонких арифметических свойствах модулярных форм и находится, к сожалению, вне рамок этой книги.

Запишем $\mathscr{A} = \mathscr{A}^+\mathscr{A}^-$, где $\mathscr{A}^+ = \mathscr{A}_2\mathscr{A}_4 \ldots \mathscr{A}_{l-1}$ и $\mathscr{A}^- = \mathscr{A}_3\mathscr{A}_5 \ldots \mathscr{A}_{l-2}$. Тогда $\mathscr{A} = \mathscr{A}^+\mathscr{A}^-$ и $\mathscr{A}^+ \cap \mathscr{A}^- = (e)$ (см. упр. 23). Из теоремы Хербранда следует, что $|\mathscr{A}^-| = 1$, если $l \nmid B_j$ для $j = 2, 4, \ldots, l-3$. Это было известно уже Куммеру, который в сущности показал, что из $|\mathscr{A}^-| = 1$ следует равенство $|\mathscr{A}^+| = 1$. Таким образом, как мы упоминали ранее, Куммер установил, что из $l \nmid B_j$ для $j = 2, 4, \ldots, l-3$ следует, что число классов поля $\mathbf{Q}(\zeta)$ не делится на l.

Одна из наиболее знаменитых открытых проблем в теории алгебраических чисел — гипотеза Вандивера. В ней утверждается, что группа $\mathscr{A}^+$ из предыдущего абзаца всегда тривиальна. Не слишком трудно показать, что это эквивалентно утверждению о том, что число классов поля $\mathbf{Q}(\zeta_l + \zeta_l^{-1}) = \mathbf{Q}(\cos(2\pi/l))$ не делится на l. Вандивер выдвинул эту гипотезу приблизительно в 1920 г.; см. его статью о последней теореме Ферма [231]. Если она верна, то из нее вытекает много важных следствий. Вагстаф показал, что гипотеза Вандивера верна для всех простых чисел, меньших 125 000. Это убедительный довод в пользу ее справедливости, но Ларри Вашингтон привел вероятностные соображения по поводу того, что число 125 000 слишком мало, чтобы на него опираться.

Мы закончим эту главу доказательствами предложений 15.3.1 и 15.3.2.

Начнем с предложения 15.3.1. Пусть K — поле алгебраических чисел и D — кольцо его целых чисел. Пусть $M \subset D$ — ка-

кой-либо фиксированный идеал. Для любого идеала A в D пусть $\overline{A}$ обозначает его класс идеалов. Для данного идеала A мы построим такой идеал C, что $(C, M) = 1$ и $\overline{A}^{-1} = \overline{C}$. Это показывает, что обратный к любому классу содержит идеал, взаимно простой с M. Следовательно, каждый класс содержит идеал, взаимно простой с M. Для построения C мы поступаем следующим образом. Пусть $\{P_1, P_2, \ldots, P_t\}$ — множество простых идеалов, делящих M и не делящих A. Это множество может быть пустым. Если $P \mid A$, пусть, как обычно, $a(P) = \operatorname{ord}_P A$ обозначает показатель степени для P в разложении A в произведение простых идеалов. Выберем

$$\pi(P) \in P^{a(P)} - P^{a(P)+1}.$$

По китайской теореме об остатках можно найти такой элемент $\alpha \in D$, что

$$\alpha \equiv \pi(P) \ (P^{a(P)+1}) \quad \text{для} \quad P \mid A,$$
$$\alpha \equiv 1 \ (P_i) \quad \text{для} \quad i = 1, 2, \ldots, t.$$

Нетрудно проверить, что $(\alpha) = AC$, где $(C, M) = 1$. Таким образом, $\overline{A}^{-1} = \overline{C}$ и доказательство завершено. □

Наконец, мы обращаемся к доказательству предложения 15.3.2. Нам понадобится при этом следующая лемма, которая доказывается тем же способом, что и частный случай $m = l$, рассмотренный при доказательстве теоремы 7.

Лемма 2. *Пусть G обозначает группу Галуа поля $\mathbf{Q}(\zeta_m)/\mathbf{Q}$. Элемент $r_b = (\sigma_b - b)\,\theta$ лежит в $\mathbf{Z}[G]$. В действительности, $r_b = -\sum [bt/m]\,\sigma_t^{-1}$, где сумма берется по $1 \leqslant t < m$ с $(t, m) = 1$.*

Пусть P — некоторый простой идеал в D_m, кольце целых чисел поля $\mathbf{Q}(\zeta_m)$. Предположим, что $m \notin P$, и пусть $P \cap \mathbf{Z} = (p)$. Как в § 3 гл. 14, поставим в соответствие идеалу P сумму Гаусса $g(P)$. Мы знаем, что $g(P) \in \mathbf{Q}(\zeta_m, \zeta_p) = \mathbf{Q}(\zeta_{p,m})$.

Лемма 3. *Пусть b — некоторое целое число, взаимно простое с m. Определим b' условиями $b' \equiv b \ (m)$ и $b' \equiv 1 \ (p)$. Пусть σ_b — соответствующий автоморфизм поля $\mathbf{Q}(\zeta_{pm})$. Тогда*

$$g(P)^{\sigma_{b'}-b} \in \mathbf{Q}(\zeta_m).$$

Доказательство. Автоморфизмы поля $\mathbf{Q}(\zeta_{pm})$, которые оставляют ζ_m на месте, имеют вид σ_c, где $(c, pm) = 1$ и $c \equiv 1 \ (m)$. Пусть

$$\Omega_b(P) = g(P)^{\sigma_{b'}-b}.$$

Мы покажем, что $\Omega_b(P)^{\sigma_c} = \Omega_b(P)$. Это доказывает, согласно теории Галуа, что $\Omega_b(P) \in \mathbf{Q}(\zeta_m)$.

Напомним, что $g(P) = \sum \chi_p(t)\psi(t)$, где сумма берется по приведенной системе вычетов по модулю m. Так как $\chi_p(t) \in \mathbf{Q}(\zeta_m)$ и $\psi(t) \in \mathbf{Q}(\zeta_p)$, то

$$g(P)^{\sigma_{b'}} = \sum \chi_p(t)^b \psi(t)$$

и

$$g(P)^{\sigma_{b'}\sigma_c} = \sum \chi_p(t)^b \psi(t)^c = \sum \chi_p(t)^b \psi(ct).$$

Таким образом,

$$g(P)^{\sigma_{b'}\sigma_c} = \chi_p(c)^{-b} g(P)^{\sigma_{b'}}. \tag{1}$$

Аналогично

$$g(P)^{\sigma_c} = \chi_p(c)^{-1} g(P). \tag{2}$$

Возводя обе части равенства (2) в степень b и деля на результат равенство (1), получаем $\Omega_b(P)^{\sigma_c} = \Omega_b(P)$, как и утверждалось. □

Мы теперь можем закончить доказательство предложения 15.3.2. Пусть $P \subset D_m$ — некоторый простой идеал, не содержащий m. Из соотношения Штикельбергера получаем, что $g(P)^m \in \mathbf{Q}(\zeta_m)$ и $(g(P)^m) = P^{m\theta}$. Применение $\sigma_b - b$ к обеим частям последнего равенства показывает, что $(\Omega_b(P)^m) = (P^{r_b})^m$. В силу лемм 2 и 3, это превращается в D_m в равенство $(\Omega_b(P))^m = (P^{r_b})^m$. Из однозначности разложения для идеалов следует, что $P^{r_b} = (\Omega_b(P))$. Таким образом, P^{r_b} — главный идеал и потому A^{r_b} — главный идеал для любого идеала A, взаимно простого с (m). В силу предложения 15.3.1 это означает, что r_b аннулирует группу классов кольца D_m. □

Замечания

В 1960 г. Вандивер опубликовал обзорную статью [232], в которой он отмечает, что по числам Бернулли появилось около 1500 работ. Ясно, что эта последовательность чисел имеет большую притягательную силу и значительную ценность. Наиболее обширным классическим трудом по числам Бернулли является [199]. Довольно доступный современный источник — две главы из книги по аналитической теории чисел [204]. Эта книга содержит изложение формулы суммирования Эйлера—Маклорена, важного приложения чисел Бернулли, которое мы не рассматривали.

Крупным достижением было вычисление значений функции $\zeta(s)$ в положительных четных целых числах. Удивительно, что

почти ничего не известно о значениях $\zeta(s)$ в положительных нечетных целых числах. В 1978 г. французский математик Апери произвел сенсацию, найдя исключительно остроумное доказательство того, что $\zeta(3)$ иррационально. См. интересную статью [233] с неформальным изложением этого результата.

Числа Бернулли очень тесно связаны с последней теоремой Ферма и арифметикой круговых полей, что подтверждается многочисленными ссылками на числа Бернулли в учебнике [206]; см., в частности, § 2 лекции VI. Короткая вводная статья [231] также заслуживает того, чтобы с ней познакомиться.

Работа [159] содержит довольно доступное обсуждение регулярных и иррегулярных простых чисел; в ней упоминается несколько интересных открытых проблем. Мы воспользуемся этой работой при изложении краткой истории вычислений, связанных с иррегулярными числами. Куммер обнаружил, что 8 из первых 37 простых чисел иррегулярны. В 30-х годах Вандивер и другие распространили вычисления на все простые числа, меньшие 618. К 1955 г. Вандивер, Д. Лемер, Эмма Лемер, Селфридж и Николь сдвинули границу до 4001. В 1964 г. Селфридж и Поллак анонсировали вычисления до 25 000. Они не были опубликованы. В 1970 г. Кобелев опубликовал таблицы вплоть до 5500, а в 1973 г. Джонсон достиг 8000. В 1975 г. Джонсон отодвинул границу до 30 000. Как отмечалось ранее, теперешний рекорд принадлежит Вагстафу: 125 000. Искусство вычислений прошло значительный путь!

Следующий результат получили независимо Метсянкюля [188] и Ёкои [247]. Пусть $m > 2$ — некоторое целое число и H — собственная подгруппа в $U(\mathbf{Z}/m\mathbf{Z})$. Существует бесконечно много иррегулярных чисел p, класс вычетов которых по модулю m не принадлежит H. По контрасту с этим неизвестно ни одного модуля $m > 2$, для которого существует бесконечно много иррегулярных простых чисел $p \equiv 1\ (m)$.

Основная теорема § 3 была опубликована Хербрандом в 1932 г. [149]. Доказательство, использующее p-адические числа и сравнения для обобщенных чисел Бернулли, можно найти в работе [208]. См. также гл. 1 книги [167]. Имеется несколько интересных гипотез относительно p-примарной компоненты группы классов поля $\mathbf{Q}(\zeta_p)$. Во введении к статье [242] описывается гипотеза, уточняющая теорему Хербранда.

Упражнения

1. Используя определение чисел Бернулли, показать, что $B_{10} = 5/66$ и $B_{12} = -691/2730$.

2. Показать, что если $a \in \mathbf{Z}$, то $a(a^m - 1)B_m \in \mathbf{Z}$ для всех $m > 0$.

3. Показать, что если $a \in \mathbf{Z}$, то $a^m(a^m - 1)B_m/m \in \mathbf{Z}$ для всех $m > 0$.

4. Показать, что если $m \geqslant 4$ четное, то $2B_m = 1$ (4).

5. Показать, что если p — нечетное простое число и $p - 1 \mid m$, то $(B_m + p^{-1} - 1)/m$ будет p-целым. Этот результат принадлежит Карлитцу [1]).

6. Для $m \geqslant 3$ показать, что $|B_{2m+2}| > |B_{2m}|$. [*Указание.* Использовать теорему 2.]

7. Пусть $m \geqslant 2$ — четное целое число. Показать, что существует бесконечно много чисел $n \geqslant m$, для которых $B_n - B_m \in \mathbf{Z}$. [*Указание.* Пусть q — простое число, для которого $q - 1 \mid ((m+1)!)$; попробовать $n = qm$. Существование бесконечного числа таких простых чисел q показано в гл. 16. Этот результат принадлежит Радо.]

8. *Рассмотрим разложение в степенной ряд в окрестности начала координат для* tg (x):

$$\sum_{k=1}^{\infty} T_k \frac{x^{2k-1}}{(2k-1)!}.$$

Показать, что $T_k = (-1)^{k-1}(B_{2k}/2k)(2^k - 1)\,2^{2k}$. Заметим, что $T_k \in \mathbf{Z}$ для всех k в силу упр. 3.

9. Используя лемму 1 из § 1, показать, что радиус сходимости ряда

$$\sum_{n=0}^{\infty} B_n (t^n/n!)$$

равен 2π. В качестве следствия показать, что для любых C, $k > 0$ существует бесконечно много таких n, что $|B_n| > Cn^k$. (Этот результат слабее оценки, задаваемой неравенством (8) из § 1. С другой стороны, его значительно легче получить.)

10. Воспользоваться сравнениями Вороного для получения следующего результата Куммера:

$$\sum_{k=0}^{r} (-1)^k \binom{r}{k} \frac{B_{2n+k(p-1)}}{2n + k(p-1)} \equiv 0 \ (p^r),$$

если только $2 \leqslant r + 1 \leqslant 2n$ и $p - 1 \nmid 2n$. Сделать это не так-то просто. С небольшими изменениями в обозначениях доказательство содержится в § 8 гл. IX книги [230].

11. Те, кто знаком с подходом Мазура к p-адическим дзета- и L-функциям, могут попытаться проделать следующее. Пусть μ_α — нормализованная «мера Мазура» на $\mathbf{Z}_p$. Воспользоваться сравнениями Вороного для доказательства того, что

$$\int_{\mathbf{Z}_p}^{*} x^{k-1}\, d\mu_\alpha = (\alpha^{-k} - 1)(1 - p^{k-1})(-B_k/k).$$

Обозначения и определение меры Мазура можно посмотреть в [162].

12. Напомним определение многочленов Бернулли:

$$B_m(x) = \sum_{k=0}^{m} \binom{m}{k} B_k x^{m-k}.$$

---

[1]) Carlitz L. Some congruences for the Bernoulli numbers. — Amer. J. Math., 1953, v. 75, p. 163—172.

Показать, что

$$te^{tx}/(e^t - 1) = \sum_{m=0}^{\infty} B_m(x)\,(t^m/m!).$$

13. Показать, что $B_m(x+1) - B_m(x) = mx^{m-1}$.

14. Воспользоваться упр. 13 для нового доказательства теоремы 1.

15. Предположим, что $f(x) = \sum_{k=0}^{n} a_k x^k$ — многочлен с комплексными коэффициентами. Воспользоваться упр. 13 для нахождения многочлена $F(x)$, для которого $F(x+1) - F(x) = f(x)$.

16. Показать, что для $n \geqslant 1$ $(d/dx)\,B_n(x) = nB_{n-1}(x)$.

17. Показать, что $B_n(1-x) = (-1)^n B_n(x)$.

18. Воспользоваться упр. 13 и 17 для нового доказательства того, что $B_n = 0$ при нечетном $n > 1$.

19. Предположим, что n и F — целые числа и n, $F > 0$. Показать, что

$$B_n(Fx) = F^{n-1} \sum_{a=0}^{F-1} B_n\left(x + \frac{a}{F}\right).$$

[*Указание*. Воспользоваться упр. 12.]

20. Предположим, что $H(x)$ — многочлен степени n с комплексными коэффициентами. Предположим, что для всех целых чисел n, $F > 0$ мы имеем $H(Fx) = F^{n-1} \sum_{a=0}^{F-1} H(x + (a/F))$. Показать, что $H(x) = CB_n(x)$ с некоторой константой C. [*Указание*. Воспользоваться упр. 16 и индукцией по n].

21. Показать, что $B_n(1/2) = (1 - 2^{n-1})B_n$.

22. В более общем виде показать, что

$$(1 - F^{n-1})\,B_n = \sum_{a=1}^{F-1} B_a(a/F).$$

23. Доказать, что $\mathscr{A} = \mathscr{A}^+\mathscr{A}^-$ и $\mathscr{A}^+ \cap \mathscr{A}^- = (e)$.

Глава 16

L-ФУНКЦИИ ДИРИХЛЕ

Теория аналитических функций имеет много приложений в теории чисел. Особенно эффективное приложение было найдено Дирихле, который в 1837 г. доказал, что в любой арифметической прогрессии b, $b+m$, $b+2m$, ..., где $(m, b)=1$, имеется бесконечно много простых чисел. Для этого он ввел L-функции, которые теперь носят его имя. В данной главе мы определим эти функции, изучим их свойства и докажем теорему об арифметических прогрессиях. L-функции Дирихле используются не только при доказательстве этой теоремы. Оказывается, что их значения в отрицательных целых числах особенно важны. Мы найдем эти значения и покажем, как они связаны с числами Бернулли.

В большей части главы мы используем лишь основы анализа. Однако в § 6, где рассматривается значение L-функций в 1, существенно используется теория функций комплексной переменной. Последнего можно было бы избежать, но при этом пришлось бы пожертвовать как глубиной, так и изяществом. Все необходимые предварительные сведения можно найти в любом стандартном курсе. Удобным справочником является книга [85] (*или* [19*]. — *Ред.*). *В* § 1—4 *буква s будет обозначать вещественную переменную, $s>1$.*

§ 1. Дзета-функция

Дзета-функция Римана $\zeta(s)$ определяется рядом

$$\zeta(s)=\sum_{n=1}^{\infty} n^{-s}.$$

Он сходится при $s>1$ и сходится равномерно при $s \geqslant 1+\delta>1$ для любого $\delta>0$.

Предложение 16.1.1. *Для $s>1$*

$$\zeta(s)=\prod_{p}(1-p^{-s})^{-1},$$

где произведение берется по всем простым p.

Доказательство. Для $s > 1$ имеем $p^{-s} < 1$, так что

$$(1 - p^{-s})^{-1} = \sum_{m=0}^{\infty} p^{-ms}.$$

По теореме об однозначном разложении на простые множители получаем

$$\prod_{p \le N} (1 - p^{-s})^{-1} = \sum_{n \le N} n^{-s} + R_N(s).$$

Очевидно, что $R_N(s) \le \sum_{n=N+1}^{\infty} n^{-s}$. Так как $\zeta(s)$ сходится, то $R_N(s) \to 0$ при $N \to \infty$, откуда и следует наш результат. □

Поведение функции $\zeta(s)$ при $s \to 1$ имеет очень большое значение. Так как ряд $\sum_{n=1}^{\infty} n^{-1}$ расходится, мы, конечно, ожидаем, что $\zeta(s) \to \infty$ при $s \to 1$. В самом деле, справедлив такой результат:

Предложение 16.1.2. *Предположим, что* $s > 1$. *Тогда*

$$\lim_{s \to 1} (s - 1)\zeta(s) = 1.$$

Доказательство. При фиксированном s функция t^{-s} будет монотонно убывающей по t. Таким образом,

$$(n+1)^{-s} < \int_n^{n+1} t^{-s}\,dt < n^{-s}.$$

Суммируя эти неравенства от $n = 1$ до ∞, получаем

$$\zeta(s) - 1 < \int_1^{\infty} t^{-s}\,dt < \zeta(s).$$

Значение выписанного интеграла равно $(s-1)^{-1}$. Отсюда следует, что $1 < (s-1)\zeta(s) < s$. Беря предел при $s \to 1$, получаем нужный результат. □

Следствие. *При* $s \to 1$

$$\frac{\ln \zeta(s)}{\ln (s-1)^{-1}} \to 1.$$

Доказательство. Положим $(s-1)\zeta(s) = \rho(s)$. Тогда $\ln(s-1) + \ln \zeta(s) = \ln \rho(s)$, так что

$$\ln \zeta(s)/\ln (s-1)^{-1} = 1 + (\ln \rho(s)/\ln (s-1)^{-1}).$$

При $s \to 1$ имеем $\rho(s) \to 1$ в силу предложения 16.1.2. Поэтому $\ln \rho(s) \to 0$ и следствие доказано. □

Предложение 16.1.3. $\ln \zeta(s) = \sum_p p^{-s} + R(s)$, *где* $R(s)$ *остается ограниченным при* $s \to 1$.

Доказательство. Мы воспользуемся формулой $\ln (1-x)^{-1} = x + x^2/2 + x^3/3 + \ldots$, которая справедлива при $-1 < x < 1$. В силу предложения 16.1.1

$$\zeta(s) = \prod_{p \leqslant N} (1 - p^{-s})^{-1} \lambda_N(s),$$

где $\lambda_N(s) \to 1$ при $N \to \infty$. Взятие логарифма от обеих частей приводит к равенству

$$\ln \zeta(s) = \sum_{p \leqslant N} \sum_{m=1}^{\infty} m^{-1} p^{-ms} + \ln \lambda_N(s).$$

Возьмем предел при $N \to \infty$:

$$\ln \zeta(s) = \sum_p \sum_{m=1}^{\infty} m^{-1} p^{-ms} = \sum_p p^{-s} + \sum_p \sum_{m=2}^{\infty} m^{-1} p^{-ms}.$$

Вторая сумма меньше, чем

$$\sum_p \sum_{m=2}^{\infty} p^{-ms} = \sum_p p^{-2s} (1 - p^{-s})^{-1} \leqslant (1 - 2^{-s})^{-1} \sum_p p^{-2s} \leqslant 2\zeta(2).$$

Всюду было использовано предположение о том, что $s > 1$. □

Определение. Говорят, что некоторое множество положительных простых чисел $\mathscr{P}$ имеет *плотность Дирихле*, если существует предел

$$\lim_{s \to 1} \frac{\sum_{p \in \mathscr{P}} p^{-s}}{\ln (s-1)^{-1}}.$$

Если предел существует, мы обозначаем его через $d(\mathscr{P})$ и называем $d(\mathscr{P})$ *плотностью Дирихле* множества $\mathscr{P}$.

Предложение 16.1.4. *Пусть* $\mathscr{P}$ *— некоторое множество положительных простых чисел. Тогда*

(a) *если* $\mathscr{P}$ *конечно, то* $d(\mathscr{P}) = 0$;

(b) *если* $\mathscr{P}$ *состоит из всех кроме конечного числа положительных простых чисел, то* $d(\mathscr{P}) = 1$;

(c) *если* $\mathscr{P} = \mathscr{P}_1 \cup \mathscr{P}_2$, *где* $\mathscr{P}_1$ *и* $\mathscr{P}_2$ *не пересекаются и оба предела* $d(\mathscr{P}_1)$ *и* $d(\mathscr{P}_2)$ *существуют, то* $d(\mathscr{P}) = d(\mathscr{P}_1) + d(\mathscr{P}_2)$.

Доказательство. Утверждения (a) и (c) очевидны согласно определению плотности Дирихле. Утверждение (b) сразу же получается из следствия предложения 16.1.2 и предложения 16.1.3. □

Мы теперь можем сформулировать основную теорему этого параграфа. Доказательство будет рассредоточено по следующим трем параграфам.

Теорема 1 (Дирихле). *Предположим, что* $a, m \in \mathbf{Z}$, *причем* $(a, m) = 1$. *Пусть* $\mathscr{P}(a; m)$ — *множество положительных простых чисел* p, *для которых* $p \equiv a\ (m)$. *Тогда* $d(\mathscr{P}(a; m)) = 1/\varphi(m)$.

Заметим, что из теоремы 1 несомненно следует, что множество $\mathscr{P}(a; m)$ бесконечно, ибо если бы это было не так, то его плотность равнялась бы нулю.

§ 2. Частный случай

Сначала мы докажем теорему 1 в случае, когда $m = 4$. Все основные идеи доказательства проявляются уже в этом частном случае, а детали при этом значительно упрощаются.

Определим функцию χ из $\mathbf{Z}$ в $\{\pm 1\}$ следующим образом: $\chi(n) = 0$, если n четно; $\chi(n) = 1$, если $n \equiv 1\ (4)$, и $\chi(n) = -1$, если $n \equiv 3\ (4)$. Как нетрудно убедиться, $\chi(mn) = \chi(m)\chi(n)$ для всех $m, n \in \mathbf{Z}$.

Положим

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s} = 1 - 3^{-s} + 5^{-s} - 7^{-s} + \ldots.$$

Для всех n имеем $|\chi(n) n^{-s}| \leqslant n^{-s}$. Отсюда следует, что члены ряда $L(s, \chi)$ мажорируются по абсолютной величине членами ряда $\zeta(s)$. Таким образом, ряд $L(s, \chi)$ сходится и является непрерывной функцией для $s > 1$. Так как функция χ полностью мультипликативна, то доказательство предложения 16.1.1 показывает, что

$$L(s, \chi) = \prod_p (1 - \chi(p) p^{-s})^{-1}.$$

Полезно модифицировать $\zeta(s)$ так, чтобы исключить четные члены. Пусть

$$\zeta^*(s) = \sum_{n \equiv 1\ (2)} n^{-s}.$$

Так как

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \sum_{n\equiv 1\,(2)} n^{-s} + \sum_{n\equiv 0\,(2)} n^{-s} = \zeta^*(s) + 2^{-s}\zeta(s),$$

то $\zeta^*(s) = (1 - 2^{-s})\,\zeta(s)$, а потому

$$\zeta^*(s) = \prod_{p\neq 2} (1 - p^{-s})^{-1}.$$

Используя метод доказательства предложения 16.1.3, получаем

$$\ln L(s, \chi) = \sum_{p\neq 2} \chi(p)\, p^{-s} + R_1(s), \qquad \text{(i)}$$

$$\ln \zeta^*(s) = \sum_{p\neq 2} p^{-s} + R_2(s), \qquad \text{(ii)}$$

где $R_1(s)$ и $R_2(s)$ остаются ограниченными при $s \to 1$.

Имеем $1 + \chi(p) = 2$ при $p \equiv 1\ (4)$ и $1 + \chi(p) = 0$ при $p \equiv 3\ (4)$. Аналогично $1 - \chi(p) = 2$ при $p \equiv 3\ (4)$ и $1 - \chi(p) = 0$ при $p \equiv 1\ (4)$. Из (i) и (ii) получаем

$$\ln \zeta^*(s) + \ln L(s, \chi) = 2 \sum_{p\equiv 1\,(4)} p^{-s} + R_3(s), \qquad \text{(iii)}$$

$$\ln \zeta^*(s) - \ln L(s, \chi) = 2 \sum_{p\equiv 3\,(4)} p^{-s} + R_4(s), \qquad \text{(iv)}$$

где $R_3(s)$ и $R_4(s)$ остаются ограниченными при $s \to 1$.

Следующий шаг состоит в том, чтобы показать, что $\ln L(s, \chi)$ остается ограниченной при $s \to 1$. Для этого запишем $L(s, \chi) = 1 - 3^{-s} + 5^{-s} - \ldots = (1 - 3^{-s}) + (5^{-s} - 7^{-s}) + \ldots = 1 - (3^{-s} - 5^{-s}) - (7^{-s} - 9^{-s}) - \ldots$. Отсюда следует, что $2/3 < L(s, \chi) < 1$ для всех $s > 1$. Таким образом, $\ln 2/3 < \ln L(s, \chi) < \ln 1 = 0$ для $s > 1$.

В качестве последнего подготовительного шага заметим, что $\ln \zeta^*(s) = \ln(1 - 2^{-s}) + \ln \zeta(s)$, так что в силу следствия предложения 16.1.2 $\ln \zeta^*(s)/\ln (s-1)^{-1} \to 1$ при $s \to 1$.

Деля теперь каждый член равенств (iii) и (iv) на $\ln (s-1)^{-1}$ и переходя к пределу при $s \to 1$, в результате получаем

Предложение 16.2.1. *$d(\mathscr{P}(1;\ 4)) = 1/2$ и $d(\mathscr{P}(3;\ 4)) = 1/2$.*

Для доказательства теоремы 1 в общем случае надо обобщить χ и $L(s, \chi)$. Это приводит к рассмотрению характеров Дирихле и L-функций.

§ 3. Характеры Дирихле

Функция χ, рассмотренная в последнем параграфе, может быть получена при помощи следующей конструкции. Рассмотрим группу $U(\mathbf{Z}/4\mathbf{Z})$. Эта группа имеет два элемента $1 + 4\mathbf{Z}$ и $3 + 4\mathbf{Z}$.

Определим χ': $U(\mathbf{Z}/4\mathbf{Z}) \to \{\pm 1\}$ посредством $\chi'(1 + 4\mathbf{Z}) = 1$ и $\chi'(3 + 4\mathbf{Z}) = -1$. Тогда χ' будет гомоморфизмом из $U(\mathbf{Z}/4\mathbf{Z})$ в $\mathbf{C}^*$. Для $n \in \mathbf{Z}$ положим $\chi(n) = 0$, если $(n, 4) > 1$, и $\chi(n) = \chi'(n + 4\mathbf{Z})$, если $(n, 4) = 1$. Эта функция χ: $\mathbf{Z} \to \mathbf{C}^*$ совпадает с функцией χ последнего параграфа.

Эту конструкцию нетрудно обобщить. Пусть m — некоторое фиксированное положительное целое число. Пусть χ': $U(\mathbf{Z}/m\mathbf{Z}) \to \mathbf{C}^*$ — какой-нибудь гомоморфизм. Для данного χ' определим χ: $\mathbf{Z} \to \mathbf{C}$ следующим образом: при $(n, m) > 1$ положим $\chi(n) = 0$, при $(n, m) = 1$ положим $\chi(n) = \chi'(n + m\mathbf{Z})$. Так определенные функции χ называются *характерами Дирихле по модулю* m. Другая их характеризация задается следующими тремя условиями на функцию χ: $\mathbf{Z} \to \mathbf{C}$:

(a) $\chi(n + m) = \chi(n)$ для всех $n \in \mathbf{Z}$;
(b) $\chi(kn) = \chi(k)\chi(n)$ для всех $k, n \in \mathbf{Z}$;
(c) $\chi(n) \neq 0$ тогда и только тогда, когда $(n, m) = 1$.

Нетрудно убедиться в том, что эти три условия определяют множество характеров Дирихле по модулю m.

Для изучения свойств характеров Дирихле мы рассмотрим сначала более общую проблему.

Пусть A — некоторая конечная абелева группа (записываемая мультипликативно). *Характером* на A называется гомоморфизм из A в $\mathbf{C}^*$. Множество таких характеров будет обозначаться через $\hat{A}$. Если $\chi, \psi \in \hat{A}$, определим $\chi\psi$ как функцию, которая переводит $a \in A$ в $\chi(a)\psi(a)$. Тогда $\chi\psi$ тоже будет характером. Мы покажем, что это произведение превращает $\hat{A}$ в группу. Определим χ_0, тривиальный характер, формулой $\chi_0(a) = 1$ для всех $a \in A$. Если $\chi \in \hat{A}$, то определим χ^{-1} формулой $\chi^{-1}(a) = \chi(a)^{-1}$ для всех $a \in A$. Нетрудно убедиться в том, что $\chi^{-1} \in \hat{A}$ и $\chi\chi^{-1} = \chi_0$. С этими определениями $\hat{A}$ становится абелевой группой, у которой χ_0 — единичный элемент. Более или менее очевидные детали мы опускаем.

Пусть n — порядок группы A. Если $a \in A$, то a^n равно e, единичному элементу в A. Таким образом, если $\chi \in \hat{A}$, то $\chi(a)^n = 1$, т. е. значениями χ будут корни степени n из единицы. Отсюда следует, что $\overline{\chi(a)} = \chi(a)^{-1} = \chi^{-1}(a)$, где черта обозначает комплексное сопряжение. Поэтому χ^{-1} иногда записывается как $\bar{\chi}$ и называется *сопряженным характером* для χ.

Сразу же возникают два вопроса. Насколько велика группа $\hat{A}$? Каково ее строение? На эти вопросы легко ответить в случае, когда A циклическая. В общем случае мы воспользуемся теоремой из теории групп, в которой утверждается, что конечная абелева группа является прямым произведением циклических групп (см. [150] (или [9*]. — *Ред.*)). Для $A = U(\mathbf{Z}/m\mathbf{Z})$, т. е.

в интересующем нас случае, этот результат следует из теоремы 3 гл. 4.

Предположим, что группа A — циклическая и порождается элементом g порядка n. Пусть $\zeta_n = e^{2\pi i/n}$. Если $\chi \in \widehat{A}$, то $\chi(g) = \zeta_n^e$ при некотором однозначно определенном целом числе e, для которого $0 \leqslant e < n$. Так как $\chi(g^m) = \chi(g)^m$, то χ определено его значением в g. Обратно, если $0 \leqslant e < n$, определим $\chi(g^m) = \zeta_n^{me}$. Нетрудно убедиться в том, что функция χ определена корректно и является характером. Следовательно, на A существует в точности n характеров. Пусть $\chi_1 \in \widehat{A}$ таков, что $\chi_1(g) = \zeta_n$. Если $\chi \in \widehat{A}$ и $\chi(g) = \zeta_n^e$, то $\chi(g) = \chi_1^e(g)$, откуда следует, что $\chi = \chi_1^e$. Это показывает, что $\widehat{A}$ циклическая и порождена характером χ_1. Таким образом, $A \approx \widehat{A}$.

В общем случае A будет прямым произведением циклических групп. Это означает, что существуют такие элементы $g_1, g_2, \ldots, g_t \in A$, что

(i) порядок g_i равен n_i;

(ii) каждый элемент $a \in A$ может быть однозначно записан в виде $a = g_1^{m_1} g_2^{m_2} \ldots g_t^{m_t}$, где $0 \leqslant m_i < n_i$ для всех i.

Если порядок A равен n, то очевидно, что $n = n_1 n_2 \ldots n_t$.

Предположим, что $\chi \in \widehat{A}$. Тогда χ определяется значениями $\chi(g_i) = \zeta_{n_i}^{e_i}$, где $0 \leqslant e_i < n_i$. Обратно, для заданного t-набора $(e_1, e_2, \ldots, e_t)$ с $0 \leqslant e_i < n_i$ при всех i мы можем определить характер χ следующим образом. Для $a \in A$ запишем $a = g_1^{m_1} g_2^{m_2} \ldots g_t^{m_t}$ по (ii) и положим $\chi(a) = \zeta_{n_1}^{m_1 e_1} \zeta_{n_2}^{m_2 e_2} \ldots \zeta_{n_t}^{m_t e_t}$. Нетрудно проверить, что χ будет характером. Следовательно, на A имеется $n_1 n_2 \ldots n_t = n$ характеров. Кроме того, пусть χ_i выделяется условиями $\chi_i(g_i) = \zeta_{n_i}$ и $\chi_i(g_j) = 1$ при $i \neq j$. Тогда χ_i имеет порядок n_i и $\widehat{A}$ будет прямым произведением циклических подгрупп, порожденных χ_i. Это показывает, что $A \approx \widehat{A}$.

Следующие два результата будут иметь большое значение в § 4.

Предложение 16.3.1. *Пусть A — конечная абелева группа. Если $\chi, \psi \in \widehat{A}$ и $a, b \in A$, то*

(i) $\sum_{a \in A} \chi(a) \overline{\psi(a)} = n\delta(\chi, \psi)$, *где* $\delta(\chi, \chi) = 1$ *и* $\delta(\chi, \psi) = 0$ *при* $\chi \neq \psi$;

(ii) $\sum_{\chi \in \widehat{A}} \chi(a) \overline{\chi(b)} = n\delta(a, b)$, *где* $\delta(a, a) = 1$ *и* $\delta(a, b) = 0$ *при* $a \neq b$.

Доказательство. Так как

$$\sum_{a \in A} \chi(a)\overline{\psi(a)} = \sum_{a \in A} \chi\psi^{-1}(a),$$

то для получения (i) достаточно доказать, что

$$\sum_{a \in A} \chi(a) = n \quad \text{при } \chi = \chi_0 \quad \text{и} \quad \sum_{a \in A} \chi(a) = 0 \quad \text{при} \quad \chi \neq \chi_0.$$

Первое утверждение очевидно из определения. Предположим, что $\chi \neq \chi_0$. Тогда существует такой элемент $b \in A$, что $\chi(b) \neq 1$. Имеем

$$\sum_a \chi(a) = \sum_a \chi(ba) = \chi(b) \sum_a \chi(a),$$

так что $(\chi(b) - 1)\sum_a \chi(a) = 0$. Поскольку $\chi(b) - 1 \neq 0$, отсюда следует, что $\sum_a \chi(a) = 0$.

Для доказательства утверждения (ii) мы заметим сначала, что

$$\sum_\chi \chi(a)\overline{\chi(b)} = \sum_\chi \chi(ab^{-1}).$$

Достаточно показать, что $\sum_\chi \chi(a) = n$ при $a = e$ и $\sum_\chi \chi(a) = 0$ при $a \neq e$. Первое утверждение очевидно. Предположим, что $a \neq e$. Мы утверждаем, что существует характер ψ, для которого $\psi(a) \neq 1$. Чтобы убедиться в этом, запишем $a = g_1^{m_1} g_2^{m_2} \ldots g_t^{m_t}$ с $0 \leqslant m_i < n_i$ для всех i. Так как $a \neq e$, то по крайней мере одно m_i отлично от нуля. Тогда $\chi_i(a) = \chi_i(g_i)^{m_i} = \zeta_{n_i}^{m_i} \neq 1$. Положим $\psi = \chi_i$. Тогда

$$\sum_\chi \chi(a) = \sum_\chi \psi\chi(a) = \psi(a) \sum_\chi \chi(a),$$

так что $(\psi(a) - 1)\sum_\chi \chi(a) = 0$. Поскольку $\psi(a) - 1 \neq 0$, то $\sum_\chi \chi(a) = 0$. □

Соотношения, задаваемые (i) и (ii), называются *соотношениями ортогональности*. Мы проинтерпретируем теперь эти соотношения для характеров Дирихле по модулю m. В данном случае $A = U(\mathbf{Z}/m\mathbf{Z})$. Характеры Дирихле определены на $\mathbf{Z}$, но индуцируют и сами индуцируются элементами группы характеров для $U(\mathbf{Z}/m\mathbf{Z})$. Следовательно, существует в точности $\varphi(m)$ характеров Дирихле по модулю m. Из определения и последнего предложения мы получаем

Предложение 16.3.2. *Пусть* χ *и* ψ — *характеры Дирихле по модулю* m *и* $a, b \in \mathbf{Z}$. *Тогда*

(i) $\sum_{a=0}^{m-1} \chi(a)\overline{\psi(a)} = \varphi(m)\,\delta(\chi, \psi)$;

(ii) $\sum_{\chi} \chi(a)\overline{\chi(b)} = \varphi(m)\,\delta(a, b)$.

В п. (ii) *сумма берется по всем характерам Дирихле по модулю* m *и* $\delta(a, b) = 1$ *при* $a \equiv b\ (m)$ *и* $\delta(a, b) = 0$ *при* $a \not\equiv b\ (m)$.

§ 4. L-функции Дирихле

Пусть χ — характер Дирихле по модулю m. Мы определяем *L-функцию Дирихле, соответствующую* χ, формулой

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n)\, n^{-s}.$$

Так как $|\chi(n)\, n^{-s}| \leqslant n^{-s}$, члены ряда $L(s, \chi)$ мажорируются по абсолютной величине соответствующими членами ряда $\zeta(s)$. Таким образом, ряд $L(s, \chi)$ сходится и непрерывен при $s > 1$. Кроме того, поскольку характер χ вполне мультипликативен, мы получаем представление $L(s, \chi)$ в виде произведения точно так же, как и для $\zeta(s)$. А именно,

$$L(s, \chi) = \prod_{p} (1 - \chi(p)\, p^{-s})^{-1}.$$

Так как $\chi(p) = 0$ для $p \mid m$, написанное произведение берется по положительным простым числам, не делящим m. Формула справедлива при $s > 1$.

Между $L(s, \chi_0)$ и $\zeta(s)$ имеется тесная связь. В самом деле,

$$\begin{aligned} L(s, \chi_0) &= \prod_{p \nmid m} (1 - p^{-s})^{-1} = \\ &= \prod_{p \mid m} (1 - p^{-s}) \prod_{p} (1 - p^{-s})^{-1} = \\ &= \prod_{p \mid m} (1 - p^{-s})\, \zeta(s). \end{aligned}$$

Из предложения 16.1.2 получаем, что

$$\lim_{s \to 1} (s - 1) L(s, \chi_0) = \prod_{p \mid m} (1 - p^{-1}) = \varphi(m)/m.$$

В частности, $L(s, \chi_0) \to \infty$ при $s \to 1$.

Для обобщения доказательства предложения 16.2.1 нам нужно рассмотреть $\ln L(s, \chi)$. Даже если ограничиться вещественными значениями s, значения ряда $L(s, \chi)$ в общем случае комплексные, так что необходимо учитывать, что $\ln z$ — многозначная функция комплексной переменной z. Один из способов обойти это обстоятельство состоит в определении $\ln L(s, \chi)$ бесконечным рядом.

Пусть χ — характер Дирихле. Положим

$$G(s, \chi) = \sum_p \sum_{k=1}^{\infty} (1/k) \chi(p^k) p^{-ks}.$$

Так как $|(1/k)\chi(p^k) p^{-ks}| \leqslant p^{-ks}$ и $\zeta(s)$ сходится при $s > 1$ и равномерно сходится при $s \geqslant 1 + \delta > 1$, мы можем сделать вывод о том, что те же самые утверждения имеют место для $G(s, \chi)$. Следовательно, $G(s, \chi)$ непрерывна для $s > 1$. Более того, для комплексного числа z, $|z| < 1$,

$$\exp\left(\sum_{k=1}^{\infty} (1/k) z^k\right) = (1 - z)^{-1},$$

где exp обозначает обычную экспоненциальную функцию. Подставляя сюда $z = \chi(p) p^{-s}$, получаем

$$\exp\left(\sum_{k=1}^{\infty} (1/k) \chi(p^k) p^{-ks}\right) = (1 - \chi(p) p^{-s})^{-1}.$$

Простое рассуждение в таком случае показывает, что $\exp G(s, \chi) = L(s, \chi)$ для всех $s > 1$. Таким образом, бесконечный ряд $G(s, \chi)$ дает однозначное определение функции $\ln L(s, \chi)$. Во избежание недоразумений мы будем работать непосредственно с $G(s, \chi)$.

Из определения и рассуждения, использованного при доказательстве предложения 16.1.3, получаем

$$G(s, \chi) = \sum_{p \nmid m} \chi(p) p^{-s} + R_\chi(s), \qquad \text{(i)}$$

где $R_\chi(s)$ остается ограниченным при $s \to 1$. Умножим обе части равенства (i) на $\overline{\chi(a)}$, где $a \in \mathbf{Z}$, $(a, m) = 1$. Затем произведем суммирование по всем характерам Дирихле по модулю m. В результате получим

$$\sum_\chi \overline{\chi(a)} G(\chi, s) = \sum_{p \nmid m} p^{-s} \sum_\chi \overline{\chi(a)} \chi(p) + \sum_\chi \overline{\chi(a)} R_\chi(s).$$

Воспользовавшись предложением 16.3.2, п. (ii), убеждаемся в том, что

$$\sum_\chi \overline{\chi(a)} G(s, \chi) = \varphi(m) \sum_{p \equiv a\,(m)} p^{-s} + R_{\chi, a}(s), \qquad \text{(ii)}$$

где $R_{\chi, a}(s)$ остается ограниченным при $s \to 1$.

Для завершения доказательства теоремы 1 нам понадобится следующее предложение.

Предложение 16.4.1. *Если χ_0 обозначает тривиальный характер по модулю m, то $\lim_{s \to 1} G(s, \chi_0)/\ln(s-1)^{-1} = 1$. Если χ — нетривиальный характер Дирихле по модулю m, то $G(s, \chi)$ остается ограниченным при $s \to 1$.*

Доказательство. Первое утверждение доказать нетрудно. $L(s, \chi_0)$ — вещественнозначная функция на положительных вещественных числах. Как мы видели,

$$L(s, \chi_0) = \prod_{p \mid m} (1 - p^{-s}) \zeta(s).$$

Отсюда следует, что

$$G(s, \chi_0) = \sum_{p \mid m} \ln(1 - p^{-s}) + \ln \zeta(s).$$

Нужное утверждение получается теперь из следствия предложения 16.1.2.

Второе утверждение значительно более глубокое. Оно является наиболее трудной частью в доказательстве теоремы Дирихле об арифметических прогрессиях. Доказательство его будет отложено до следующего параграфа.

Теперь же, предполагая известным сформулированное предложение, мы очень быстро получаем доказательство теоремы Дирихле из равенства (ii). Разделим все члены обеих частей на $\ln(s-1)^{-1}$ и перейдем к пределу при $s \to 1$. Согласно предложению, предел в левой части равен 1, в то время как предел в правой части равен $\varphi(m)\, d(\mathscr{P}(a; m))$. Таким образом, $d(\mathscr{P}(a; m)) = 1/\varphi(m)$, что и требовалось. □

§ 5. Ключевой шаг

До сих пор все наши функции были определены для $s > 1$. Теперь мы покажем, как расширить область определения до $s > 0$. В частности, если χ — нетривиальный характер, мы убедимся в том, что $L(1, \chi)$ — корректно определенное комплексное число, и докажем, что $L(1, \chi) \neq 0$. Это ключевой момент. Как только мы это установим, относительно просто показать, что $G(s, \chi)$ остается ограниченной при $s \to 1$. Именно это осталось недоказанным в § 4.

В последующем изложении мы будем считать s комплексной переменной. Запишем $s = \sigma + it$, где σ и t вещественные. Сим-

вол σ будет использоваться далее для обозначения вещественной части s.

Если $a > 0$ вещественно, то $|a^s| = a^\sigma$. Отсюда видно, что ряды, определяющие $\zeta(s)$ и $L(s, \chi)$, сходятся и задают аналитические функции комплексной переменной s в полуплоскости $\{s \in \mathbf{C} \mid \sigma > 1\}$.

Лемма 1. *Пусть* $\{a_n\}$ *и* $\{b_n\}$ *при* $n = 1, 2, 3, \ldots$ — *такие последовательности комплексных чисел, что ряд* $\sum\limits_{n=1}^{\infty} a_n b_n$ *сходится. Положим* $A_n = a_1 + a_2 + \ldots + a_n$ *и предположим, что* $A_n b_n \to 0$ *при* $n \to \infty$. *Тогда*

$$\sum_{n=1}^{\infty} a_n b_n = \sum_{n=1}^{\infty} A_n (b_n - b_{n+1}).$$

Доказательство. Пусть $S_N = \sum\limits_{n=1}^{N} a_n b_n$. Положим $A_0 = 0$. Тогда

$$\begin{aligned} S_N &= \sum_{n=1}^{N} (A_n - A_{n-1}) b_n = \sum_{n=1}^{N} A_n b_n - \sum_{n=1}^{N} A_{n-1} b_n = \\ &= \sum_{n=1}^{N} A_n b_n - \sum_{n=1}^{N-1} A_n b_{n+1} = \\ &= A_N b_N + \sum_{n=1}^{N-1} A_n (b_n - b_{n+1}). \end{aligned}$$

Переход к пределу при $N \to \infty$ приводит к нужному результату. □

Предложение 16.5.1. $\zeta(s) - (s-1)^{-1}$ *можно продолжить до аналитической функции в области* $\{s \in \mathbf{C} \mid \sigma > 0\}$.

Доказательство. Предположим, что $\sigma > 1$. Тогда по лемме 1

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \sum_{n=1}^{\infty} n \left(n^{-s} - (n+1)^{-s}\right).$$

Напомним, что $[x]$ для вещественного числа x есть наибольшее целое число, меньшее или равное x, и $\langle x \rangle = x - [x]$. Из приведенного выше выражения для $\zeta(s)$ получаем, что

$$\begin{aligned} \zeta(s) &= s \sum_{n=1}^{\infty} n \int_n^{n+1} x^{-s-1}\, dx = \\ &= s \sum_{n=1}^{\infty} \int_n^{n+1} [x]\, x^{-s-1}\, dx = \end{aligned}$$

$$= s \int_1^\infty [x]\, x^{-s-1}\, dx =$$

$$= s \int_1^\infty x^{-s}\, dx - s \int_1^\infty \langle x \rangle\, x^{-s-1}\, dx =$$

$$= \frac{s}{s-1} - s \int_1^\infty \langle x \rangle\, x^{-s-1}\, dx.$$

Так как $|\langle x \rangle| \leqslant 1$ при всех x, последний интеграл сходится и определяет аналитическую функцию при $\sigma > 0$, откуда и следует доказываемый результат. □

Тем же самым способом мы воспользуемся для продолжения ряда $L(s, \chi)$, но сначала нам понадобится еще одна лемма.

Лемма 2. *Пусть χ — некоторый нетривиальный характер по модулю m. Для всех $N > 0$*

$$\left| \sum_{n=0}^{N} \chi(n) \right| \leqslant \varphi(m).$$

Доказательство. Запишем $N = qm + r$, где $0 \leqslant r < m$. Так как $\chi(n + m) = \chi(n)$ при всех n, то

$$\sum_{n=1}^{N} \chi(n) = q \left(\sum_{n=0}^{m-1} \chi(n) \right) + \sum_{n=0}^{r} \chi(n).$$

В силу предложения 16.3.2 (п. (i)) $\sum\limits_{n=0}^{m-1} \chi(n) = 0$. Поэтому

$$\left| \sum_{n=0}^{N} \chi(n) \right| = \left| \sum_{n=0}^{r} \chi(n) \right| \leqslant \sum_{n=0}^{m-1} |\chi(n)| = \varphi(m). \qquad \square$$

Предложение 16.5.2. *Пусть χ — нетривиальный характер Дирихле по модулю m. Тогда $L(s, \chi)$ можно продолжить до аналитической функции в области $\{s \in \mathbf{C} \mid \sigma > 0\}$.*

Доказательство. Положим $S(x) = \sum\limits_{n \leqslant x} \chi(n)$.

В силу леммы 1 для $\sigma > 1$

$$L(s, \chi) = \sum_{n=1}^{\infty} S(n) \left(n^{-s} - (n+1)^{-s} \right) =$$

$$= s \sum_{n=1}^{\infty} S(n) \int_{n}^{n+1} x^{-s-1}\, dx =$$

$$= s \int_{1}^{\infty} S(x) x^{-s-1}\, dx.$$

По лемме 2 $|S(x)| \leqslant \varphi(m)$ для всех x. Отсюда следует, что написанный выше интеграл сходится и определяет аналитическую функцию для всех s с $\sigma > 0$. □

Наша цель теперь — показать, что $L(1, \chi) \neq 0$ для нетривиального характера χ. Следующее предложение даст нам возможность получить простое доказательство этого факта в случае, когда χ — комплексный характер, т. е. характер, принимающий невещественные значения.

Предложение 16.5.3. *Пусть* $F(s) = \prod_{\chi} L(s, \chi)$, *где произведение берется по всем характерам Дирихле по модулю* m. *Тогда* $F(s) \geqslant 1$ *при вещественном* $s > 1$.

Доказательство. Предположим, что s вещественное и $s > 1$. Напомним, что

$$G(s, \chi) = \sum_{p} \sum_{k=1}^{\infty} \frac{1}{k} \chi(p^k) p^{-ks}.$$

Суммируя по χ и используя предложение 16.3.2, п. (ii), получаем

$$\sum_{\chi} G(s, \chi) = \varphi(m) \sum \frac{1}{k} p^{-ks},$$

где сумма берется по всем простым p и целым числам k, для которых $p^k \equiv 1\ (m)$.

Правая часть последнего равенства неотрицательна (на самом деле она положительна). Взятие экспоненты от обеих частей показывает, что $\prod_{\chi} L(s, \chi) \geqslant 1$, как и утверждалось. □

Предложение 16.5.4. *Если* χ — *нетривиальный комплексный характер по модулю* m, *то* $L(1, \chi) \neq 0$.

Доказательство. Ряд, определяющий $L(s, \chi)$, показывает, что для вещественного s, $s > 1$, $\overline{L(s, \chi)} = L(s, \bar{\chi})$. Устремляя s к 1, получаем, что из $L(1, \chi) = 0$ следует $L(1, \bar{\chi}) = 0$.

Предположим, что $L(1, \chi) = 0$, где χ — комплексный характер. Функции $L(s, \chi)$ и $L(s, \bar{\chi})$ различны и обе имеют в силу нашего предположения нуль в $s = 1$. В произведении $F(s) = \prod_{\chi} L(s, \chi)$, как мы знаем, $L(s, \chi_0)$ имеет простой полюс в $s = 1$, а все другие множители аналитичны в $s = 1$. Отсюда следует, что $F(1) = 0$. В то же время предложение 16.5.3 показывает, что $F(s) \geqslant 1$ для всех вещественных $s > 1$ (противоречие). Поэтому $L(1, \chi) \neq 0$. □

Остается рассмотреть случай, когда χ — некоторый нетривиальный вещественный характер, т. е. когда $\chi(n) = 0$, 1 или -1 для всех $n \in \mathbf{Z}$. Дирихле смог доказать, что $L(1, \chi) \neq 0$, используя свою формулу для числа классов квадратичных числовых полей (точнее, для числа классов эквивалентности бинарных квадратичных форм фиксированного дискриминанта). Мы воспользуемся изящным доказательством Валле-Пуссена (1896 г.), следуя изложению в [119].

Лемма 3. *Предположим, что f — неотрицательная мультипликативная функция на $\mathbf{Z}^+$, т. е. $f(mn) = f(m) f(n)$ для всех m, $n > 0$, таких, что $(m, n) = 1$. Предположим, что существует такая константа c, что $f(p^k) < c$ для всех степеней простых чисел p^k. Тогда ряд $\sum_{n=1}^{\infty} f(n) n^{-s}$ сходится для всех вещественных $s > 1$. Кроме того,*

$$\sum_{n=1}^{\infty} f(n) n^{-s} = \prod_{p} \left(1 + \sum_{k=1}^{\infty} f(p^k) p^{-ks}\right).$$

Доказательство. Фиксируем $s > 1$. Пусть $a(p) = \sum_{k=1}^{\infty} f(p^k) p^{-ks}$. Тогда $a(p) < cp^{-s} \sum_{k=0}^{\infty} p^{-ks} = cp^{-s}(1 - p^{-s})^{-1}$, а потому $a(p) < 2cp^{-s}$. Для положительного x имеем $1 + x < \exp x$. Таким образом,

$$\prod_{p \leqslant N} (1 + a(p)) < \prod_{p \leqslant N} \exp a(p) = \exp \sum_{p \leqslant N} a(p).$$

Далее, $\sum_{p \leqslant N} a(p) < 2c \sum_{p} p^{-s} = M$. Из определения $a(p)$ и мультипликативности f следует, что

$$\sum_{n=1}^{N} f(n) n^{-s} < \prod_{p \leqslant N} (1 + a(p)).$$

Отсюда вытекает, что $\sum_{n=1}^{N} f(n) n^{-s} < \exp M$ для всех N. Так как f по предположению неотрицательна, мы получаем, что $\sum_{n=1}^{\infty} f(n) n^{-s}$ сходится.

Последнее утверждение леммы получается при помощи рассуждения, использованного в доказательстве предложения 16.1.1. □

Теорема 2. *Пусть χ — нетривиальный характер Дирихле по модулю m. Тогда $L(1, \chi) \neq 0$.*

Доказательство. Доказав уже, что $L(1, \chi) \neq 0$ для комплексного характера χ, мы предполагаем χ вещественным.

Предположим, что $L(1, \chi) = 0$, и рассмотрим функцию

$$\psi(s) = \frac{L(s, \chi) L(s, \chi_0)}{L(2s, \chi_0)}.$$

Нуль $L(s, \chi)$ в $s = 1$ уничтожает простой полюс $L(s, \chi_0)$, так что числитель аналитичен при $\sigma > 0$. Знаменатель отличен от нуля и аналитичен при $\sigma > 1/2$. Таким образом, $\psi(s)$ аналитична при $\sigma > 1/2$. Кроме того, так как $L(2s, \chi_0)$ имеет полюс в $s = 1/2$, то $\psi(s) \to 0$ при $s \to 1/2$.

Мы предположим временно, что s вещественно и $s > 1$. Тогда $\psi(s)$ имеет такое разложение в бесконечное произведение:

$$\psi(s) = \prod (1 - \chi(p) p^{-s})^{-1} (1 - \chi_0(p) p^{-s})^{-1} (1 - \chi_0(p) p^{-2s}) =$$

$$= \prod_{p \nmid m}^{p} \frac{(1 - p^{-2s})}{(1 - p^{-s})(1 - \chi(p) p^{-s})}.$$

Если $\chi(p) = -1$, то p-множитель равен 1. Следовательно,

$$\psi(s) = \prod_{\chi(p)=1} \frac{1 + p^{-s}}{1 - p^{-s}},$$

где произведение берется по всем p с $\chi(p) = 1$. Далее,

$$\frac{1 + p^{-s}}{1 - p^{-s}} = (1 + p^{-s}) \left(\sum_{k=0}^{\infty} p^{-ks} \right) = 1 + 2p^{-s} + 2p^{-2s} + \ldots.$$

Применяя лемму 3, получаем, что $\psi(s) = \sum_{n=1}^{\infty} a_n n^{-s}$, где $a_n \geqslant 0$ и ряд сходится для $s > 1$. Заметим, что $a_1 = 1$. (Можно, но не нужно получить явную формулу для a_n.)

Мы опять возвращаемся к рассмотрению $\psi(s)$ как функции комплексной переменной. Разложим ее в степенной ряд в окрестности точки $s = 2$:

$$\psi(s) = \sum_{m=0}^{\infty} b_m (s-2)^m.$$

Так как $\psi(s)$ аналитична для $\sigma > 1/2$, то радиус сходимости последнего ряда не меньше $3/2$. Для вычисления b_m мы воспользуемся теоремой Тейлора, т. е. $b_m = \psi^{(m)}(2)/m!$, где $\psi^{(m)}(s)$ есть m-я производная функции $\psi(s)$. Так как $\psi(s) = \sum_{n=1}^{\infty} a_n n^{-s}$, то

$$\psi^{(m)}(2) = \sum_{n=1}^{\infty} a_n (-\ln n)^m n^{-2} = (-1)^m c_m$$

с $c_m \geqslant 0$. Таким образом,

$$\psi(s) = \sum_{n=0}^{\infty} c_m (2-s)^m$$

с неотрицательными c_m и

$$c_0 = \psi(2) = \sum_{n=1}^{\infty} a_n n^{-2} \geqslant a_1 = 1.$$

Отсюда следует, что $\psi(s) \geqslant 1$ для вещественного s в интервале $(1/2, 2)$. Это противоречит тому, что $\psi(s) \to 0$ при $s \to 1/2$, а значит, $L(1, \chi) \neq 0$. □

Мы теперь в состоянии доказать предложение 16.4.1. Предположим, что χ — некоторый нетривиальный характер Дирихле. Мы хотим показать, что $G(s, \chi)$ остается ограниченной при $s \to 1$ по вещественным значениям $s > 1$.

Так как $L(1, \chi) \neq 0$, существует такой круг D с центром в $L(1, \chi)$, что $0 \notin D$. Пусть $\ln z$ — однозначная ветвь логарифма, определенная на D. Существует такое $\delta > 0$, что $L(s, \chi) \in D$ для $s \in (1, 1+\delta)$. Рассмотрим $\ln L(s, \chi)$ и $G(s, \chi)$ для s в этом интервале. Экспонента от обеих функций равна $L(s, \chi)$. Следовательно, существует такое целое число N, для которого $G(s, \chi) = 2\pi i N + \ln L(s, \chi)$ при $s \in (1, 1+\delta)$. Это означает, что $\lim_{s \to 1} G(s, \chi)$ существует и равен $2\pi i N + \ln L(1, \chi)$. Так как $G(s, \chi)$ имеет предел при $s \to 1$, она, очевидно, ограничена.

§ 6. Значения $L(s, \chi)$ в отрицательных целых числах

В последнем параграфе мы показали, как аналитически продолжить $L(s, \chi)$ в область $\{s \in \mathbf{C} \mid \sigma > 0\}$. Риман показал, как аналитически продолжить эти функции на всю комплексную

плоскость [1]). Как отмечалось ранее, этот факт имеет большое значение для теории чисел. Например, значения $L(1-k, \chi)$, где k — положительное целое число, тесно связаны с числами Бернулли. Эти же числа имеют глубокие связи с теорией круговых полей. Мы аналитически продолжим $L(s, \chi)$ и вычислим числа $L(1-k, \chi)$, следуя методу из [141].

Предварительно нам нужно рассмотреть некоторые свойства Г-функции. Последняя определена равенством

$$\Gamma(s) = \int_0^\infty e^{-t} t^{s-1}\, dt. \tag{i}$$

Нетрудно убедиться в том, что этот интеграл сходится и определяет аналитическую функцию в области $\{s \in \mathbf{C} \mid \sigma > 0\}$. Для $\sigma > 1$ мы производим интегрирование по частям и получаем

$$\Gamma(s) = -e^{-t} t^{s-1}\Big|_0^\infty + (s-1) \int_0^\infty e^{-t} t^{s-2}\, dt.$$

Отсюда следует, что $\Gamma(s) = (s-1)\,\Gamma(s-1)$ для $\sigma > 1$. Так как

$$\Gamma(1) = \int_0^\infty e^{-t}\, dt = 1,$$

то $\Gamma(n+1) = n!$ для положительных целых чисел n.

Функциональное уравнение $\Gamma(s) = (s-1)\,\Gamma(s-1)$ позволяет нам аналитически продолжать $\Gamma(s)$ шаг за шагом.

При $\sigma > -1$ определим $\Gamma_1(s)$ формулой

$$\Gamma_1(s) = \frac{1}{s}\,\Gamma(s+1). \tag{ii}$$

При $\sigma > 0$ имеем $\Gamma_1(s) = \Gamma(s)$. Кроме того, $\Gamma_1(s)$ аналитична при $\sigma > -1$, за исключением простого полюса в $s = 0$.

Аналогично, если k — некоторое положительное целое число, полагаем

$$\Gamma_k(s) = \frac{1}{s(s+1)\ldots(s+k-1)}\,\Gamma(s+k).$$

$\Gamma_k(s)$ аналитична в области $\{s \in \mathbf{C} \mid \sigma > -k\}$, за исключением простых полюсов в $s = 0,\ 1, \ldots, 1-k$, и $\Gamma_k(s) = \Gamma(s)$ при

---

[1]) И показал, что для них выполняется функциональное уравнение, которое в случае дзета-функции Римана $\zeta(s)$ имеет вид $\pi^{-s/2}\,\Gamma(s/2)\,\zeta(s) = \pi^{-(1-s)/2} \cdot \Gamma((1-s)/2)\,\zeta(1-s)$ (см. элементарное доказательство в [169], гл. 20, § 2, и дальнейшие обобщения в [8*], [168], [44]). — *Прим. ред.*

$\sigma > 0$. Эти функции вместе задают аналитическое продолжение $\Gamma(s)$ на всю комплексную плоскость с полюсами в неположительных целых числах и нигде больше. Начиная с этого места, $\Gamma(s)$ будет обозначать эту продолженную функцию. Мы заметим (без доказательства), что $\Gamma(s)^{-1}$ — целая функция.

Мы покажем теперь, как аналитически продолжить $\zeta(s)$ тем же способом. Нужно представить $\zeta(s)$ в виде интеграла. В равенстве (i) подставим nt вместо t. При $\sigma > 1$ получаем

$$n^{-s}\Gamma(s) = \int_0^\infty e^{-nt} t^{s-1}\, dt. \tag{iii}$$

Просуммируем обе части равенства (iii) для $n = 1, 2, 3, \ldots$. Нетрудно убедиться в том, что суммирование и интегрирование перестановочны. В результате получим

$$\Gamma(s)\zeta(s) = \int_0^\infty \frac{e^{-t}}{1 - e^{-t}}\, t^{s-1}\, dt. \tag{iv}$$

При попытке произвести интегрирование по частям интеграла в таком виде нам помешает тот факт, что $1 - e^{-t}$ равно нулю при $t = 0$. Чтобы обойти это препятствие, мы применим искусственный прием. В равенство (iv) подставим $2t$ вместо t:

$$2^{1-s}\Gamma(s)\zeta(s) = 2\int_0^\infty \frac{e^{-2t}}{1 - e^{-2t}}\, t^{s-1}\, dt. \tag{v}$$

Определим функции $\zeta^*(s) = (1 - 2^{1-s})\,\zeta(s)$ и $R(x) = x/(1 - x) - 2(x^2/(1 - x^2))$. Вычитая (v) из (iv), получаем

$$\Gamma(s)\zeta^*(s) = \int_0^\infty R(e^{-t})\, t^{s-1}\, dt. \tag{vi}$$

Чего мы добились? Простое алгебраическое преобразование показывает, что $R(x) = x/(1 + x)$. Таким образом, $R(e^{-t}) = e^{-t}/(1 + e^{-t})$ имеет знаменатель, который не обращается в нуль при $t = 0$. Интеграл в равенстве (vi), таким образом, сходится при $\sigma > 0$ и это равенство задает продолжение функции $\zeta(s)$ на область $\{s \in \mathbf{C} \mid \sigma > 0\}$.

Пусть $R_0(t) = R(e^{-t})$ и $R_m(t) = (d^m/dt^m)\, R(e^{-t})$ при $m \geqslant 1$. Нетрудно убедиться в том, что $R_m(t) = e^{-t}P_m(e^{-t})\,(1 + e^{-t})^{-2m-1}$, где P_m — многочлен. Отсюда следует, что $R_m(0)$ конечно и что $R_m(t)/e^{-t}$ ограничена при $t \to \infty$. Эти факты позволяют нам повторно производить интегрирование по частям в равенстве (vi).

Положим $u = R(e^{-t})$ и $dv = t^{s-1}\,dt$. Тогда $du = R_1(t)\,dt$ и $v = t^s/s$. Таким образом,

$$\Gamma(s)\zeta^*(s) = \frac{1}{s}\,t^s R_0(t)\Big|_0^\infty - \frac{1}{s}\int_0^\infty R_1(t)\,t^s\,dt,$$

так что

$$\Gamma(s+1)\zeta^*(s) = -\int_0^\infty R_1(t)\,t^s\,dt. \tag{vii}$$

Интеграл в (vii) сходится к аналитической функции в области $\{s \in \mathbf{C} \mid \sigma > -1\}$ и задает аналитическое продолжение функции $\zeta(s)$ в этой области. Продолжая этот процесс, мы получаем при положительном целом числе k

$$\Gamma(s+k)\zeta^*(s) = (-1)^k \int_0^\infty R_k(t)\,t^{s+k-1}\,dt, \tag{viii}$$

где интеграл сходится к аналитической функции от s для $\sigma > -k$. Этот способ определяет аналитическое продолжение функции $\zeta(s)$ на всю комплексную плоскость. Для этой продолженной функции мы продолжаем использовать обозначения $\zeta(s)$.

Предложение 16.6.1. *Пусть k — положительное целое число. Тогда $\zeta(0) = -1/2$ и $\zeta(1-k) = -B_k/k$ для $k > 1$, где B_k есть k-е число Бернулли.*

Доказательство. В равенство (viii) подставим $s = 1 - k$. В результате получим

$$\zeta^*(1-k) = (-1)^k \int_0^\infty R_k(t)\,dt.$$

Так как $R_k(t) = (d/dt)\,R_{k-1}(t)$, то $(1-2^k)\,\zeta(1-k) = (-1)^{k-1}\,R_{k-1}(0)$. По определению $R_{k-1}(t)$ есть $(k-1)$-я производная от

$$\frac{e^{-t}}{1-e^{-t}} - 2\,\frac{e^{-2t}}{1-e^{-2t}} = \frac{1}{t}\left(\frac{t}{e^t-1} - \frac{2t}{e^{2t-1}}\right).$$

В силу теоремы Тейлора $R_{k-1}(0)$ есть $(k-1)!$, умноженное на коэффициент при t^{k-1} в разложении в степенной ряд этой функции в $t = 0$. Так как

$$t/(e^t - 1) = \sum_{k=0}^\infty B_k/k!,$$

то $\zeta(1-k) = (-1)^{k-1} B_k/k$. Если $k = 1$, то $\zeta(0) = B_1 = -1/2$. Если $k > 1$ и нечетно, то $B_k = 0$. Таким образом, $\zeta(1-k) = -B_k/k$ для $k > 1$. □

Предположим теперь, что χ — некоторый нетривиальный характер по модулю m. При рассмотрении $L(s, \chi)$ мы поступаем точно так же, как и при рассмотрении $\zeta(s)$. Умножим обе части равенства (iii) на $\chi(n)$ и просуммируем их по n. В результате получим

$$\Gamma(s) L(s, \chi) = \int_0^\infty F_\chi(e^{-t})\, t^{s-1}\, dt,$$

где

$$F_\chi(e^{-t}) = \sum_{n=1}^{\infty} \chi(n) e^{-nt} = \sum_{a=1}^{m} \chi(a) \sum_{k=0}^{\infty} e^{-(a+km)t} =$$

$$= \sum_{a=1}^{m} \chi(a) \frac{e^{-at}}{1-e^{-mt}}.$$

Если положить $L^*(s, \chi) = (1-2^{1-s}) L(s, \chi)$, то тем же способом, как было получено равенство (vi), получаем

$$\Gamma(s) L^*(s, \chi) = \int_0^\infty R_\chi(e^{-t})\, t^{s-1}\, dt, \tag{ix}$$

где

$$R_\chi(x) = F_\chi(x) - 2F_\chi(x^2) =$$

$$= \sum_{a=1}^{m} \chi(a) \left(\frac{x^a}{1-x^m} - 2\frac{x^{2a}}{1-x^{2m}} \right) =$$

$$= \sum_{a=1}^{m} \chi(a)\, x^a \left(\frac{1+x^m-2x^a}{(1-x)(1+x+\cdots+x^{2m-1})} \right).$$

Для каждого значения a $x = 1$ будет корнем многочлена $1 + x^m - 2x^a$, откуда следует, что $R_\chi(x)$ имеет вид

$$R_\chi(x) = \frac{xf(x)}{1+x+\cdots+x^{2m-1}},$$

где $f(x)$ — многочлен. Положим $R_{\chi,0}(t) = R_\chi(e^{-t})$ и $R_{\chi,n}(t) = (d^n/dt^n) R_\chi(e^{-t})$. Повторным интегрированием по частям тем же

самым способом, каким было получено равенство (viii), находим, что

$$\Gamma(s+k)L^*(s,\ \chi) = (-1)^k \int\limits_0^\infty R_{\chi,k}(t)\, t^{s+k-1}\, dt. \qquad \text{(x)}$$

Интеграл в (x) сходится к аналитической функции в $\{s \in \mathbf{C} \mid \sigma > -k\}$. Эти формулы задают аналитическое продолжение функции $L^*(s, \chi)$, а потому и $L(s, \chi)$, на всю комплексную плоскость.

Перед тем как приступить к вычислению $L(s, \chi)$ в отрицательных целых числах, приведем еще одно определение.

Определение. Пусть χ — некоторый нетривиальный характер Дирихле по модулю m. *Обобщенные числа Бернулли* $B_{n,\chi}$ определяются следующей формулой:

$$\sum_{a=1}^{m} \chi(a)\, \frac{te^{at}}{e^{mt}-1} = \sum_{n=0}^{\infty} \frac{B_{n,\chi}}{n!}\, t^n. \qquad \text{(xi)}$$

В литературе обычно определяют $B_{n,\chi}$ этим способом лишь в случае, когда χ — примитивный характер по модулю m. Мы возвратимся к этому вопросу позже.

Лемма 1. $tF_\chi(e^{-t}) = \sum\limits_{n=0}^{\infty} (-1)^n (B_{n,\chi}/n!)\, t^n$.

Доказательство. Нужно подставить $-t$ вместо t в равенство (xi). □

Предложение 16.6.2. *Пусть k — положительное целое число. Тогда* $L(1-k, \chi) = -B_{k,\chi}/k$.

Доказательство. В равенство (x) подставим $s = 1-k$. В результате получим

$$(1-2^k)\, L(1-k,\ \chi) = (-1)^k \int\limits_0^\infty R_{\chi,k}(t)\, dt.$$

Так как $R_{\chi,k}(t) = (d/dt)\, R_{\chi,k-1}(t)$, отсюда следует, что $(1-2^k)\, L(1-k, \chi) = (-1)^{k-1} R_{\chi,k-1}(0)$. Так как

$$R_{\chi,k-1}(t) = \frac{d^{k-1}}{dt^{k-1}} R_\chi(e^{-t})$$

и

$$R_\chi(e^{-t}) = F_\chi(e^{-t}) - 2F_\chi(e^{-2t}) =$$

$$= (1/t)\sum_{k=1}^{\infty}(-1)^k(1-2^k)(B_{k,\chi}/k!)\,t^k \quad \text{(по лемме 1)},$$

то $(-1)^{k-1} R_{\chi, k-1}(0) = -(1-2^k)(B_{k,\chi}/k)$. Таким образом, $L(1-k, \chi) = -B_{k,\chi}/k$, как и утверждалось. □

Из равенства (xi) следует, что числа $B_{k,\chi}$ лежат в поле, порожденном над $\mathbf{Q}$ значениями характера χ. Значит, в частности, они являются алгебраическими числами.

Как уже упоминалось, обычно числа $B_{n,\chi}$ определяются равенством (xi) лишь в случае, когда χ — примитивный характер по модулю m. Это означает, что ограничение χ на $\{n \in \mathbf{Z} \mid (n, m) = 1\}$ имеет порядок, не меньший чем m. Тривиальный характер примитивен лишь для модуля 1. В этом случае мы получаем из равенства (xi)

$$\sum_{n=0}^{\infty}\frac{B_{n,\chi_0}}{n!}t^n = \frac{te^t}{e^t-1} = t + \frac{t}{e^t-1} = 1 + \frac{1}{2}t + \sum_{n=2}^{\infty}\frac{B_n}{n!}t^n.$$

Таким образом, $-B_{1,\chi_0} = B_1$ и $B_{n,\chi_0} = B_n$ для $n \geqslant 2$. Это объясняет, почему $B_{n,\chi}$ называются обобщенными числами Бернулли.

Числа $B_{n,\chi}$ обладают многими интересными арифметическими свойствами. Заинтересованному читателю следует обратиться к гл. 2 монографии [155]. Эта монография посвящена доказательству того, что равенство $L(1-k, \chi) = -B_{k,\chi}/k$ приводит к p-адическим L-функциям и к замечательной связи между этими функциями и теорией круговых полей. Другой подход к этому кругу вопросов содержится в книгах [167], [171] (и [24*], [31*]. — *Ред.*). Более доступное для начинающих изложение имеется в книге [162].

Замечания

Лежандр безуспешно пытался доказать существование бесконечного числа простых чисел в арифметической прогрессии $a + bn$, $(a, b) = 1$. Дирихле отмечал, что после того, как ему не удалось преодолеть трудности, возникавшие при завершении рассуждений Лежандра, он был вынужден приступить к изучению одного класса бесконечных рядов и произведений, аналогичных тем, которые рассматривались Эйлером (см. [124]). Результаты исследования Дирихле оказали значительное воздействие

на развитие алгебраической и аналитической теории чисел. В дополнение к доказательству существования простых чисел в произвольной арифметической прогрессии Дирихле смог, воспользовавшись развитой им аналитической техникой, получить явные формулы, часть которых была сформулирована в виде гипотезы Якоби (см. замечания к гл. 14), для числа классов квадратичных числовых полей. Например, если p — некоторое простое число >3, то число классов поля $\mathbf{Q}(\sqrt{-p})$ равно $(\pi/\sqrt{p})\,L(1, \chi)$, где χ — характер Дирихле, соответствующий символу Лежандра. Хорошее известное выражение $(-\sum x\chi(x))/p$ для числа классов получается отсюда приведением $L(1, \chi)$ к конечному виду (см. [9], с. 364). Последнее в свою очередь получается с использованием значений классических сумм Гаусса. Так как числа классов положительны, этот подход показывает, что $L(1, \chi) \neq 0$.

Если F — нормальное расширение поля $\mathbf{Q}$ степени n, то, развивая методы этой главы, можно показать, что множество простых чисел p, которые полностью разлагаются в F, т. е. которые являются произведением n различных простых идеалов в F, имеет плотность Дирихле $1/n$. В качестве следствия можно показать, что если $f(x)$ — некоторый неприводимый многочлен с целыми коэффициентами, то множество простых чисел p, для которых $f(x)$ будет произведением линейных множителей по модулю p, имеет плотность $1/n$, где n — степень поля разложения многочлена $f(x)$.

Обобщенные числа Бернулли для квадратичных характеров появляются в [153]. В этой статье Гурвиц получает функциональное уравнение для $L(s, \chi)$ с квадратичным характером χ, рассматривая частичные дзета-функции $\sum_{t=0}^{\infty} 1/(mt + a)^s$. Значения в отрицательных целых числах этих последних функций можно найти либо классическим методом, либо методом Госса, как это было сделано в данной главе. Подходящая линейная комбинация этих значений приводит затем к выражению для $L(1 - k, \chi)$ (предложение 16.6.2). Анкени, Артин и Чоула также ввели обобщенные числа Бернулли для квадратичных характеров в связи с некоторыми замечательными сравнениями, которые содержат число классов вещественного квадратичного поля и компоненты фундаментальной единицы [86]. Определение и основные свойства обобщенных чисел Бернулли приведены у Леопольда [178], который использует их в другом месте для получения обобщения на произвольное абелево расширение поля $\mathbf{Q}$ критерия Куммера делимости числа классов для $\mathbf{Q}(\zeta_p)$ (см. замечание после теоремы 4 гл. 15). В этой статье Леопольд доказывает теорему типа теоремы Клаусcена—фон Штаудта для $B_{n,\chi}$. См. также [104] и монографию о p-адических L-функциях [155].

Упражнения

1. Используя метод § 2, вычислить плотность множества простых чисел, сравнимых с 1 по модулю 3.

2. Пусть $p_1, \ldots, p_n$ — простые числа, сравнимые с 1 по модулю 4. Показать, что если p — простое число, делящее $\left(2\prod_{i=1}^{n} p_i\right)^2 + 1$, то $p \equiv 1$ (4) и $p \neq p_i$, $i = 1, \ldots, n$.

3. Вычислить множество характеров Дирихле по модулю 8 и по модулю 12.

4. Пусть χ — нетривиальный характер Дирихле по модулю 3. Показать, что

$$L(1, \chi) = \sum_{n=0}^{\infty} \frac{1}{(3n+1)(3n+2)}.$$

Можете ли вы найти точное значение для $L(1, \chi)$? (См. упр. 8.)

5. Воспользоваться теоремой 2 из гл. 13 для определения плотности Дирихле множества простых чисел, которые разлагаются на 4 различных простых идеала в кольце целых чисел поля $\mathbf{Q}(\zeta)$, $\zeta = e^{2\pi i/5}$.

6. Обобщить упр. 5 на поле $\mathbf{Q}(\zeta_m)$ при произвольном m.

7. Рассматривая $\Phi_m(x)$ по модулю p, дать алгебраическое доказательство того, что в прогрессии $mk+1$, $k = 1, 2, 3, \ldots$, существует бесконечно много простых чисел.

8. Пусть $g(\chi)$ — классическая сумма Гаусса $\sum_{x=1}^{p-1} \chi(x)\zeta^x$, χ — символ Лежандра, $\zeta = e^{2\pi i/p}$, p — простое число. Положим $P = \prod(1-\zeta^n)\prod(1-\zeta^r)^{-1}$, где n, r пробегают соответственно неквадраты и квадраты по модулю p. Показать, что

$$P = \exp(g(\chi)\, L(1, \chi)).$$

9. Воспользовавшись упр. 8, вычислить $L(1, \chi)$, где χ — нетривиальный квадратичный характер по модулю 5.

10 (Чоула). При тех же обозначениях, что и в упр. 8, показать, что $P \neq 1$ (а следовательно, $L(1, \chi) \neq 0$!!) следующим образом. Обозначим через C какой-нибудь неквадрат по модулю p. Доказать, что если $P = 1$, то

$$1 + x + \cdots + x^{p-1} \left| \prod \left(\frac{1 - x^{Cr}}{1 - x^r} \right) - 1. \right.$$

Конкретизируя x, получить противоречие!

11. Используя теорему Дирихле, показать, что существует нормальное расширение поля $\mathbf{Q}$ с любой заданной конечной циклической группой в качестве группы автоморфизмов.

12. Из теоремы Дирихле получить неприводимость над $\mathbf{Q}$ кругового многочлена $\Phi_n(x)$ ([166], т. 2).

13. Пусть χ — некоторый характер Дирихле по модулю m, $\chi(2) \neq 0$. Показать, что

$$L(s, \chi) = (1 - 2^{-s}\chi(2))^{-1} \sum_{n=0}^{\infty} \frac{\chi(2n+1)}{(2n+1)^s}.$$

Следующие упражнения, извлеченные из [193], дают короткое доказательство того, что на интервале $[1, (p-1)/2]$ для $p \equiv 3\ (4)$, p — простое число, имеется больше квадратов, чем неквадратов. В упр. 14—17 $p \equiv 3\ (4)$.

14. Пусть $p \equiv 3\ (4)$. Показать, что

$$\sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \sin \frac{2\pi x}{p} = \sqrt{p}.$$

15. Используя упр. 14, показать, что

$$\sum_{n \equiv 1\ (2)} \left(\frac{n}{p}\right) \frac{1}{n} = \frac{1}{\sqrt{p}} \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \sum_{m \equiv 1\ (2)} \frac{\sin(2\pi t m/p)}{m}.$$

[*Указание*. Заменить x на nt и просуммировать.]

16. Используя элементарный факт из анализа Фурье о том, что

$$\sum_{n=1}^{\infty} \frac{\sin(2n-1)x}{2n-1} = \begin{cases} \pi/4, & 0 < x < \pi, \\ -\pi/4, & \pi < x < 2\pi, \end{cases}$$

показать, что

$$\sum_{n \equiv 1\ (2)} \left(\frac{n}{p}\right) \frac{1}{n} = \frac{\pi}{4\sqrt{p}} \left[\sum_{t=1}^{(p-1)/2} \left(\frac{t}{p}\right) - \sum_{t=(p+1)/2}^{p-1} \left(\frac{t}{p}\right) \right] =$$

$$= \frac{\pi}{2\sqrt{p}} \sum_{t=1}^{(p-1)/2} \left(\frac{t}{p}\right).$$

17. Так как $\sum_{t=1}^{(p-1)/2} (t/p) \neq 0$ (почему?), вывести отсюда, что $\sum_{n \equiv 1\ (2)} (n/p) \cdot (1/n) > 0$ и, таким образом, $\sum_{t=1}^{(p-1)/2} (t/p) > 0$. Напомним, что $p \equiv 3\ (4)$.

18. Пусть $m \geqslant 2$, $(a, m) = 1$. Если a имеет порядок f в группе единиц по модулю m, то показать, что существует бесконечно много простых чисел p, для которых $(p) = P_1 \dots P_t$, $t = \varphi(m)/f$, P_i — различные простые идеалы в $\mathbf{Q}(\zeta_m)$. Какова плотность этого множества простых чисел?

Глава 17

ДИОФАНТОВЫ УРАВНЕНИЯ

В гл. 10 мы рассматривали диофантовы уравнения над конечными полями. В этой главе мы рассматриваем диофантовы уравнения частного вида с целыми коэффициентами и ищем целые или рациональные решения. Применяемая техника варьируется от рассмотрения элементарных сравнений до использования более тонких результатов теории алгебраических чисел. В дополнение к доказательствам существования или несуществования решений мы получаем также результаты количественного характера, как, например, при определении числа представлений некоторого целого числа в виде суммы четырех квадратов. Все рассматриваемые в этой главе уравнения являются классическими и каждое из них играло важную роль в историческом развитии этой области теории чисел.

§ 1. Общие сведения и первые примеры

Под диофантовым уравнением мы будем понимать полиномиальное уравнение

$$f(x_1, x_2, x_3, \ldots, x_n) = 0, \tag{1}$$

коэффициенты которого суть рациональные целые числа. Если это уравнение имеет решение в целых числах $x_1, \ldots, x_n$, то будем говорить, что $(x_1, \ldots, x_n)$ — *целочисленное решение*. Если уравнение (1) однородное, то отличное от $(0, \ldots, 0)$ решение называется *нетривиальным*. Решение уравнения (1) в рациональных числах $x_1, \ldots, x_n$ называется *рациональным*. Очевидно, что в однородном случае проблема нахождения рационального решения эквивалентна проблеме нахождения целочисленного решения.

Хотя степень многочлена $f(x_1, \ldots, x_n)$ в той или иной мере контролирует трудность рассматриваемой проблемы, существование или несуществование решения часто связаны с тонкими инвариантами и даже иногда с комплексной дифференциальной геометрией уравнения (1) над комплексными числами.

Мы начнем с рассмотрения линейного диофантова уравнения

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = m. \tag{2}$$

Здесь $a_1, \ldots, a_n, m$ — рациональные целые числа. Тогда из гл. 1 (см. упр. 6, 13, 14 этой главы) следует, что решение в целых числах существует тогда и только тогда, когда наибольший общий делитель чисел $a_1, \ldots, a_n$ делит m.

Если $n = 2$ и $d = (a_1, a_2)$, то алгоритм Евклида дает точное правило построения решения уравнения $a_1x_1 + a_2x_2 = d$ (упр. 2 и 4 гл. 1). Умножение этого решения на m/d приводит к решению уравнения (2). При $n \geqslant 2$ можно продолжить этот процесс по индукции, используя простое наблюдение, что $((a_1, \ldots, a_{n-1}), a_n) = (a_1, \ldots, a_n)$.

Если уравнение (1) имеет целочисленное решение, то для каждого простого числа p имеет решение сравнение

$$f(x) \equiv 0 \ (p). \tag{3}$$

Поэтому если можно найти простое число p, для которого сравнение (3) не имеет решения, то уравнение (1) тоже не имеет решения. Этот метод можно применить ко многим частным случаям для получения теорем несуществования. Мы приведем несколько примеров применения этой техники.

Например, рассмотрим уравнение

$$y^2 = x^3 + 7. \tag{4}$$

Если уравнение (4) имеет решение, то x нечетно, ибо в противном случае редукция по модулю 4 привела бы к тому, что 3 — квадратичный вычет по модулю 4, что не так. Запишем уравнение (4) в виде

$$y^2 + 1 = (x + 2)(x^2 - 2x + 4) = (x + 2)((x - 1)^2 + 3). \tag{5}$$

Далее, так как $(x - 1)^2 + 3$ имеет вид $4n + 3$, то существует простое число p вида $4n + 3$, делящее его, и редукция равенства (5) по модулю p приводит к тому, что -1 — квадратичный вычет по модулю p. Но это противоречит следствию 3 предложения 5.1.2. Разумеется, это искусное рассуждение проходит лишь потому, что мы выбрали $x^3 + 7$. Имеется много результатов относительно рациональных и целочисленных решений уравнения

$$y^2 = x^3 + k \tag{6}$$

для частных значений k (см. § 10). Заинтересовавшийся читатель может обратиться к [189], где указан широкий набор приемов, используемых при рассмотрении уравнений (6). Мы упомянем мимоходом, что из глубоких теорем Морделла и Зигеля следует, что уравнение (6) имеет лишь конечное число целочисленных решений. Вопрос о рациональных решениях приводит к знаменитым гипотезам Бёрча и Суиннертона-Дайера. Формулировка этих гипотез будет дана в следующей главе.

Рассмотрим теперь уравнение

$$y^3 = px + 2. \tag{7}$$

Здесь p — простое число с $p \equiv 1$ (3). Заметим, что это диофантово уравнение эквивалентно сравнению

$$y^3 \equiv 2 \ (p). \tag{8}$$

В силу предложения 9.6.2 уравнение (7) имеет решение тогда и только тогда, когда $p = C^2 + 27D^2$ при подходящих целых числах C и D. Таким образом, диофантова задача (7) связана с вопросом о представимости числа p квадратичной формой $x^2 + 27y^2$.

Аналогично квадратичный закон взаимности может быть использован для доказательства того, что уравнение

$$y^2 = 41x + 3 \tag{9}$$

не имеет решения. Действительно, если решение существует, редукция по модулю 41 показывает, что 3 — квадратичный вычет по модулю 41. Но так как $41 \equiv 1$ (4), квадратичный закон взаимности означает, что 41 — квадратичный вычет по модулю 3, что не так.

Общеизвестное диофантово уравнение задается равенством

$$x^2 + y^2 = z^2. \tag{10}$$

Его решения в целых числах называются *пифагоровыми тройками*. Мы решим это уравнение при помощи предложения 1.4.1, в котором утверждается, что $\mathbf{Z}[i]$ — область однозначного разложения на простые множители. Доказательство без использования комплексных чисел можно найти, например, в [40], с. 190. Предположим, что уравнение (10) имеет решение и что $(x, y) = 1$. Тогда числа x и y не могут одновременно быть четными, и редукция (10) по модулю 4 показывает, что z нечетно. Представим (10) в $\mathbf{Z}[i]$ в виде

$$(x + iy)(x - iy) = z^2. \tag{11}$$

Если π — неприводимый элемент в $\mathbf{Z}[i]$, делящий $x + iy$ и $x - iy$, то π делит $2x$ и $2y$. Так как z нечетно, то $(\pi) \neq (1 + i)$, ибо в противном случае $\pi\bar{\pi} = 2 \mid z^2$. Поэтому $\pi \mid x$ и $\pi \mid y$. Взятие норм показывает, что $p \mid x$ и $p \mid y$, где $p = N(\pi)$, что противоречит предположению о том, что $(x, y) = 1$. Следовательно, $x + iy$ и $x - iy$ взаимно просты. Если $z = u\pi_1^{a_1} \ldots \pi_s^{a_s}$, где u — единица, есть разложение на простые множители в $\mathbf{Z}[i]$, то в силу однозначности разложения

$$x + iy = u\beta^2. \tag{12}$$

Записывая $\beta = a + bi$ и беря $u = 1$, получаем решения

$$\begin{aligned} x &= a^2 - b^2, \\ y &= 2ab, \\ z &= a^2 + b^2. \end{aligned}$$

Другие выборы единицы ($u = -1, \pm i$) приводят, в сущности (т. е. с точностью до знака), к тому же самому решению. Тождество $(a^2 - b^2)^2 + (2ab)^2 = (a^2 + b^2)^2$ показывает, что уравнение (10) имеет бесконечно много решений. Рассуждение, приведенное выше, показывает, что других решений нет.

Мы закончим этот параграф простым примером однородного кубического уравнения, которое не имеет нетривиальных решений. Для произвольного простого числа p рассмотрим уравнение

$$x^3 + py^3 + p^2z^3 = 0. \tag{13}$$

Предположим, что (13) имеет целочисленное решение (x, y, z), причем x, y, z не все делятся на p. Тогда $p \mid x^3$, а потому $p \mid x$. Полагая $x = px'$ и производя сокращение, получаем, что $p \mid y^3$, а потому $p \mid y$. Полагая $y = py'$ и производя сокращения, получаем, что $p \mid z^3$, или $p \mid z$ (противоречие). Этот изящный пример принадлежит Эйлеру (см. [154], с. 455).

§ 2. Метод спуска

Этот метод, примененный впервые Ферма, можно использовать при рассмотрении различных интересных диофановых уравнений. Иллюстрировать его лучше всего на примерах. Для этого рассмотрим диофантово уравнение

$$x^4 + y^4 = z^2. \tag{14}$$

Мы покажем, что это уравнение не имеет целочисленных решений с $xyz \neq 0$, $z > 0$. Предполагая, что (14) имеет такое целочисленное решение, мы построим другое решение с меньшим *положительным* z. Очевидно, что это невозможно, ибо в этом случае мы получили бы бесконечную последовательность убывающих положительных целых чисел. Более подробно это выглядит следующим образом.

Мы можем предполагать, что $(x, y, z) = 1$, $z > 0$. Далее, числа x и y не могут быть одновременно нечетными, ибо в противном случае редукция по модулю 4 приводила бы к сравнению $z^2 \equiv 2$ (4), что невозможно. Пусть x будет нечетным, y четным, так что z нечетно. Запишем $y^4 = (z - x^2)(z + x^2)$ и заметим, что так как любое простое число p, делящее два сомножителя справа, должно делить также $2z$ и $2x^2$, то должно быть $(z - x^2, z + x^2) = 2$. Но произведение этих двух сомножителей есть четвертая степень. Поэтому возможны два случая:

$$\begin{aligned} &z - x^2 = 2a^4, \quad a > 0, \\ &z + x^2 = 8b^4, \\ &a \text{ нечетно}, \ (a, b) = 1, \end{aligned} \tag{15}$$

или

$$z - x^2 = 8b^4,$$
$$z + x^2 = 2a^4, \quad a > 0, \tag{16}$$
$$a \text{ нечётно}, \ (a, b) = 1.$$

Первый случай означает, что $x^2 = -a^4 + 4b^4$; это невозможно, ибо тогда $1 = -1$ (4). Поэтому имеет место случай (16) и $z = a^4 + 4b^4$. Заметим, что $0 < a < z$. Исключая z из (16), получаем $4b^4 = (a^2 - x)(a^2 + x)$.

Так как $(a, b) = 1$, то $(a, x) = 1$, и рассуждая, как прежде, убеждаемся в том, что $(a^2 - x, a^2 + x) = 2$. Записывая $a^2 - x = 2c^4$ и $a^2 + x = 2d^4$, получаем

$$a^2 = c^4 + d^4.$$

Таким образом, мы нашли решение уравнения (14) с меньшим положительным значением для z и тем самым завершили доказательство. □

В частности, уравнение $x^4 + y^4 = z^4$ не имеет решений с $xyz \neq 0$. Это есть один из случаев последней теоремы Ферма.

§ 3. Теорема Лежандра

В этом параграфе мы рассматриваем диофантово уравнение

$$ax^2 + by^2 + cz^2 = 0, \tag{17}$$

где a, b, c — свободные от квадратов попарно взаимно простые целые числа. Мы хотели бы получить необходимые и достаточные условия для того, чтобы уравнение (17) имело нетривиальное целочисленное решение. Для существования решения необходимо, конечно, предположить, что a, b и c не все имеют одинаковый знак.

Если m и n — отличные от нуля целые числа, то пусть $m\ R\ n$ обозначает тот факт, что m есть квадрат по модулю n. Другими словами, существует некоторое целое число x с $x^2 \equiv m\ (n)$. Лежандр доказал следующую красивую теорему.

Предложение 17.3.1. *Пусть a, b, c — отличные от нуля целые числа, свободные от квадратов, попарно взаимно простые и не все одинакового знака. Тогда уравнение* (17) *имеет нетривиальное целочисленное решение в том и только том случае, когда выполняются следующие условия*:

(i) — $ab\ R\ c$.
(ii) — $ac\ R\ b$.
(iii) — $bc\ R\ a$.

Доказательство этого результата удобно проводить в следующем эквивалентном виде.

Предложение 17.3.2. *Пусть a и b — положительные свободные от квадратов целые числа. Тогда уравнение*

$$ax^2 + by^2 = z^2 \tag{18}$$

имеет нетривиальное решение тогда и только тогда, когда выполняются следующие три условия:

(i) $a \; R \; b$.
(ii) $b \; R \; a$.
(iii) $-(ab/d^2) \; R \; d$, *где* $d = (a, b)$.

Чтобы убедиться в том, что из предложения 17.3.2 следует предложение 17.3.1, рассмотрим уравнение $ax^2 + by^2 + cz^2 = 0$ из предложения 17.3.1 и предположим, что a и b положительны, в то время как c отрицательно. Тогда, как нетрудно видеть, уравнение $-acx^2 - bcy^2 - z^2 = 0$ удовлетворяет условиям предложения 17.3.2. Если (x, y, z) — решение последнего уравнения, то, так как c свободно от квадратов, $c \mid z$. Полагая $z = cz'$ и производя сокращение, получаем решение уравнения (17). Тот факт, что из предложения 17.3.1 следует предложение 17.3.2, предлагается доказать читателю в качестве упражнения.

Мы приступаем теперь к доказательству предложения 17.3.2. Если $a = 1$, то предложение очевидно. Кроме того, можно считать, что $a > b$. При $b > a$ следует лишь поменять местами x и y. Если $a = b$, то по (iii) -1 будет квадратом по модулю b. В силу упр. 25 в конце этой главы можно найти такие целые числа r и s, что $b = r^2 + s^2$. Решение задается тогда в виде $x = r$, $y = s$, $z = r^2 + s^2$.

Проведя эти предварительные рассмотрения, мы приступаем к построению нового уравнения $Ax^2 + by^2 = z^2$, удовлетворяющего тем же условиям, что и (18), с $0 < A < a$ и такого, что если оно имеет нетривиальное решение, то нетривиальное решение имеет и (18). После конечного числа шагов, меняя местами A и b при $A < b$, мы получаем один из случаев $A = 1$ или $A = b$, каждый из которых уже был рассмотрен. Теперь остановимся на деталях.

В силу (ii) существуют такие T и c, что

$$c^2 - b = aT = aAm^2; \quad A, \; m \in \mathbf{Z}, \tag{19}$$

где A свободно от квадратов и $|c| \leqslant a/2$. Прежде всего мы покажем, что $0 < A < a$. Это следует из (19), так как $0 \leqslant c^2 = aAm^2 + b < a(Am^2 + 1)$. Таким образом, $A \geqslant 0$. Но так как b свободно от квадратов, то $A > 0$ в силу (19). Кроме того, из (19) следует, что $aAm^2 < c^2 \leqslant a^4/4$, так что $A \leqslant Am^2 < a/4 < a$.

Проверим теперь, что $A\ R\ b$. Положим $b = b_1 d$, $a = a_1 d$, где $(a_1, b_1) = 1$, и заметим, что $(a_1, d) = (b_1, d) = 1$, так как a и b свободны от квадратов. Тогда (19) превращается в

$$c^2 - b_1 d = a_1 d A m^2 \tag{20}$$

и, так как d свободно от квадратов, $d \mid c$. Полагая $c = c_1 d$ и производя сокращение, получаем

$$dc_1^2 - b_1 = a_1 A m^2. \tag{21}$$

Таким образом, $A a_1 m^2 \equiv -b_1\ (d)$, или $A a_1^2 m^2 \equiv -a_1 b_1\ (d)$. Но $(d, m) = 1$ в силу того, что по (21) общий делитель делил бы b_1 и d и, таким образом, число b не было бы свободным от квадратов. Используя (iii) и тот факт, что m — единица по модулю d, получаем. что $A\ R\ d$. Кроме того, $c^2 \equiv aAm^2\ (b_1)$. Так как $a\ R\ b$, то $a\ R\ b_1$. Помимо этого, $(a, b_1) = 1$, ибо общий делитель делил бы d и b_1 в противоречие с тем фактом, что $b = b_1 d$ свободно от квадратов. Аналогично $(m, b_1) = 1$, откуда следует, что $A\ R\ b_1$. В силу упр. 26 $A\ R\ db_1$, или $A\ R\ b$.

Запишем теперь $A = rA_1$, $b = rb_2$, $(A_1, b_2) = 1$. Мы должны проверить, что $-A_1 b_2\ R\ r$. Из (19) получаем, что

$$c^2 - rb_2 = arA_1 m^2. \tag{22}$$

Но r свободно от квадратов, так что $r \mid c$. Если $c = rc_1$, то

$$aA_1 m^2 \equiv -b_2\ (r).$$

Так как $a\ R\ b$, то $a\ R\ r$. Записывая, наконец,

$$-aA_1 b_2 m^2 \equiv -b_2^2\ (r)$$

и замечая, что $(a, r) = (m, r) = 1$, мы получаем $-A_1 b_2\ R\ r$.

Предположим теперь, что $AX^2 + bY^2 = Z^2$ имеет нетривиальное решение. Тогда

$$AX^2 = Z^2 - bY^2. \tag{23}$$

Умножая (23) на (19), получаем

$$\begin{aligned} a\,(AXm)^2 &= (Z^2 - bY^2)\,(c^2 - b) = \\ &= (Zc + bY)^2 - b\,(cY + Z)^2. \end{aligned}$$

(Обратите внимание на использование мультипликативности нормменного отображения на $\mathbf{Q}(\sqrt{b})$!) Таким образом, уравнение (18) имеет решение

$$\begin{aligned} x &= AXm, \\ y &= cY + Z, \\ z &= Zc + bY. \end{aligned}$$

Это завершает доказательство, так как $X \neq 0$; кроме того, $m \neq 0$, как следует из того факта, что b свободно от квадратов. □

Важным следствием предложения 17.3.1 является один частный случай так называемого принципа Хассе. Грубо говоря, этот принцип утверждает, что из локальной разрешимости следует глобальная разрешимость. Здесь локальная разрешимость означает, что рассматриваемое уравнение имеет как нетривиальное решение по модулю p^m для всех простых чисел p и всех положительных целых чисел m, так и вещественное решение, в то время как глобальная разрешимость означает разрешимость в целых числах. Этот принцип верен для квадратичных форм, но нарушается для уравнений более высокой степени. Например, уравнение $x^4 - 17y^4 = 2z^4$ имеет нетривиальное решение по модулю p^m при всех p и m и вещественное решение, но не имеет нетривиального решения в целых числах [205].

Следствие. *Пусть a, b, c — положительные свободные от квадратов попарно взаимно простые целые числа, не все одного знака. Если для каждой степени простого числа p^m сравнение*

$$ax^2 + by^2 + cz^2 \equiv 0 \ (p^m)$$

имеет решение в целых числах (x, y, z), причем не все они делятся на p, то уравнение $ax^2 + by^2 + cz^2 = 0$ имеет нетривиальное целочисленное решение.

Доказательство. Пусть $m = 2$, и предположим, что $p \mid a$. Тогда если (x, y, z) — решение, о котором говорится в следствии, то мы покажем, что $p \nmid yz$. Действительно, если, скажем, $p \mid y$, то $p \mid cz^2$, откуда следует, в силу $(a, c) = 1$, что $p \mid z$. Таким образом, $p^2 \mid ax^2$ и в силу $p \nmid x$ мы получаем противоречие $p^2 \mid a$. Подобно этому $p \nmid z$. Значит, $by^2 + cz^2 \equiv 0 \ (p)$ и деление (по модулю p) показывает, что $-bc \ R \ p$. Так как это имеет место для каждого $p \mid a$, то $-bc \ R \ a$ (упр. 26). Аналогично $-ab \ R \ c$ и $-ac \ R \ b$, и следствие получается теперь из предложения 17.3.1. □

§ 4. Теорема Софи Жермен

В гл. 14 мы доказали, что если уравнение Ферма для нечетного простого числа p

$$x^p + y^p + z^p = 0 \tag{24}$$

имеет решение с $p \nmid xyz$, то выполняется очень сильное сравнение, а именно,

$$2^{p-1} \equiv 1 \ (p^2).$$

В 1823 г. Софи Жермен при помощи вполне элементарных соображений доказала следующий замечательный результат.

Предложение 17.4.1. *Если p — такое нечетное простое число, что $2p + 1 = q$ — тоже простое число, то уравнение* (24) *не имеет целочисленных решений с $p \nmid xyz$.*

Доказательство. Предположим, что вопреки утверждению такое решение существует и $(x, y, z) = 1$. Запишем

$$-x^p = (y + z)(z^{p-1} - z^{p-2}y + \cdots + y^{p-1}). \tag{25}$$

Два сомножителя справа взаимно просты. Действительно, $p \nmid y + z$, и если $r \neq p$ — какое-либо простое число, делящее оба сомножителя, то, поскольку $y \equiv -z\ (r)$,

$$0 \equiv z^{p-1} - z^{p-2}y + \cdots + y^{p-1}\ (r) \equiv py^{p-1}\ (r),$$

откуда следует, что $r \mid y$. Это в свою очередь означает, что $r \mid z$ (по (24)), в противоречие с предположением $(x, y, z) = 1$. В силу однозначности разложения на простые множители в $\mathbf{Z}$ мы получаем, что

$$x + y = A^p, \tag{26}$$

$$z^{p-1} - z^{p-2}y + \cdots + y^{p-1} = T^p \tag{27}$$

при соответствующих целых числах A и T. Аналогично

$$x + y = B^p, \tag{28}$$

$$x + z = C^p. \tag{29}$$

Так как $p = (q - 1)/2$, редукция (24) по модулю q дает

$$x^{(q-1)/2} + y^{(q-1)/2} + z^{(q-1)/2} \equiv 0\,(q).$$

Если $q \nmid xyz$, то каждый из членов слева равен ± 1 по модулю q, что невозможно, ибо $q \geqslant 5$. Таким образом, по симметрии можем считать, что $q \mid x$. Из (26), (28) и (29) получаем, что

$$B^p + C^p - A^p = 2x,$$

так что

$$B^{(q-1)/2} + C^{(q-1)/2} - A^{(q-1)/2} \equiv 0\ (q). \tag{30}$$

Опять отсюда следует, что $q \mid ABC$. Но, так как $q \mid x$, из (28) и (29) вытекает, что $q \mid BC$ невозможно. Поэтому $q \mid A$. Из (26) и (27) мы видим, что

$$T^p \equiv py^{p-1}\ (q).$$

Из (28) получаем $y \equiv B^p\ (q)$, а так как $(A, T) = 1$, то $q \nmid T$. Таким образом, поскольку $p = (q - 1)/2$, то $\pm 1 \equiv \pm p\ (q)$, что невозможно, и доказательство закончено. □

К сожалению, неизвестно, бесконечно ли много простых чисел «типа Жермен», т. е. простых чисел p, для которых $2p + 1$ простое. Интересующимся этим вопросом следует обратиться к лекции IV в книге [206].

§ 5. Уравнение Пелля

Пусть d — некоторое положительное свободное от квадратов целое число. Диофантово уравнение, которое будет рассматриваться, — это

$$x^2 - dy^2 = 1. \tag{31}$$

То, что это уравнение имеет бесконечное число решений, было высказано в виде гипотезы Ферма в 1657 г. и полностью доказано Лагранжем. По-видимому, Пелль не имеет к этому уравнению никакого отношения, а ошибка приписывания его имени этому уравнению принадлежит Эйлеру. По поводу полной истории этого вопроса (и многих других) заинтересованному читателю следует обратиться к книге [128]. См. также [22] и [240].

Решение уравнения (31) использует следующее предложение, являющееся приложением принципа ящиков Дирихле.

Предложение 17.5.1. *Если ξ иррационально, то существует бесконечно много таких рациональных чисел x/y, $(x, y) = 1$, что $|x/y - \xi| < 1/y^2$.*

Доказательство. Разобьем полуоткрытый интервал $[0, 1)$ на полуоткрытые интервалы:

$$[0, 1) = \left[0, \frac{1}{n}\right) \cup \left[\frac{1}{n}, \frac{2}{n}\right) \cup \ldots \cup \left[\frac{n-1}{n}, 1\right).$$

Если $[\alpha]$ означает, как обычно, наибольшее целое число, меньшее или равное α, то дробная часть α определяется как $\alpha - [\alpha]$. Она лежит в единственном члене разбиения. Рассмотрим дробные части чисел $0, \xi, 2\xi, \ldots, n\xi$. По крайней мере две из них должны лежать в одном и том же подынтервале [1]). Другими словами, существуют такие j и k с $j > k$, $0 \leqslant j, k \leqslant n$, что

$$|j\xi - [j\xi] - (k\xi - [k\xi])| < \frac{1}{n}. \tag{32}$$

Положим $y = j - k$, $x = [k\xi] - [j\xi]$, так что (32) превращается в неравенство $|x - y\xi| < 1/n$. Здесь мы можем считать, что $(x, y) = 1$, так как деление на (x, y) лишь усилит неравенство.

---

[1]) Это и есть принцип ящиков. — *Прим. ред.*

Но из $0 < y < n$ следует, что $|x/y - \xi| < 1/ny < 1/y^2$. Для получения бесконечного числа решений заметим, что $|x/y - \xi| \neq 0$, и выберем целое число $m > 1/|x/y - \xi|$. Описанный выше прием приводит к существованию таких целых чисел x_1, y_1, что $|x_1/y_1 - \xi| < 1/my_1 < |x/y - \xi|$ и $0 < y_1 < m$. Это дает бесконечное число решений. □

Это предложение будет использовано, чтобы показать, что $|x^2 - dy^2|$ принимает бесконечно часто одно и то же значение.

Лемма 1. *Если d — некоторое положительное свободное от квадратов целое число, то существует такая константа M, что неравенство $|x^2 - dy^2| < M$ имеет бесконечное число целочисленных решений.*

Доказательство. Запишем $x^2 - dy^2 = (x + \sqrt{d}y)(x - \sqrt{d}y)$. В силу предложения 17.5.1 существует бесконечно много пар взаимно простых целых чисел (x, y), $y > 0$, удовлетворяющих неравенству $|x - \sqrt{d}y| < 1/y$. Отсюда следует, что

$$|x + \sqrt{d}y| < |x - \sqrt{d}y| + 2\sqrt{d}|y| < \frac{1}{y} + 2\sqrt{d}y.$$

Значит, $|x^2 - dy^2| < |1/y + 2\sqrt{d}y|\, 1/y \leqslant 2\sqrt{d} + 1$ и доказательство завершено. □

Сформулируем основной результат этого параграфа:

Предложение 17.5.2. *Если d — положительное свободное от квадратов целое число, то уравнение $x^2 - dy^2 = 1$ имеет бесконечно много целочисленных решений. Более того, существует такое решение (x_1, y_1), что каждое другое решение имеет вид $\pm(x_n, y_n)$, где $x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n$, $n \in \mathbf{Z}$.*

Доказательство. Согласно лемме 1, существует такое $m \in \mathbf{Z}$, что равенство $x^2 - dy^2 = m$ выполняется для бесконечного числа целых пар (x, y), $x > 0$, $y > 0$. Можно предполагать, что все координаты x различны. Кроме того, так как имеется лишь конечное число классов вычетов по модулю $|m|$, можно найти такие пары (x_1, y_1), (x_2, y_2), $x_1 \neq x_2$, что $x_1 \equiv x_2$ $(|m|)$, $y_1 \equiv y_2$ $(|m|)$. Положим $\alpha = x_1 - y_1\sqrt{d}$, $\beta = x_2 - y_2\sqrt{d}$. При $\gamma = x - y\sqrt{d}$ пусть $\gamma' = x + y\sqrt{d}$ обозначает сопряженный элемент к γ и $N(\gamma) = x^2 - dy^2$ обозначает норму. Напомним, что $N(\alpha\beta) = N(\alpha)\,N(\beta)$. Короткое вычисление показывает, что $\alpha\beta' = A + B\sqrt{d}$, где $m \mid A$, $m \mid B$. Таким образом, $\alpha\beta' = m(u +$

$+ v\sqrt{d}$) для целых чисел u и v. Взятие нормы от обеих частей приводит к равенству $m^2 = m^2 (u^2 - v^2 d)$, откуда получаем

$$u^2 - v^2 d = 1. \tag{33}$$

Остается убедиться в том, что $v \neq 0$. Но при $v = 0$ получаем $u = \pm 1$ и $\alpha\beta' = \pm m$. Умножение на β приводит к равенству $\alpha m = \pm m\beta$, или $\alpha = \pm \beta$. Последнее же означает, что $x_1 = x_2$. Таким образом, уравнение Пелля имеет решение с $xy \neq 0$.

Для доказательства второго утверждения введем на множестве решений упорядочение: будем говорить, что решение (x, y) больше, чем решение (u, v), если $x + y\sqrt{d} > u + v\sqrt{d}$. Рассмотрим теперь наименьшее решение α с $x > 0$, $y > 0$. Такое решение существует (почему?) и единственно. Оно называется *фундаментальным решением*.

Рассмотрим любое решение $\beta = u + v\sqrt{d}$, $u > 0$, $v > 0$. Мы покажем, что существует такое положительное целое число n, что $\beta = \alpha^n$. Если это не так, то выберем $n > 0$ так, чтобы $\alpha^n < \beta < \alpha^{n+1}$. Тогда, поскольку $\alpha' = \alpha^{-1}$, то $1 < (\alpha')^n \beta < \alpha$. Но если $(\alpha')^n \beta = A + B\sqrt{d}$, то (A, B) есть решение уравнения Пелля и $1 < A + B\sqrt{d} < \alpha$. Далее, $A + B\sqrt{d} > 0$, так что $A - B\sqrt{d} = (A + B\sqrt{d})^{-1} > 0$. Значит, $A > 0$. Кроме того, $A - B\sqrt{d} = (A + B\sqrt{d})^{-1} < 1$, так что $B\sqrt{d} > A - 1 \geqslant 0$. Таким образом, $B > 0$. Это противоречит выбору α. Если $\beta = a + b\sqrt{d}$ — решение с $a > 0$, $b < 0$, то $\beta^{-1} = a - b\sqrt{d} = \alpha^n$ в силу доказанного, так что $\beta = \alpha^{-n}$. Случаи $a < 0$, $b > 0$ и $a < 0$, $b < 0$ приводят, очевидно, к $-\alpha^n$ для $n \in \mathbf{Z}$. Это завершает доказательство. □

Решение частных случаев уравнения Пелля с использованием круговых полей см. в [126] и [145].

§ 6. Сумма двух квадратов

Если p — простое число, $p \equiv 1$ (4), то, согласно предложению 8.3.1, диофантово уравнение $x^2 + y^2 = p$ имеет целочисленное решение, которое по существу единственно. Имеется много доказательств этого результата. Напомним, что в доказательстве из гл. 8 используется кольцо гауссовых целых чисел. Глубже используя арифметику этого кольца, мы найдем число представлений произвольного положительного целого числа в виде суммы двух квадратов. Результат удобно формулировать и доказывать при помощи нетривиального характера Дирихле по модулю 4, введенного в § 2 гл. 16. Напомним, что этот характер определяется на $\mathbf{Z}$ так: $\chi(d) = 1$ при $d \equiv 1$ (4), $\chi(d) = -1$ при $d \equiv 3$ (4) и $\chi(2k) = 0$.

Предложение 17.6.1. *Число целых решений* (x, y), $x > 0$, $y \geqslant 0$, *уравнения* $x^2 + y^2 = n$ *равно* $\sum_{d \mid n} \chi(d)$.

Другими словами, число представлений n в виде суммы двух неотрицательных квадратов, первый из которых положителен, равно разности между числом делителей вида $4k + 1$ и числом делителей вида $4k + 3$. Как нетрудно убедиться, общее число решений (x, y), $x, y \in \mathbf{Z}$, равно тогда $4 \sum_{d \mid n} \chi(d)$.

Прежде чем приступить к доказательству, мы получим два следствия.

Следствие 1. *Уравнение* $x^2 + y^2 = n$, $n > 0$, *имеет целое решение тогда и только тогда, когда* $\operatorname{ord}_p n$ *четно для каждого простого числа* $p \equiv 3$ (4). *Когда это условие выполняется, число решений равно* $\prod_{p \equiv 1\,(4)} (1 + \operatorname{ord}_p n)$.

Доказательство. Так как характер $\chi(n)$ мультипликативен, из упр. 10 гл. 2 следует, что функция $\sum_{d \mid n} \chi(d)$ мультипликативна. Если $p \equiv 1$ (4), то $\sum_{d \mid p^n} \chi(d) = n + 1$, в то время как при $p \equiv 3$ (4) величина $\sum_{d \mid p^n} \chi(d)$ равна 0 или 1 в зависимости от того, будет n нечетным или четным. Отсюда и следует наш результат. □

Следствие 2. *Пусть* m *— некоторое положительное нечетное число. Число решений* (x, y), $x > 0$, $y > 0$, *уравнения* $x^2 + y^2 = 2m$ *равно* $\sum_{d \mid m} \chi(d)$.

Доказательство. Так как $2m \equiv 2$ (4), то y положительно. С другой стороны, $\chi(2d) = 0$ для любого делителя $2d$ числа $2m$. □

Мы приступаем теперь к доказательству предложения 17.6.1. Рассмотрим кольцо $\mathbf{Z}[i]$ гауссовых целых чисел. По упр. 33 из гл. 1 единицами в нем будут ± 1, $\pm i$. Таким образом, любое ненулевое число $\alpha \in \mathbf{Z}[i]$ имеет единственное ассоциированное с ним $x + yi$, $x > 0$, $y \geqslant 0$. Если $N(x + yi) = x^2 + y^2$ — отображение нормы, то, как нетрудно убедиться, число решений уравнения $x^2 + y^2 = n$, $x > 0$, $y \geqslant 0$, равно числу идеалов (α), таких, что $N(\alpha) = n$. Обозначим это число через a_n. Напомним, далее, что каждый идеал $(\alpha) \neq 0$ может быть единственным образом (с точностью до порядка) записан в виде $(\pi_1)^{t_1} \ldots (\pi_s)^{t_s}$, где π_i неприводимы. Наконец, согласно § 7 гл. 9, неприводимые эле-

менты задаются с точностью до единиц, числами $1+i$, π с $\pi\bar{\pi} = p \equiv 1$ (4) и q, рациональными простыми числами, $q \equiv 3$ (4). Кроме того, π и $\bar{\pi}$ не ассоциированы.

Введем теперь формальный ряд Дирихле $\sum_{n=1}^{\infty} a_n/n^s$. Этот ряд известен как *дзета-функция* кольца $\mathbf{Z}[i]$. Мы рассматриваем это выражение формально и не будем использовать какие-либо аналитические свойства соответствующей функции комплексной переменной. Используя однозначность разложения на простые идеалы в $\mathbf{Z}[i]$, которая была доказана в § 4 гл. 1, с помощью тех же рассуждений, что в упр. 25 из гл. 2, получаем, что

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{(\pi)} \frac{1}{(1-1/N(\pi)^s)}, \tag{34}$$

где произведение берется по множеству (неассоциированных) неприводимых элементов в $\mathbf{Z}[i]$. Правая часть равенства (34) превращается, если воспользоваться приведенной выше классификацией неприводимых элементов, в

$$\frac{1}{(1-1/2^s)} \prod_{p\equiv 1\,(4)} \left(\frac{1}{1-1/p^s}\right)^2 \prod_{q\equiv 3\,(4)} \left(\frac{1}{1-1/q^{2s}}\right). \tag{35}$$

Напомним теперь, что

$$\zeta(s) = \prod_{p} \frac{1}{1-1/p^s} = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Замечая, что $1/(1-q^{-2s}) = (1/(1-q^{-s}))\,(1/(1+q^{-s}))$, мы видим, перегруппировывая члены, что (35) превращается в

$$\zeta(s) \prod_{p\equiv 1\,(4)} \frac{1}{1-1/p^s} \prod_{q\equiv 3\,(4)} \frac{1}{1+1/q^s}. \tag{36}$$

Это может быть записано в виде

$$\zeta(s) \prod_{p} \frac{1}{1-\chi(p)/p^s}. \tag{37}$$

Наконец, используя то, что характер χ мультипликативен, получаем, что (37) может быть записано как

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}. \tag{38}$$

Напомним, что второй сомножитель в (38) есть L-ряд Дирихле, введенный в гл. 16, § 2, для вычисления плотности простых чисел $p \equiv 1$ (4). Мы показали, что

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}\right). \tag{39}$$

Предложение 17.6.1 сразу же следует из (39), ибо коэффициент в правой части равенства (39) равен в силу определения умножения Дирихле $\sum_{d \mid n} \chi(d)$. Это завершает доказательство. □

Следует заметить, что перегруппировка членов ряда чисто формальна и не требует каких-либо аналитических свойств бесконечных произведений.

§ 7. Сумма четырех квадратов

В 1621 г. Баше сформулировал без доказательства утверждение о том, что каждое положительное целое число является суммой четырех квадратов. Это утверждение было доказано Лагранжем в 1770 г. В 1834 г. Якоби смог получить замечательно простую формулу для общего числа представлений некоторого целого числа в виде суммы четырех квадратов, из которой сразу же получается результат Лагранжа.

Мы начнем этот параграф со стандартного доказательства теоремы Лагранжа. Применяется техника спуска. После получения теоремы для простых чисел общий результат следует из одного формального тождества Эйлера, выражающего тот факт, что норма квартерниона является мультипликативной функцией. В последней, несколько растянутой части этого параграфа мы доказываем теорему Якоби. Доказательство основано на одном письме (1856 г.) Дирихле Лиувиллю ([122], с. 201—208), в котором упрощается доказательство Якоби. См. также [237].

Мы начнем с одной диофантовой задачи по модулю p.

Лемма 1. *При простом числе p сравнение $x^2 + y^2 + 1 \equiv 0$ (p) имеет решение в целых числах x, y.*

Доказательство. Обозначим через S множество квадратов по модулю p. Тогда S и $\{-1 - x \mid x \in S\} = S'$ имеют каждое по $(p+1)/2$ элементов. Поэтому S и S' пересекаются, откуда и следует результат. □

По доказанной лемме существует такое целое число m, что уравнение $mp = 1 + x^2 + y^2$ имеет целое решение, и, более того,

переходя к вычетам, можем считать, что $|x| < p/2$, $|y| < p/2$. Следовательно, $mp < 1 + p^2/4 + p^2/4$, так что $m < p$.

Лемма 2. *Предположим, что для простого числа p существует такое целое число m, $1 < m < p$, что mp представляется в виде суммы четырех квадратов. Тогда существует такое n, $0 < n < m$, что np есть сумма четырех квадратов.*

Доказательство. Запишем

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2. \tag{40}$$

Пусть $x_i \equiv y_i\ (m)$, где $-m/2 < y_i \leqslant m/2$. Тогда $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0\ (m)$, так что существует целое число $r \geqslant 0$, для которого

$$rm = y_1^2 + y_2^2 + y_3^2 + y_4^2. \tag{41}$$

Имеем $rm \leqslant m^2/4 + m^2/4 + m^2/4 + m^2/4 = m^2$, так что $r \leqslant m$. Кроме того, $r \neq 0$, ибо в противном случае $y_i = 0$, $i = 1, \ldots, 4$, откуда следовало бы в силу (40), что $m \mid p$ (противоречие). Кроме того, $r \neq m$, ибо в противном случае $y_i = m/2$; в таком случае сравнения $x_i^2 \equiv m^2/4\ (m^2)$ и (40) означали бы, что $mp \equiv m^2\ (m^2)$, или $m \mid p$. Перемножение равенств (40) и (41) приводит, согласно упр. 28, к равенству

$$\begin{aligned} m^2rp = {} & (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + \\ & + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 + \\ & + (x_1y_3 - x_3y_1 + x_2y_4 - x_4y_2)^2 + \\ & + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2. \end{aligned} \tag{42}$$

Используя сравнения $x_i \equiv y_i\ (m)$, убеждаемся в том, что каждый член справа в (42) делится на m^2. Сокращение на m^2 показывает, что rp есть сумма четырех квадратов. □

Предложение 17.7.1. *Каждое положительное целое число представляется в виде суммы четырех квадратов.*

Доказательство непосредственно следует из лемм 1 и 2 и упр. 28. □

Возвратимся теперь к формулировке и доказательству теоремы Якоби. Мы установим следующий результат.

Предложение 17.7.2. *Пусть n — некоторое положительное число, $n \equiv 4$ (8). Число целочисленных решений (x, y, z, w), для которых x, y, z, w положительны и нечетны, уравнения*

$$x^2 + y^2 + z^2 + w^2 = n \tag{43}$$

равно сумме положительных нечетных делителей числа n.

Мы переносим в упражнения доказательство такого следствия.

Следствие. *Пусть n — некоторое положительное целое число. Число целочисленных решений (x, y, z, w) уравнения $x^2 + y^2 + z^2 + w^2 = n$ равно $8 \sum_{d \mid n} d$ при нечетном n и $24 \sum_{d \mid n} d$ при четном n.*

Доказательством предложения 17.7.2 распадается на несколько лемм. Пусть N обозначает число целых решений (x, y, z, w) уравнения (43) с положительными и нечетными x, y, z, w. Так как $n \equiv 4$ (8), можно записать $n = 2m$, $m \equiv 2$ (4).

Лемма 3. *N равно числу решений (x, y, z, u, v) системы диофантовых уравнений*

$$\begin{aligned} x^2 + y^2 &= 2u, \\ z^2 + w^2 &= 2v, \\ u + v &= m \end{aligned} \tag{44}$$

с положительными и нечетными x, y, z, u, v.

Доказательство является простым упражнением. □

Как в § 5, пусть χ обозначает нетривиальный характер Дирихле по модулю 4.

Лемма 4. $N = \sum \chi(de) = \sum (-1)^{(de-1)/2} = \sum (-1)^{(d-e)/2}$, *где сумма берется по всем решениям (d, e, t, s) в положительных нечетных целых числах уравнения $ds + et = m$.*

Доказательство. Из леммы 3 и следствия 2 предложения 17.6.1 нетрудно получить, что

$$N = \sum_{\substack{u, v \\ u+v=m}} \Big(\sum_{\substack{d \mid u \\ d \mid v}} \chi(d)\chi(e) \Big). \tag{45}$$

Запишем $u = ds$, $v = et$, так что члены в (45) будут находиться во взаимно однозначном соответствии с наборами (d, e, t, s), где числа d, e, t, s положительны, нечетны и удовлетворяют уравнению $ds + et = m$. Это доказывает первое равенство в лемме. Второе следует из определения χ и того факта, что $(d - 1)/2 + (e - 1)/2 \equiv (de - 1)/2$ (2) при нечетных d и e. □

Рассмотрим теперь в сумме $\sum \chi(de)$ из леммы 4 члены с $d = e$. Для каждого нечетного $d \mid m$ уравнение $s + t = m/d$ имеет $m/2d$ решений в положительных нечетных числах s и t. Общее число решений поэтому равно $\sum_{d \mid m} m/2d = \sum_{d \mid m} d$. Каждое решение

уравнения $ds + et = m$ при $d = e$ добавляет $\chi(d^2) = 1$ к N, согласно лемме 4. Доказательство предложения 17.7.2 будет завершено, если показать, что $\sum \chi(de) = 0$, где сумма такая же, как в лемме 4, и $d \neq e$. Объединение членов с (d, e, t, s) и (e, d, s, t) показывает, что достаточно доказать равенство $\sum \chi(de) = 0$, где суммирование ведется по $d > e$.

Обозначим через S множество наборов (d, e, t, s), где $d > e$, $ds + et = m$ и все числа d, e, t, s положительны и нечетны. Основная идея оставшейся части доказательства состоит в построении такого биективного отображения множества S в себя, которое переводит $\sum\limits_S \chi(de)$ в $-\sum\limits_S \chi(de)$. Это, конечно, означает, что $\sum\limits_S \chi(de) = 0$.

Для некоторого положительного целого числа n положим

$$A_n = \begin{pmatrix} n+1 & n+2 \\ n & n+1 \end{pmatrix}$$

и определим (d', e', t', s') посредством формул

$$\begin{aligned} A_n \begin{pmatrix} t \\ s \end{pmatrix} &= \begin{pmatrix} d' \\ e' \end{pmatrix}, \\ A_n^{-1} \begin{pmatrix} d \\ e \end{pmatrix} &= \begin{pmatrix} t' \\ s' \end{pmatrix}. \end{aligned} \tag{46}$$

Так как

$$A_n^{-1} = \begin{pmatrix} n+1 & -n-2 \\ -n & n+1 \end{pmatrix},$$

легко проверяется, что

$$A_n \begin{pmatrix} t & d \\ s & -e \end{pmatrix} = \begin{pmatrix} d' & t' \\ e' & -s' \end{pmatrix}.$$

Беря определители, получаем

$$ds + et = d's' + e't'. \tag{47}$$

Таким образом, для каждого n мы имеем отображение $\mathbf{Z}^4$ в $\mathbf{Z}^4$, которое будет обозначаться через ψ_n.

Лемма 5. *Для заданного набора $(d, e, t, s) \in S$ существует единственное $n \in \mathbf{Z}^+$, для которого $\psi_n(d, e, t, s) \in S$.*

Доказательство. Из (46) сразу же видно, что d', e', t', s' нечетны, $d' > e'$, $d' > 0$, $e' > 0$. Кроме того, условия $s' > 0$, $t' > 0$ эквивалентны в силу (46) неравенствам $e/(d - e) - 1 < n < e/(d -$

— e). Но d — e положительно и четно, а e нечетно, откуда вытекает, что последние неравенства удовлетворяются при единственном $n > 0$. Это и завершает доказательство. □

Обозначим через Φ отображение из S в S, определенное в лемме 5.

Лемма 6. Φ — *биекция.*

Доказательство. Мы покажем, что Φ^2 — единичное отображение. Действительно, если $(d, e, t, s) \in S$, то

$$\Phi^2(d, e, t, s) = \Phi\left(\left(A_n\binom{t}{s}\right)^*, \left(A_n^{-1}\binom{d}{e}\right)^*\right) =$$

$$= \left(\left(A_k A_n^{-1}\binom{d}{e}\right)^*, \left(A_k^{-1}A_n\binom{t}{s}\right)^*\right), \quad (48)$$

где звездочка означает транспонирование. Здесь k и n определены леммой 5. Но целое число k определено условием, что правая часть в (48) принадлежит S, однозначно, причем это условие выполняется при $k = n$. Таким образом, $\Phi^2(d, e, t, s) = (d, e, t, s)$ и доказательство леммы завершено. □

Для окончания доказательства предложения 17.7.2 заметим, что из (46) имеем $d' - e' = s + t$. Но $\chi(de) = (-1)^{(d-e)/2}$. Так как $ds + et \equiv 2$ (4), мы видим, что $(d - e)/2$ четно в том и только том случае, когда $(s + t)/2$ нечетно. Таким образом, $\chi(de) = -\chi(d'e')$. Наконец,

$$M = \sum_S \chi(de) = -\sum_S \chi(d'e') = -M,$$

откуда следует, что $M = 0$, и доказательство закончено. □

§ 8. Уравнение Ферма: экспонента 3

Уравнение Ферма

$$x^p + y^p = z^p \quad (49)$$

рассматривалось в частных случаях в § 2 и 4 и в гл. 14 (теорема 5). В этом параграфе, используя арифметику в кольце $\mathbf{Z}[\omega]$, где $\omega^3 = 1$, $\omega \neq 1$, мы полностью решаем вопрос для уравнения

$$x^3 + y^3 = z^3. \quad (50)$$

Тот факт, что это уравнение не имеет целых решений (x, y, z), $xyz \neq 0$, был впервые доказан по существу Эйлером. См., однако, [91].

Вместо (50) мы рассмотрим более общее уравнение

$$x^3 + y^3 = uz^3, \quad (51)$$

где u — некоторая фиксированная единица в $\mathbf{Z}[\omega]$, и докажем следующий результат.

Предложение 17.8.1. *Уравнение* $x^3 + y^3 = uz^3$, *где* u — *некоторая фиксированная единица в* $\mathbf{Z}[\omega]$, *не имеет целых решений* (x, y, z), $xyz \neq 0$, *где* $x, y, z \in \mathbf{Z}[\omega]$.

Отсюда следует, конечно, что ненулевой куб в $\mathbf{Z}$ не представляется в виде суммы двух ненулевых кубов в $\mathbf{Z}$.

Предложение 17.8.1 будет доказано при помощи ряда лемм. Мы напомним сначала основные факты об арифметике кольца $\mathbf{Z}[\omega]$, которые были получены в гл. 9. Кольцо $\mathbf{Z}[\omega]$ есть кольцо главных идеалов с единицами ± 1, $\pm\omega$, $\pm\omega^2$. Положим $\lambda = 1 - \omega$ и напомним, что $(\lambda)^2 = (3)$ и что λ неразложим. Каждый элемент $\alpha \in \mathbf{Z}[\omega]$ сравним по модулю λ с $+1$, -1 или 0. Этот факт будет далее постоянно использоваться. Если $\alpha = u\lambda^n\beta$, где u — единица и $\lambda \nmid \beta$, то мы пишем $n = \operatorname{ord}_\lambda \alpha$.

Сначала мы докажем более слабый результат, так называемый первый случай, о том, что уравнение (51) не имеет решений с $\lambda \nmid xyz$.

Лемма 1. *Уравнение* $x^3 + y^3 = uz^3$, u — *единица в* $\mathbf{Z}[\omega]$, *не имеет решений с* $x, y, z \in \mathbf{Z}[\omega]$, $\lambda \nmid xyz$.

Доказательство. Заметим, что, так как λ неразложим, условие $\lambda \nmid xyz$ эквивалентно условиям $\lambda \nmid x$, $\lambda \nmid y$, $\lambda \nmid z$. Если $x \in \mathbf{Z}[\omega]$, $x \equiv 1\ (\lambda)$, то $x^3 \equiv 1\ (\lambda^4)$. Действительно, если $x = 1 + \lambda t$, то

$$\begin{aligned} x^3 - 1 &= (x-1)(x-\omega)(x-\omega^2) = \\ &= \lambda t(1 - \omega + \lambda t)(1 - \omega^2 + \lambda t) = \\ &= \lambda t(\lambda + \lambda t)((1+\omega)\lambda + \lambda t) = \\ &= \lambda^3 t(1+t)(t-\omega^2). \end{aligned}$$

Так как $\omega^2 \equiv 1\ (\lambda)$ и t сравнимо по модулю λ с $+1$, -1 или 0, то получается нужное сравнение.

Предположим теперь, что существует решение уравнения (51) с $\lambda \nmid xyz$, и приведем (51) по модулю λ^4:

$$\pm 1 \pm 1 \equiv \pm u\ (\lambda^4). \tag{52}$$

Нетрудно убедиться, однако, что сравнение (52) невозможно ни при каком выборе знаков и единицы. Это завершает доказательство. □

Мы переходим теперь к более трудному случаю, когда предполагается существование решения с $\lambda \mid z$ и $(x, y) = 1$. Таким образом, $\lambda \nmid xy$.

Следующая лемма показывает, что при этих условиях на самом деле $\lambda^2 \mid z$.

Лемма 2. *Если* $x^3 + y^3 = uz^3$ *для* $x, y, z \in \mathbf{Z}[\omega]$, $\lambda \nmid xy$, $\lambda \mid z$, *то* $\lambda^2 \mid z$.

Доказательство. Приведение равенства (51) по модулю λ^4 дает

$$\pm 1 \pm 1 \equiv uz^3 \ (\lambda^4).$$

Если $0 \equiv uz^3 \ (\lambda^4)$, то $3 \operatorname{ord}_\lambda z \geqslant 4$, так что $\operatorname{ord}_\lambda z \geqslant 2$. Если $\pm 2 \equiv uz^3 \ (\lambda^4)$, то $\lambda \mid 2$, что неверно. □

Следующая лемма реализует шаг «спуска».

Лемма 3. *Если* $x^3 + y^3 = uz^3$, $(x, y) = 1$, $\lambda \nmid xy$, $\operatorname{ord}_\lambda z \geqslant 2$, *то существуют такие* $u_1, x_1, y_1, z_1 \in \mathbf{Z}[\omega]$, u_1 — *единица*, $\lambda \nmid x_1 y_1$, $\operatorname{ord}_\lambda z_1 = \operatorname{ord}_\lambda z - 1$, *что*

$$x_1^3 + y_1^3 = u_1 z_1^3.$$

Доказательство. Напомним, что если $\operatorname{ord}_\lambda \alpha \neq \operatorname{ord}_\lambda \beta$, то $\operatorname{ord}_\lambda (\alpha \pm \beta) = \min (\operatorname{ord}_\lambda \alpha, \operatorname{ord}_\lambda \beta)$. Далее,

$$(x + y)(x + \omega y)(x + \omega^2 y) = uz^3. \tag{53}$$

Так как $\operatorname{ord}_\lambda (uz^3) \geqslant 6$, то хотя бы один сомножитель слева в (53) делится на λ^2. Заменяя в случае необходимости y на ωy или $\omega^2 y$, можем считать, что $\operatorname{ord}_\lambda (x + y) \geqslant 2$. Так как $\operatorname{ord}_\lambda (1 - \omega) y = \operatorname{ord}_\lambda \lambda y = 1$, то

$$\operatorname{ord}_\lambda (x + \omega y) = \operatorname{ord}_\lambda (x + y + (1 - \omega) y) = 1.$$

Аналогично $\operatorname{ord}_\lambda (x + \omega^2 y) = 1$. Таким образом,

$$\operatorname{ord}_\lambda (x + y) = 3 \operatorname{ord}_\lambda z - 2.$$

Если π — неразложимый элемент и $(\pi) \neq (\lambda)$, то π не может делить $x + y$ и $x + \omega y$, ибо в противном случае $\pi \mid (1 - \omega) y = \lambda y$, так что $\pi \mid y$, $\pi \mid x$. Отсюда следует, что $(x + y, x + \omega y) = (\lambda)$. Подобным же образом и другие пары множителей в (53) имеют наибольший общий делитель λ. Так как в $\mathbf{Z}[\omega]$ имеет место однозначность разложения на простые множители, мы можем записать

$$\begin{aligned} x + y &= u_1 \alpha^3 \lambda^t, \quad t = 3 \operatorname{ord}_\lambda z - 2, \quad \lambda \nmid \alpha, \\ x + y\omega &= u_2 \beta^3 \lambda, \quad \lambda \nmid \beta, \\ x + y\omega^2 &= u_3 \gamma^3 \lambda, \quad \lambda \nmid \gamma. \end{aligned} \tag{54}$$

В (54) u_1, u_2, u_3 — единицы и $(\alpha, \beta) = (\alpha, \gamma) = (\beta, \gamma) = 1$. Умножая второе равенство в (54) на ω, третье — на ω^2 и складывая, получаем

$$0 = u_1 \alpha^3 \lambda^t + \omega u_2 \beta^3 \lambda + \omega^2 u_3 \gamma^3 \lambda. \tag{55}$$

Сокращение на λ (!!) приводит к равенству

$$0 = u_1\alpha^3\lambda^{3(\operatorname{ord} z-1)} + \omega u_2\beta^3 + \omega^2 u_3\gamma^3. \tag{56}$$

Наконец, полагая $\alpha\lambda^{\operatorname{ord} z-1} = z_1$, $\beta = x_1$, $\gamma = y_1$, переписываем (56) с единицами ε_1, ε_2 в виде

$$x_1^3 + \varepsilon_1 y_1^3 = \varepsilon_2 z_1^3. \tag{57}$$

Приводя (57) по модулю λ^2 и замечая, что $\operatorname{ord}_\lambda (z_1^3) > 2$, получаем

$$\pm 1 \pm \varepsilon_1 \equiv 0 \ (\lambda^2). \tag{58}$$

Разбор случаев приводит сразу же к равенству $\varepsilon_1 = \pm 1$. Таким образом, заменяя в случае необходимости y_1 на $-y_1$, получаем новое соотношение

$$x_1^3 + y_1^3 = \varepsilon z_1^3$$

с $\lambda \nmid x_1 y_1$, $\operatorname{ord}_\lambda z_1 = \operatorname{ord}_\lambda z - 1$, единицей ε. Это завершает доказательство. □

Для доказательства предложения 17.8.1 мы поступаем следующим образом. Если $\lambda \nmid xyz$, то ссылаемся на лемму 1. Если $\lambda \nmid xy$, но $\lambda \mid z$, то леммы 2 и 3 приводят к противоречию. Наконец, если $\lambda \mid x$, но $\lambda \nmid yz$, то $\pm 1 \equiv u \ (\lambda^4)$, а это означает, что $\pm 1 = u$. Но тогда $(\pm z)^3 + (-y)^3 = x^3$, и мы попадаем в уже рассмотренный случай.

§ 9. Кубические кривые с бесконечным числом рациональных точек

В предыдущем параграфе было показано, что уравнение $x^3 + y^3 = z^3$ не имеет решений в целых числах (x, y, z) с $xyz \neq 0$. Деление на z^3 показывает, что кубическая кривая $x^3 + y^3 = 1$ не имеет рациональных точек (x, y), $xy \neq 0$. Аналогично из результата, полученного в § 2, о том, что $x^4 + y^4 = z^2$ не имеет целых решений с $xyz \neq 0$, делается вывод о том, что рациональными точками кривой, определенной уравнением $y^2 = x^4 + 1$, будут лишь $(0, \pm 1)$ (см. упр. 31).

В этом параграфе мы приводим примеры кубических кривых с бесконечным числом рациональных точек. Доказательство основано на простом наблюдении, что касательная прямая к кубической кривой в рациональной точке пересекает эту кривую в единственной, не обязательно новой, точке, которая тоже рациональна. Мы говорим, что целое число *а свободно от кубов*, если $\operatorname{ord}_p a < 2$ для всех простых p, т. е. нет кубов $\neq 1, -1$, делящих a.

Предложение 17.9.1. *Пусть $a > 2$ — свободное от кубов целое число. Если кубическая кривая с уравнением*

$$x^3 + y^3 = a \tag{59}$$

имеет некоторую рациональную точку, то она имеет бесконечно много рациональных точек.

Доказательство. Пусть (α, β) — рациональная точка на (59). Если $\alpha = x_1/z_1$, $\beta = y_1/z_2$, $(x_1, z_1) = (y_1, z_2) = 1$ с целыми числами x_1, y_1, z_1, z_2, то нетрудно убедиться в том, что $z_1 = z_2$. Так как $a > 2$ свободно от кубов, то $x_1 y_1 \neq 0$ и $x_1 \neq y_1$. Касательной прямой к (59) в (α, β) будет $\alpha^2 x + \beta^2 y = a$. Разрешая последнее уравнение относительно y и подставляя результат в (59), получаем

$$x^3 + \left(\frac{a - \alpha^2 x}{\beta^2}\right)^3 - a = 0. \tag{60}$$

Левая часть уравнения (60) — кубический многочлен с α в качестве (по крайней мере) двукратного корня. Если обозначить третий корень через γ, то, так как сумма всех корней равна взятому с обратным знаком коэффициенту при x^2, после простого вычисления получаем

$$2\alpha + \gamma = \frac{3\alpha^4}{\alpha^3 - \beta^3}. \tag{61}$$

Таким образом,

$$\gamma = \frac{\alpha(\alpha^3 + 2\beta^3)}{\alpha^3 - \beta^3} = \frac{x_1}{z_1}\frac{(x_1^3 + 2y_1^3)}{(x_1^3 - y_1^3)}. \tag{62}$$

Соответствующее значение для $y = (a - \alpha^2 x)/\beta^2$ равно

$$\rho = \frac{-y_1}{z_1}\frac{(2x_1^3 + y_1^3)}{(x_1^3 - y_1^3)} \tag{63}$$

и в силу (60) (γ, ρ) — рациональная точка на кубике. Читатель может, конечно, и непосредственно проверить, что $\gamma^3 + \rho^3 = a$. Остается проверить, что (γ, ρ) отлична от (α, β) и, кроме того, что таким способом получается бесконечное число точек на кривой. Определим целое число A равенствами

$$\begin{aligned} Ax_2 &= x_1(x_1^3 + 2y_1^3), \\ Ay_2 &= -y_1(2x_1^3 + y_1^3), \\ Az_2 &= z_1(x_1^3 - y_1^3), \end{aligned} \tag{64}$$

где $(x_2, y_2, z_2) = 1$. Таким образом, A есть наибольший общий делитель целых чисел в правых частях (64). Очевидно, что

$$x_2^3 + y_2^3 = az_2^3, \quad z_2 \neq 0. \tag{65}$$

Так как a свободно от кубов и $(x_2, y_2, z_2) = 1$, то $(x_2, y_2) = (x_2, z_2) = (y_2, z_2) = 1$. Мы утверждаем, что A равно 1 или 3. Действительно, если p — простое число и $p \mid A$, то из (64) нетрудно получить, что $p \nmid x_1 y_1 z_1$. Таким образом, p делит каждый второй сомножитель в правых частях равенств (64) и, следовательно, $p \mid 3y_1^3$. Поэтому p равно 1 или 3. Заметим, кроме того, что из $(A, z_1) = 1$ следует $A \mid x_1^3 - y_1^3$.

Доказательство будет завершено, если показать, что $|z_2| > |z_1|$. Для получения этого запишем

$$|z_2| = \frac{|z_1|}{A} |x_1^3 - y_1^3| = \frac{|z_1|}{A} |x_1 - y_1| |x_1^2 + x_1 y_1 + y_1^2|. \tag{66}$$

Имеем $4 |x_1^2 + x_1 y_1 + y_1^2| = |(2x_1 + y_1)^2 + 3y_1^2| > 4$, и, следовательно, выполняется неравенство $|z_2| > |z_1| |x_1 - y_1|/A$. Если $A = 1$, то (66) показывает, что $|z_2| > |z_1|$. С другой стороны, если $A = 3$, то, так как $A \mid x_1^3 - y_1^3$, $x_1^3 \equiv y_1^3$ (3), откуда следует, что $x_1 \equiv y_1$ (3). Опять из (66) вытекает, что $|z_2| > |z_1|$. Продолжая этот процесс, получаем последовательность точек $(x_n/z_n, y_n/z_n)$, такую, что $x_n y_n \neq 0$, $(x_n, z_n) = (y_n, z_n) = 1$ и $|z_n| > |z_{n-1}|$, и это завершает доказательство.

§ 10. Уравнение $y^2 = x^3 + k$

Диофантово уравнение

$$y^2 = x^3 + k \tag{67}$$

было впервые рассмотрено в семнадцатом веке Ферма и Баше в частном случае $k = -2$ и с тех пор интенсивно изучалось. До сих пор не выяснено, при каких целых значениях k уравнение (67) имеет по крайней мере одно рациональное решение. Баше и другие утверждали, но не доказали этого, что если установлено существование одного решения (x, y), $xy \neq 0$, то метод касательных, использованный в § 9, приводит к бесконечному числу решений. Таким образом, на современном языке эллиптическая кривая (67) имеет в таком случае положительный ранг (см. гл. 18). С несколькими исключениями этот результат был получен Фуетером в 1930 г.

В 1966 г. замечательно короткое доказательство результата Фуетера было получено Морделлом [191]. Более точно, он доказал

Предложение 17.10.1. *Если уравнение $y^2 = x^3 + k$, где k — свободное от шестых степеней целое число, имеет некоторое рациональное решение (x, y), $xy \neq 0$, то при $k \neq 1, -432$ существует бесконечно много рациональных решений этого уравнения.*

В упражнениях показано, что случай $k = -432$ эквивалентен уравнению Ферма $x^3 + y^3 = 1$, которое в силу основного результата § 8, как нетрудно показать, имеет лишь рациональные решения (1, 0), (0, 1). Мы не будем вдаваться в подробности доказательства предложения 17.10.1, а отошлем заинтересованного читателя к статье Морделла. Оно сводится к тому, чтобы показать, что метод касательных, использованный в предыдущем параграфе, приводит к бесконечному числу решений.

Таким образом, кривая $y^2 = x^3 - 2$ имеет бесконечное число рациональных точек, ибо она имеет одну такую точку, а именно (3, 5). Однако отметим, что существует лишь конечное число целых решений соответствующего уравнения. Это трудная теорема для произвольного k, но в случае $k = -2$ можно дать очень короткое доказательство, если воспользоваться упр. 36 гл. 1. Действительно,

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3. \tag{68}$$

Если элемент π неприводим в $\mathbf{Z}[\sqrt{-2}]$ и делит оба множителя в левой части равенства (68), то $\pi \mid 2\sqrt{-2}$. Таким образом, $(\pi) = (\sqrt{-2})$ и $\sqrt{-2} \mid x$, откуда следует, если взять нормы, что $2 \mid x$. Отсюда вытекает $y^2 \equiv 2 \pmod 4$, что невозможно. Так как $\mathbf{Z}[\sqrt{-2}]$ — кольцо с однозначным разложением на множители и единицами ± 1, то (68) показывает, что

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3.$$

Таким образом,

$$y = a^3 - 6ab^2, \tag{69}$$

$$1 = 3a^2b - 4b^3 = b(3a^2 - 4b^2). \tag{70}$$

Следовательно, $b = -1$, и мы получаем в качестве единственных решений $(3, \pm 5)$.

Если d — положительное свободное от квадратов целое число, то в некоторых случаях, воспользовавшись арифметикой мнимого квадратичного поля $\mathbf{Q}(\sqrt{-d})$, можно найти целые решения для уравнения $y^2 = x^3 - d$. Как и в случае последней теоремы Ферма (см. § 11), при таком подходе необходимо наложить на число классов h поля $\mathbf{Q}(\sqrt{-d})$ некоторое условие делимости, а именно потребуем, чтобы $3 \nmid h$. Если мы ограничимся рассмотрением d, таких, что $d \not\equiv +1, +3$ и $-d \equiv 2$ или $3 \pmod 4$, то по результатам гл. 13 кольцом целых чисел поля $\mathbf{Q}(\sqrt{-d})$ будет $\mathbf{Z}[\sqrt{-d}]$ и ± 1 — единственные единицы в нем. При этих условиях предположим, что (x, y) — некоторое целое решение уравнения $y^2 = x^3 - d$. Тогда (упр. 32) x нечетно и $(x, d) = 1$. Далее,

$$x^3 = (y + \sqrt{-d})(y - \sqrt{-d}).$$

Если $P \subset \mathbf{Z}[\sqrt{-d}]$ — простой идеал, содержащий $y \pm \sqrt{-d}$, то $2\sqrt{-d} \in P$ и $x \in P$. Таким образом, $N(P) \mid 4d$ и $N(P) \mid x^2$, что невозможно. Отсюда следует, что $(y+\sqrt{-d})$ и $(y-\sqrt{-d})$ не имеют общих идеальных делителей. Так как $\mathbf{Z}[\sqrt{-d}]$ — дедекиндово кольцо, то

$$(y+\sqrt{-d}) = \mathfrak{A}^3$$

для некоторого идеала $\mathfrak{A}$. Поскольку $3 \nmid h$, группа классов идеалов кольца $\mathbf{Z}[\sqrt{-d}]$ не имеет элементов порядка 3, а потому $\mathfrak{A}$ — главный идеал. Следовательно, так как ± 1 — единственные единицы, то

$$y + \sqrt{-d} = \pm (a + b\sqrt{-d})^3. \tag{71}$$

Отсюда вытекает, что

$$\begin{aligned} 1 &= \pm b(3a^2 - db^2), \\ y &= \pm a(a^2 - 3db^2), \end{aligned} \tag{72}$$

откуда нетрудно получить, что $b = \pm 1$ и

$$d = 3a^2 \pm 1. \tag{73}$$

Таким образом, уравнение $y^2 = x^3 - d$ имеет решение в точности тогда, когда d лежит в одной из квадратичных прогрессий $3a^2 \pm 1$. Если это так, то нетрудно убедиться в том, что значение x равно $a^2 + d$. Следовательно, получено такое предложение.

Предложение 17.10.2. *Пусть $d > 1$ свободно от квадратов и $d \equiv 2$ или 1 (4). Предположим, что число классов поля $\mathbf{Q}(\sqrt{-d})$ не делится на 3. Тогда уравнение $y^2 = x^3 - d$ имеет целочисленное решение в том и только том случае, когда d имеет вид $3t^2 \pm 1$. Решениями в таком случае будут $(t^2 + d, \pm t(t^2 - 3d))$.*

Для знакомства с вещественным квадратичным случаем следует обратиться к [84], гл. 10, и к [189], гл. 26.

§ 11. Первый случай гипотезы Ферма для регулярных показателей

В этом параграфе мы используем результаты гл. 12 и 13 об арифметике круговых числовых полей для доказательства одного частного случая гипотезы Ферма. Если ζ обозначает корень степени l из 1, где l — нечетное простое число, то $\mathbf{Q}(\zeta)$ будет полем алгебраических чисел степени $l - 1$, у которого кольцо целых чисел в силу предложения 13.2.10 совпадает с $\mathbf{Z}[\zeta]$. Таким образом, согласно теореме 2 из гл. 12, каждый ненулевой идеал в $\mathbf{Z}[\zeta]$

может быть однозначно представлен в виде произведения степеней различных простых идеалов. Напомним, что l называется регулярным, если $l \nmid h$, где h обозначает число классов поля $\mathbf{Q}(\zeta)$. Таким образом, если в этом случае $\mathfrak{A}$ — идеал, для которого $\mathfrak{A}^l$ — главный идеал, то $\mathfrak{A}$ сам будет главным идеалом; этот факт имеет очень важное значение в последующем изложении.

Нам понадобится один дополнительный результат, относящийся к арифметике кольца $\mathbf{Z}[\zeta]$.

Лемма 1. *Если u — какая-либо единица в $\mathbf{Z}[\zeta]$, то $\zeta^s u$ вещественно для некоторого рационального целого числа s.*

Доказательство. Заметим сначала, что комплексное сопряжение будет автоморфизмом поля $\mathbf{Q}(\zeta)$, ибо $\bar{\zeta} = \zeta^{p-1}$. Таким образом, если u — какая-либо единица, то $\bar{u}$ тоже будет единицей и $\tau = u/\bar{u} \in \mathbf{Z}[\zeta]$. Кроме того, если ρ — произвольный автоморфизм поля $\mathbf{Q}(\zeta)$, то $\rho(\tau) = \rho(u)/\rho(\bar{u}) = \rho(u)/\overline{\rho(u)}$, так что $|\rho(\tau)| = 1$. В силу лемм 1 и 2 § 5 гл. 14 $\tau = \pm \zeta^t$ для некоторого целого числа t. Если $\lambda = 1 - \zeta$, то $\zeta^j \equiv 1\ (\lambda)$ для всех j, так что, записав $u = a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2}$ и воспользовавшись тем фактом, что $\rho(\zeta) = \zeta^k$ при некотором k, убеждаемся в том, что $u \equiv \rho(u)\ (\lambda)$. В частности, $u \equiv \bar{u}\ (\lambda)$. Если $\tau = -\zeta^t$, то $u = -\zeta^t\bar{u}$, так что $u \equiv -\bar{u}\ (\lambda)$. Таким образом, $2u \equiv 0\ (\lambda)$, что невозможно. Поэтому $u = \zeta^t\bar{u} = \zeta^{-2s}\bar{u}$, где $-2s \equiv t\ (l)$. Наконец, $\zeta^s u = \overline{\zeta^s u}$, что показывает вещественность $\zeta^s u$. □

Основной результат этого параграфа состоит в следующем.

Предложение 17.11.1. *Если l — регулярное простое число, то диофантово уравнение*

$$x^l + y^l = z^l \tag{74}$$

не имеет решения в рациональных целых числах x, y, z с $l \nmid xyz$.

Доказательство этого предложения будет разбито на несколько лемм. Мы начнем с разложения левой части уравнения (74) на множители:

$$x^l + y^l = (x+y)(x+\zeta y)\ \ldots\ (x+\zeta^{l-1}y). \tag{75}$$

Напомним, что два идеала $\mathfrak{A}$ и $\mathfrak{B}$ взаимно просты в $\mathbf{Z}[\zeta]$, если $\mathfrak{A} + \mathfrak{B} = \mathbf{Z}[\zeta]$. Если это имеет место, то у идеалов $\mathfrak{A}$ и $\mathfrak{B}$ нет общих простых идеальных делителей. До конца этого параграфа будем считать, что уравнение (74) имеет некоторое решение в целых числах x, y, z, $l \nmid xyz$ и $l \nmid h$. Предположим также, что x, y, z попарно взаимно просты.

Лемма 2. *Идеалы* $(x + \zeta^i y)$ *и* $(x + \zeta^j y)$ *взаимно просты при* $i \neq j$ (l).

Эта лемма уже была доказана в § 6 гл. 14.

Лемма 3. *Существуют такие* u, $\beta \in \mathbf{Z}[\zeta]$, *где* u *— вещественная единица, что* $x + \zeta y = \zeta^s u\beta$, *где* $s \in \mathbf{Z}$ *и* $\beta \equiv n$ (l) *для некоторого* $n \in \mathbf{Z}$.

Доказательство. Используя лемму 2, предложение 13.3.3 и тот факт, что правая часть равенства (74) есть l-я степень, убеждаемся в том, что $(x + \zeta y) = \mathfrak{A}^l$ для некоторого идеала $\mathfrak{A}$. Так как $l \nmid h$, отсюда следует, что $\mathfrak{A}$ — главный идеал. Таким образом, $x + \zeta y = \varepsilon\alpha^l$, где $\alpha \in \mathbf{Z}[\zeta]$ и ε — единица. Наш результат следует теперь из леммы 1 и замечания о том, что если $\alpha = \sum_{i=0}^{l-2} a_i \zeta^i$, то $\alpha^l \equiv \sum_{i=0}^{l-2} a_i$ (l). □

Переходя к сопряженным, получаем $x + \zeta^{-1} y = \zeta^{-s} u\bar{\beta}$, так что $\zeta^{-s}(x + \zeta y) - \zeta^s (x + \zeta^{-1} y) = u(\beta - \bar{\beta})$. Но $\bar{\beta} \equiv \beta$ $(l) \equiv n$ (l), а следовательно, мы показали, что $\zeta^{-s}(x + \zeta y) - \zeta^s (x + \zeta^{-1} y) \in l\mathbf{Z}[\zeta]$. Мы сформулируем это в таком виде:

Лемма 4. $x + \zeta y - \zeta^{2s} x - \zeta^{2s-1} y \in l\mathbf{Z}[\zeta]$.

Согласно предложению 6.4.1, числа $1, \zeta, \zeta^2, \ldots, \zeta^{l-2}$ линейно независимы над $\mathbf{Q}$. Кроме того, можно предполагать, что $l > 3$ (в силу § 8) и $0 \leqslant s \leqslant l - 1$. Доказательство предложения 17.11.1 будет завершено, если получить противоречие из включения леммы 4. По сделанному выше замечанию нам следует рассмотреть лишь случаи, когда две из степеней ζ совпадают. Таким образом, мы должны рассмотреть случаи

(a) $\zeta^{2s} = 1$;

(b) $\zeta^{2s-1} = 1$;

(c) $\zeta^{2s-1} = \zeta$.

В случае (a) из леммы 4 следует, что $-y + \zeta^2 y \in l\mathbf{Z}[\zeta]$, а поэтому $l \mid y$. В случае (c) получаем $x - \zeta^2 x \in l\mathbf{Z}[\zeta]$, так что $l \mid x$ (противоречие). Наконец, в случае (b) получаем $(x - y) + (y - x)\zeta \in l\mathbf{Z}[\zeta]$. Таким образом, $x \equiv y$ (l). Запишем уравнение Ферма в виде $x^l + (-z)^l = (-y)^l$. Рассуждая теперь, как ранее, получаем лемму 4, возможно с другим s. Однако случаи (a) и (c) приводят к противоречию, а случай (b) дает, как и выше, сравнение $x \equiv -z$ (l). Но $0 = x^l + y^l - z^l \equiv x + y -$

— z (l). Таким образом, $3x \equiv 0$ (l), что означает $l \mid x$, — противоречие! Это завершает доказательство последней теоремы Ферма для регулярных показателей. □

Приведенное выше доказательство совпадает по существу с доказательством из [9].

§ 12. Диофантовы уравнения и диофантово приближение

В этом завершающем параграфе мы проводим краткое обсуждение связи между диофантовыми уравнениями и приближением алгебраических чисел посредством рациональных чисел. Техника, используемая при доказательстве упомянутых ниже результатов, отлична от той, которая излагалась в предшествующих главах. Здесь мы можем лишь указать результаты и отослать заинтересованного читателя к библиографии.

Если α — некоторое иррациональное число, то, согласно предложению 17.5.1, существует бесконечно много рациональных чисел p/q, для которых

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Естественно спросить, может ли показатель степени 2 в этом неравенстве быть увеличен. В глубоком результате Рота 1955 г. [118], за который ему в 1958 г. была присуждена Филдсовская медаль, утверждается, что если α — алгебраическое число степени $\geqslant 2$, то для каждого фиксированного $\varepsilon > 0$ существует, самое большее, конечное число рациональных чисел p/q, $q > 0$, таких, что

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}. \tag{76}$$

Отсюда следует, что существует такая константа $c > 0$, что для всех рациональных чисел p/q

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^{2+\varepsilon}}.$$

Теореме Рота предшествовали глубокие результаты Туэ (1909 г.) и Зигеля (1921 г.), каждый из которых улучшал одну элементарную оценку Лиувилля (1844 г.). Этот простой результат состоит в следующем.

Предложение 17.12.1. *Если α — некоторое вещественное алгебраическое число степени n, $n \geqslant 2$, то существует такая константа $c > 0$, что для любого рационального числа p/q, $q > 0$,*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^n}.$$

Доказательство. Очевидно, достаточно предположить, что $|\alpha - p/q| \leqslant 1$. По теореме о среднем $|f(p/q)| = |f(\alpha) - f(p/q)| \leqslant |\alpha - p/q| A$, где $f(x) \in \mathbf{Z}[x]$ неприводим, $f(\alpha) = 0$ и $A = \sup |f'(x)|$, $|x - \alpha| \leqslant 1$. Но так как α не рационально, $f(p/q) \neq 0$ и $|f(p/q)| \geqslant 1/q^n$, что и завершает доказательство. □

В результатах Туэ и Зигеля n заменяется на $n/2 + 1$ и $2\sqrt{n}$ соответственно. Результат Рота является, в некотором смысле, наилучшим возможным в силу теоремы Дирихле (предложение 17.5.1). Однако, как мы увидим, любое улучшение оценки Лиувилля, т. е. любое снижение показателя степени n (причем он должен оставаться больше 2!), дает глубокие следствия при изучении некоторых диофантовых уравнений. Действительно, пусть $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ — какой-либо многочлен с целыми коэффициентами, неприводимый над $\mathbf{Q}$ и степени по крайней мере 3. Для ненулевого m рассмотрим диофантово уравнение

$$a_n x^n + a_{n-1}x^{n-1}y + \ldots + a_0 y^n = m. \tag{77}$$

Мы покажем, что если выполняется неравенство вида

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^{n-\varepsilon}}, \quad n - \varepsilon > 2, \tag{78}$$

для некоторого $0 < \varepsilon < n$ и всех рациональных чисел p/q, то уравнение (77) имеет не более чем конечное число целых решений. Этот замечательный результат очень легко следует из (78). Действительно, запишем (77) в виде

$$\left(\frac{x}{y} - \alpha^{(1)}\right)\left(\frac{x}{y} - \alpha^{(2)}\right)\ldots\left(\frac{x}{y} - \alpha^{(n)}\right) = \frac{m}{a_n y^n}.$$

Положим $A = \min |\alpha^{(i)} - \alpha^{(j)}|$, $i \neq j$. Если в таком случае (x, y) — некоторое целое решение с $y \neq 0$, то очевидно, что, самое большее, одно $\alpha^{(j)}$ удовлетворяет неравенству $|x/y - \alpha^{(j)}| < A/2$. Для такого $\alpha^{(j)}$ применим (78), а для остальных членов воспользуемся неравенством $|x/y - \alpha^{(i)}| \geqslant A/2$. В результате получим

$$\frac{m}{|y|^n} > \frac{T}{|y|^{n-\varepsilon}}$$

при подходящем T, зависящем от $\alpha^{(1)}, \ldots, \alpha^{(n)}$. Таким образом,

$$m > T|y|^{\varepsilon}, \quad \varepsilon > 0,$$

откуда следует, что $|y|$ ограничен. Но для любого y число x, удовлетворяющих (77), ограничено, и мы получили то, что нужно. Таким образом, в то время как $x^2 - 2y^2 = 1$ имеет бесконечное

число целых решений, $x^3 - 2y^3 = 1$ имеет их лишь конечное число.

Среди детальных изложений этой обширной области теории чисел мы укажем [225], [89] и [217] [1]).

Замечания

Литература по диофантовым уравнениям многочисленна. Мы упомянем лишь несколько статей и заметок, относящихся к вопросам, обсуждавшимся в этой главе. В качестве хорошего общего обзора мы рекомендуем статью [180], а также более раннюю работу [39] [2]). В дополнении к [146] специально рассматриваются уравнения, изучавшиеся Ферма и Эйлером в семнадцатом и восемнадцатом веках. См. также классическую работу [152], где проведен детальный анализ результатов Ферма и Эйлера и их связи с методом касательных при нахождении рациональных точек на кубических кривых, который был описан в § 9 и 10. Связи этого процесса с соответствующими диофантовыми уравнениями по модулю p будут указаны в следующей главе.

Превосходные главы по диофантовым проблемам можно найти в различных вводных курсах по теории чисел. Мы упомянем, в частности, [84], [40], [230], [22] и [61].

Четкая перспектива периода формирования этой ветви математики и теории чисел вообще намечена в неформальной лекции А. Вейля [235].

Обширное освещение диофантовых уравнений, данное современным мастером, отличает [189]. Более изощренное и абстрактное изложение можно найти в [170]. Живое обсуждение относительных достоинств этих книг заинтересованный читатель обнаружит в реферате Морделла [190] на книгу Ленга и последующем реферате Ленга [172] на книгу Морделла. См. также обзоры повышенного типа [53], [173].

---

[1]) Одним из центральных в теории диофантовых уравнений является вопрос о том, когда число решений конечно, и о нахождении в этом случае эффективной границы для координат (или высоты) решений. Для целочисленных решений уравнений с двумя переменными (т. е. целых точек на алгебраических кривых) ответ на первый вопрос был получен Зигелем в 1929 г. Число целых точек конечно, если род g кривой больше нуля или если $g = 0$ и проективное замыкание кривой имеет на бесконечности по крайней мере три точки. Основную роль в доказательстве играет описанная в § 12 техника диофантовых приближений (см., например, [170]). Вопрос об эффективности удалось решить лишь для кривых частного вида (эллиптические кривые, кривые вида (77) или $y^2 = f(x)$; см. [20*]). Гипотеза о конечности числа рациональных точек на кривых рода $g > 1$ была выдвинута Морделлом в 1922 г. Лишь недавно она была доказана Фалтингсом (см. [25*], [32*], доклады Шпиро и Делиня в [2*] и приложение к русскому переводу книги Ленга [170]). Вопрос об эффективности в этой ситуации остается открытым. — *Прим. ред.*

[2]) См. также [33*].—*Прим. ред.*

Упражнения

1. Показать, что уравнение $165x^2 - 21y^2 = 19$ не имеет целых решений.
2. Найти целые решения уравнения $y^2 + 31 = x^3$.
3. Показать, что $x^3 + y^3 = 3z^3$ не имеет решений $x, y, z \in \mathbf{Z}[\omega]$, $z \neq 0$.
4. (В память Рамануджана.) Показать, что 1729 — наименьшее положительное целое число, представимое в виде суммы двух различных целых кубов двумя способами.
5. Какие из следующих уравнений имеют нетривиальные решения?
(a) $3x^2 - 5y^2 + 7z^2 = 0$
(b) $7x^2 + 11y^2 - 19z^2 = 0$.
(c) $8x^2 - 5y^2 - 3z^2 = 0$.
(d) $11x^2 - 3y^2 - 41z^2 = 0$.
6. Найти фундаментальные решения уравнений $x^2 - 3y^2 = 1$, $x^2 - 6y^2 = 1$, $x^2 - 624y^2 = 1$.
7. Свести проблему нахождения целочисленных решений уравнения $3x^2 + 1 = 4y^3$ к предложению 17.8.1 следующим образом:
(a) Положить $t = (3x - 1)/2$; $t \neq 1, -2$, так что $t^2 + t + 1 = 3y^3$, $y \neq 0$.
(b) $(t + 2)^3 + (1 - t)^3 = (3y)^3$.
8. Найти целые решения уравнения $y^2 = x^3 - 4$.
9. Найти четыре рациональные точки на $x^3 + y^3 = 9$, используя метод предложения 17.9.1.
10. Найти целые решения уравнения $y^2 = x^3 - 1$.
11. Показать, что если $x^2 - dy^2 = -1$ имеет целое решение, то целое решение имеет и $x^2 - dy^2 = 1$.
12. Перечислить целые решения уравнения $x^2 + y^2 + z^2 + w^2 = 15$ и сравнить с предложением 17.7.2.
13. Пусть t есть целочисленный куб. Показать, что $y^2 = x^2 - t$ имеет целое решение.
14. Показать, что если уравнение $x^2 - dy^2 = n$, где $d > 0$ свободно от квадратов, имеет целое решение с $xy \neq 0$, то оно имеет их бесконечно много.
15. Пусть $a + b\sqrt{p}$ — фундаментальное решение уравнения $x^2 - py^2 = 1$, где p — простое число и $p \equiv 1$ (4). Следующие шаги показывают, что $x^2 - py^2 = -1$ имеет целое решение $x, y, xy \neq 0$.
(a) a нечетно.
(b) $a \pm 1 = 2u^2$, $a \mp 1 = 2pv^2$, $2uv = b$.
(c) $u^2 - pv^2 = \pm 1$.
(d) В (c) имеет место знак минус.

Следующие семь упражнений приводят к следствию предложения 17.7.2. Пусть $A(n)$ обозначает число целых решений уравнения $x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$. См. [52].

16. Показать, что $A(4n) = A(2n)$.
17. Если n нечетно, то показать, что $16 \sum_{d \mid n} d + A(n) = A(4n)$.
18. Для нечетного n пусть S есть число решений уравнений $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 2n$ с $x_1 \equiv x_2$ (2) $\equiv 1$ (2) и $x_3 \equiv x_4$ (2) $\equiv 0$ (2). Показать, что число элементов в S равно $A(2n)/6$.
19. Показать, что если $n \equiv 1$ (4) и S такое же, как в упр. 18, то число элементов в S равно $A(n)/2$. Сделать отсюда вывод о том, что $A(2n) = 3A(n)$.
20. Если $n \equiv 3$ (4), то $A(2n) = 3A(n)$.
21. Показать, что если n нечетно, то $A(n) = 8 \sum_{d \mid n} d$, $A(2n) = 24 \sum_{d \mid n} d$.
22. Если n четно, $n = 2^s m$, $s \geqslant 1$, m нечетно, то показать, что $A(n) = 24 \sum_{d \mid m} d$.

23. Дискриминант многочлена $t^3 + pt + q$ равен $-(4p^3 + 27q^2)$. Свести проблему нахождения кубик с дискриминантом 1 и рациональными p, q к уравнению Ферма $x^3 + y^3 = 1$, положив $x = (3q + 1)/(3q - 1)$, $y = 2p/(3q - 1)$, $q \neq 1/3$. Показать, что в результате получаются кубики $t^3 - t \pm 1/3$.

24. Показать, что из предложения 17.3.1 следует предложение 17.3.2.

25. Показать, что если b — некоторое положительное целое число и -1 — квадрат по модулю b, то уравнение $x^2 + y^2 = b$ имеет целое решение.

26. При $(n, m) = 1$ показать, что из $a \; R \; m$, $a \; R \; n$ следует $a \; R \; mn$.

27. Оправдать шаг перегруппировки членов в предложении 17.6.1.

28. Пусть — множество комплексных матриц вида

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}.$$

Показать, что тождество Эйлера, в котором утверждается, что

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)\,(y_1^2 + y_2^2 + y_3^2 + y_4^2)$$

равно правой части равенства (42), эквивалентно тождеству $\det(MN) = (\det M)(\det N)$ для $M, N \in A$.

29. Следующие рассуждения показывают, что из предложения 17.8.1 следует такое утверждение: единственными рациональными решениями уравнения $y^2 = x^3 - 432$ являются $(12, \pm 36)$. Дополнить детали. Предположим, что существует решение (x, y), отличное от $(12, \pm 36)$, $x > 0$.

(a) Записать $y/36 = a/c$, $x/12 = b/c$ с $a \equiv c \; (2) \equiv 0 \; (2)$.

(b) Положить $r = (a + c)/2$, $s = (c - a)/2$, $t = b > 0$.

(c) Показать, что $r^3 + s^3 = t^3$, $rst \neq 0$.

30. Верно также обращение упр. 29. Показать, что если $x^3 + y^3 = z^3$, $xyz \neq 0$, $x, y, z \in \mathbf{Z}$, то, полагая $r = 36\,(x - y)/(x + y)$, $s = 12z\,(x + y)$, получим, что $r^2 = s^3 - 432$.

31. Используя тот факт, что уравнение $x^4 + y^4 = z^2$ не имеет целых решений с $xyz \neq 0$, показать, что $(0, \pm 1)$ — единственные рациональные решения уравнения $y^2 = x^4 + 1$.

32. Пусть d — некоторое свободное от квадратов целое число и d сравнимо с 1 или 2 по модулю 4. Показать, что если x и y — целые числа, для которых $y^2 = x^3 - d$, то $(x, 2d) = 1$.

Глава 18

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

Многие вопросы, излагавшиеся в этой книге, объединяются вместе в арифметике эллиптических кривых. Это ветвь теории чисел, корни которой уходят далеко в прошлое, но которая, тем не менее, является предметом интенсивного исследования и в настоящее время.

В этой главе будет дан краткий обзор некоторых определений, проблем и гипотез об эллиптических кривых, имеющих отношение к теме данной книги. В частности, нашей целью будет описание одной тонкой и важной гипотезы Бёрча и Суиннертона-Дайера. По большей части мы будем опускать доказательства и ограничиваться лишь общим введением в основные идеи. Более детальный анализ мы проведем для кривых вида $y^2 = x^3 + D$ и $y^2 = x^3 - Dx$ и покажем, как глобальные дзета-функции этих кривых связаны с L-функциями Гекке. Это приведет нас к частному случаю важной теоремы Дойринга. Наше изложение основано на фундаментальных статьях [23] и [81].

Техника, используемая в настоящее время при изучении эллиптических кривых, является одной из самых изощренных во всей математике. Мы надеемся, что элементарный подход настоящей главы побудит читателя к дальнейшему изучению этой живой и пленительной ветви теории чисел. Есть много того, что следует изучить, и много работы, которую еще надо проделать.

§ 1. Общие замечания

Мы начинаем с некоторых общих наблюдений над кривыми в проективном пространстве. Чтобы вспомнить терминологию, читателю следует обратиться к гл. 10, § 1.

Пусть K — некоторое поле и $F(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$ — однородный многочлен степени d. Один общий вопрос состоит в выяснении того, будет ли уравнение $F(x_0, x_1, x_2) = 0$ иметь решение в $P^2(K)$?

Полезно ввести геометрическую терминологию. Говорят, что уравнение

$$F(x_0, x_1, x_2) = 0$$

определяет кривую степени d над K. Поле K называется ее *полем определения*. Если L — поле, содержащее K, то можно рассматривать корни многочлена F в $P^2(L)$. В нашей прежней терминологии это есть $\overline{H}_F(L)$. Гиперповерхность в проективном 2-пространстве в нашем контексте называется *кривой*. Заметим, что многочлен F задает отображение множества полей, содержащих K, в совокупность множеств точек: $L \to \overline{H}_F(L)$.

Точка $a \in \overline{H}_F(L)$ называется *неособой*, если она не является решением системы уравнений

$$\frac{\partial F}{\partial x_0} = 0, \qquad \frac{\partial F}{\partial x_1} = 0, \qquad \frac{\partial F}{\partial x_2} = 0.$$

В таком случае прямая

$$0 = \frac{\partial F}{\partial x_0}(a)\, x_0 + \frac{\partial F}{\partial x_1}(a)\, x_1 + \frac{\partial F}{\partial x_2}(a)\, x_2$$

называется *касательной к F в a*. Кривая $F(x_0, x_1, x_2) = 0$ называется *неособой*, если все точки в $\overline{H}_F(L)$ неособые для всех расширений L поля K. Можно показать, что достаточно проверять это лишь для алгебраических расширений поля K. (В гл. 11 мы называли это свойство абсолютной неособостью.)

Если две кривые пересекаются в какой-либо точке, то можно определить целое число, называемое *кратностью пересечения* этих кривых в точке. Это довольно тонкое понятие, и мы не будем в него углубляться (см. [135], гл. 3). В общем случае, когда L алгебраически замкнуто, прямая в $P^2(L)$ пересекает кривую степени d в d точках, если принять во внимание кратности пересечения. Чтобы получить представление, почему это верно, запишем $x = x_1/x_0$, $y = x_2/x_0$ и $f(x, y) = F(1, x, y)$. Мы работаем в данный момент в аффинном 2-пространстве $A^2(L)$. Для нахождения точек пересечения кривой $f(x, y) = 0$ с прямой $y = mx + b$ подставляем значение y в f и находим корни уравнения $f(x, mx + b) = 0$. Если F имеет степень d, то последнее уравнение будет иметь в общем случае степень d, а так как L алгебраически замкнуто, будет в наличии d корней, если принять во внимание кратности пересечения. Исключениями являются лишь пересечения на бесконечности, когда $f(x, mx + b)$ будет иметь степень, меньшую d.

В качестве примера рассмотрим $F(x_0, x_1, x_2) = -x_0^3 - x_1^3 + x_0 x_2^2$. Тогда $f(x, y) = -1 - x^3 + y^2$, так что аффинная часть кривой задается уравнением $y^2 = x^3 + 1$. Пересечение с прямой $y = x + 1$ задается уравнением $(x + 1)^2 = x^3 + 1$, приводящим к трем точкам $(-1, 0)$, $(0, 1)$ и $(2, 3)$. С другой стороны, прямая $y = 1$ приводит к уравнению $x^3 = 0$. Это интерпретируется сле-

дующим образом: прямая $y = 1$ пересекает кривую $y^2 = x^3 + 1$ в точке (0, 1) с кратностью 3.

Пересечение с вертикальной прямой $x = c$ определяется уравнением $f(c, y) = 0$. В нашем примере $y^2 = c^3 + 1$, так что имеются две конечные точки пересечения $(c, \sqrt{c^3+1})$ и $(c, -\sqrt{c^3+1})$ при $c^3 + 1 \neq 0$. Третья точка пересечения бесконечно удаленная. Если $c^3 + 1 = 0$, то $(c, 0)$ — точка пересечения кратности 2.

Наконец, пересечение с бесконечно удаленной прямой $x_0 = 0$ может быть получено из уравнения $F(0, x_1, x_2) = -x_1^3 = 0$, так что $[0, 0, 1] \in P^2(L)$ будет точкой пересечения кратности 3.

Если $a \in \overline{H}_F(L)$, то касательная прямая к F в a пересекается с кривой $F = 0$ с кратностью 2 или больше. Если кратность больше, чем 2, то a называется *точкой перегиба*.

Если многочлен F определен над K, то его нуль в $P^2(K)$ называется *рациональной точкой* над K.

Мы будем говорить, что неособый однородный кубический многочлен

$$F(x_0, x_1, x_2) \in K[x_0, x_1, x_2]$$

определяет *эллиптическую кривую* над K, если имеется по крайней мере одна рациональная точка. Проблема определения всех рациональных точек на эллиптической кривой породила обширную теорию.

Один из фактов, делающих эллиптические кривые столь интересными, состоит в том, что множество рациональных точек можно естественным образом превратить в абелеву группу.

Пусть $F(x_0, x_1, x_2) = 0$ определяет эллиптическую кривую над K. Если L — некоторое расширение поля K, то мы будем писать $E(L)$ вместо $\overline{H}_F(L)$.

Пусть O будет некоторым элементом из $E(K)$. Если $P_1, P_2 \in E(L)$, то прямая, проходящая через P_1 и P_2, пересекает кривую в однозначно определенной третьей точке P_3, которая, как нетрудно убедиться, будет лежать в $E(L)$. Если $P_1 = P_2$, то касательная прямая в P_1 приводит к третьей точке P_3. Заманчиво взять P_3 в качестве «суммы» точек P_1 и P_2. Однако это не определит групповой структуры, ибо будет отсутствовать единичный элемент. Мы исправляем положение тем, что находим третью точку пересечения с E прямой, соединяющей O с P_3, и называем эту новую точку $P_1 + P_2$. При таком определении $E(L)$ превращается в абелеву группу с O в качестве единичного элемента. Доказательство этого не сложно, за исключением проверки ассоциативности, т. е. условия

$$P_1 + (P_2 + P_3) = (P_1 + P_2) + P_3.$$

Строгое обоснование этой конструкции см. в [135], гл. 5, особенно с. 124 и 125.

Если характеристика поля K отлична от 2 и 3, то можно показать, что каждая эллиптическая кривая над K может быть преобразована к виду

$$x_0x_2^2 = x_1^3 - Ax_0^2x_1 - Bx_0^3, \quad A, B \in K.$$

Эта кривая имеет в точности одну бесконечно удаленную точку $\{0, 0, 1\} \in P^2(K)$. Мы обозначаем эту точку через ∞ и выбираем ее в качестве нуля нашей группы.

Бесконечно удаленная прямая $x_0 = 0$ пересекает такую кривую в точке ∞ с кратностью 3. Если $x_0 \neq 0$, положим $x = x_1/x_0$ и $y = x_2/x_0$. Тогда определяющим уравнением для данной кривой в аффинных координатах будет

$$y^2 = x^3 - Ax - B.$$

Бесконечно удаленная точка представляется лежащей бесконечно далеко в направлении оси y.

Вычисление показывает, что неособость кривой

$$F(x_0, x_1, x_2) = x_0x_2^2 - x_1^3 + Ax_0^2x_1 + Bx_0^3$$

эквивалентна необращению в нуль числа

$$\Delta = 16(4A^3 - 27B^2).$$

Это число есть умноженный на -16 дискриминант многочлена

$$x^3 - Ax - B.$$

Обратно, если $\Delta \neq 0$, то F определяет эллиптическую кривую.

Тот факт, что ∞ является точкой перегиба, можно использовать для доказательства того, что $P_1 + P_2 + P_3 = \infty$ в том и только том случае, когда P_1, P_2 и P_3 лежат на одной прямой. В частности, $-P$ будет третьей точкой пересечения прямой, соединяющей P и ∞. В аффинных координатах это означает, что $-(a, b) = (a, -b)$, ибо прямая, соединяющая (a, b) и ∞, есть $x = a$. Точки порядка 2 суть те, для которых $b = 0$. Если $x^3 - Ax - B = (x - a_1)(x - a_2)(x - a_3) \in L[x]$, то точками порядка, делящего 2, в $E(L)$ будут ∞, $(a_1, 0)$, $(a_2, 0)$, $(a_3, 0)$.

В качестве примера сложения точек рассмотрим $P_1 = (2, 3)$ и $P_2 = (-1, 0)$ на $y^2 = x^3 + 1$. Прямая, соединяющая P_1 и P_2, задается уравнением $y = x + 1$. Уравнение $(x + 1)^2 = x^3 + 1$ имеет три корня 2, -1 и 0, соответствующих P_1, P_2 и $(0, 1)$. Таким образом, $P_1 + P_2 = (0, -1)$.

Предположим теперь, что $K = \mathbf{Q}$ — поле рациональных чисел. В 1922 г. Морделл доказал следующую замечательную теорему, высказанную в виде гипотезы Пуанкаре в 1901 г. [203].

Теорема 1. *Пусть E — некоторая эллиптическая кривая, определенная над $\mathbf{Q}$. Тогда $E(\mathbf{Q})$ — конечно порожденная абелева группа.*

В 1928 г. А. Вейль распространил этот результат на случай, когда $\mathbf{Q}$ заменяется на произвольное поле алгебраических чисел. На эту теорему ссылаются теперь как на теорему Морделла — Вейля.

Подгруппа $E(\mathbf{Q})_t \subseteq E(\mathbf{Q})$, состоящая из точек конечного порядка, конечна. Существует эффективный метод вычисления $E(\mathbf{Q})_t$ в любом заданном случае.

Когда-то была высказана гипотеза о существовании равномерной верхней границы для $|E(\mathbf{Q})_t|$, когда E пробегает все эллиптические кривые, определенные над $\mathbf{Q}$. Шимурой и другими было замечено, что для решения этой проблемы может быть использована теория модулярных эллиптических кривых. Эта точка зрения была интенсивно использована Оггом, который доказал ряд частных результатов и высказал несколько довольно точных гипотез. Наконец, в 1976 г. Мазур доказал следующий очень глубокий результат, высказанный в виде гипотезы Оггом.

Теорема 2. *Пусть E — некоторая эллиптическая кривая, определенная над $\mathbf{Q}$. Тогда $E(\mathbf{Q})_t$ изоморфна одной из следующих групп: $\mathbf{Z}/m\mathbf{Z}$ при $m \leqslant 10$ или $m = 12$, $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2m\mathbf{Z}$ при $m \leqslant 4$.*

Вероятно также, что существует равномерная верхняя граница для $|E(K)_t|$, где E пробегает эллиптические кривые, определенные над некоторым фиксированным полем алгебраических чисел K. Неизвестно, верно ли это хотя бы для одного такого $K \neq \mathbf{Q}$, но частные результаты получили, среди других авторов, В. А. Демьяненко, Куберт и Ю. И. Манин.

Еще более неподатливым оказалось другое важное целое число, связанное с $E(\mathbf{Q})$, а именно ранг. Ранг абелевой группы есть максимальное число ее независимых элементов.

Мы говорим, что множество элементов $a_1, a_2, \ldots, a_t \in A$ абелевой группы A независимо, если из равенства $m_1a_1 + m_2a_2 + \ldots + m_ta_t = 0$ с $m_1, m_2, \ldots, m_t \in \mathbf{Z}$ следует, что $m_1 = m_2 = \ldots = m_t = 0$. Мы обозначаем ранг группы $E(\mathbf{Q})$ через r_E.

Ранг r_E был вычислен для многих эллиптических кривых над $\mathbf{Q}$. В большинстве примеров он очень мал: 0, 1 или 2. Нерон показал, что существует эллиптическая кривая над $\mathbf{Q}$ ранга 11. Но его метод не конструктивен. В 1977 г. Брумер и Крамер построили явный пример с $r_E \geqslant 9$. Приведем его:

$$y^2 + 525xy = x^3 + 228x^2 - 14\,972\,955x + (856\,475)^2\ ^{1}).$$

Неизвестно, существует ли верхняя граница для чисел r_E, где E определено над $\mathbf{Q}$. Касселс считает это маловероятным ([109], § 20).

---

[1]) Более простой пример $y^2 + 9767y = x^3 + 3576x^2 + 425x - 2412$ с $r_E \geqslant 9$ получен в [28*]. Там же приведены примеры кривых с $r_E \geqslant 14$. — *Прим. ред.*

Одна из наиболее знаменитых гипотез в современной теории чисел связывает число r_E с порядком в $s = 1$ некоторой аналитической функции, соответствующей E. Эта гипотеза была сформулирована английскими математиками Бёрчем и Суиннертоном-Дайером. Формулировка этой гипотезы является целью следующего параграфа.

§ 2. Локальная и глобальная дзета-функции эллиптической кривой

Пусть E — эллиптическая кривая, определенная над $\mathbf{Q}$ уравнением

$$x_0x_2^2 = x_1^3 - Ax_0^2x_1 - Bx_0^3, \quad A, B \in \mathbf{Q}. \tag{i}$$

Аффинное уравнение получим, положив $x = x_1/x_0$ и $y = x_2/x_0$:

$$y^2 = x^3 - Ax - B. \tag{ii}$$

Преобразование $(x, y) \to (c^2x, c^3y)$ переводит это уравнение в

$$y^2 = x^3 - c^4Ax - c^6B. \tag{iii}$$

Таким образом, с самого начала можем предполагать, что $A, B \in \mathbf{Z}$. Число $\Delta = 16\,(4A^3 - 27B^2)$ называется *дискриминантом* кривой E. Как мы видели, $\Delta \neq 0$.

Пусть $p \in \mathbf{Z}$ — некоторое простое число, и рассмотрим сравнение

$$y^2 \equiv x^3 - Ax - B \ (p).$$

или, что эквивалентно, уравнение

$$y^2 = x^3 - \bar{A}x - \bar{B}, \quad \bar{A}, \bar{B} \in \mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p. \tag{iv}$$

Это уравнение определяет эллиптическую кривую E_p над $\mathbf{F}_p$, если только $p \nmid \Delta$. В дальнейшем будут рассматриваться только такие простые числа, если явно не оговорено противное. Кривая E_p называется редукцией кривой E по модулю p.

Пусть N_{p^m} обозначает число точек в E_p $(\mathbf{F}_{p^m})$. Тогда, как в гл. 11, мы можем рассмотреть дзета-функцию

$$Z(E_p, u) = \exp\left(\sum_{m=1}^{\infty} N_{p^m} \frac{u^m}{m}\right). \tag{v}$$

Используя теорему Римана — Роха, можно показать (см. [8*]. — *Ред.*), что

$$Z(E_p, u) = \frac{1 - a_pu + pu^2}{(1-u)(1-pu)}, \quad a_p \in \mathbf{Z}. \tag{vi}$$

В частных случаях это можно доказать, используя методы гл. 11. Хассе смог доказать, что $a_p^2 \leqslant 4p$. Отсюда следует, что

$$1 - a_p u + pu^2 = (1 - \pi u)(1 - \bar{\pi} u), \qquad \text{(vii)}$$

где $\bar{\pi}$ — комплексно сопряженное к π. Ясно, что $\pi\bar{\pi} = p$, $a_p = \pi + \bar{\pi}$. Кроме того, $|\pi| = |\bar{\pi}| = \sqrt{p}$. Это есть «гипотеза Римана» для эллиптических кривых над $\mathbf{F}_p$ [1]).

Логарифмически дифференцируя (v) и (vi), учитывая (vii) и приравнивая коэффициенты, получаем

$$N_{p^m} = p^m + 1 - \pi^m - \bar{\pi}^m. \qquad \text{(viii)}$$

В частности, $N_p = p + 1 - a_p$. Таким образом, вычислив N_p, мы определим a_p. Так как π и $\bar{\pi}$ являются корнями уравнения $T^2 - a_p T + p = 0$, то равенство (viii) определяет N_{p^m} для всех $m \geqslant 1$.

Далее будет полезен следующий очень частный случай. Если $N_p = p + 1$, то

$$Z(E_p, u) = \frac{1 + pu^2}{(1 - u)(1 - pu)}.$$

Полезно заменить переменную u на p^{-s}. Полагаем

$$\zeta(E_p, s) = \frac{1 - a_p p^{-s} + p^{1-2s}}{(1 - p^{-s})(1 - p^{1-s})}. \qquad \text{(ix)}$$

Функция $\zeta(E_p, s)$ называется *локальной дзета-функцией* кривой E в p.

Интересно убедиться в том, что дзета-функция $\zeta(E_p, s)$ может быть получена, исходя из другой точки зрения, которая более явно выявляет ее связи с дзета-функцией Римана.

Кольцо $\mathbf{F}_p[x]$ и его поле частных $\mathbf{F}_p(x)$ аналогичны $\mathbf{Z}$ и его полю частных $\mathbf{Q}$. Пусть

$$K = \mathbf{F}_p(x)\left(\sqrt{x^3 - Ax - B}\right)$$

и D — целое замыкание кольца $\mathbf{F}_p[x]$ в K, т. е. D состоит из всех элементов K, которые являются корнями всевозможных приведенных многочленов из $\mathbf{F}_p[x]$. Кольцо D является дедекиндовой областью и каждый его ненулевой идеал имеет конечный индекс в D. Если $I \subset D$ — какой-либо ненулевой идеал, то положим $NI = |D/I|$ и $\zeta_D(s) = \sum NI^{-s}$, где сумма берется по всем

---

[1]) Если сделать подстановку $u = p^{-s}$, то функция $Z(E_p, p^{-s})$ становится, как показано ниже, аналогом дзета-функций полей алгебраических чисел, и в частности дзета-функции Римана. Условие $|\pi| = |\bar{\pi}| = \sqrt{p}$ для нулей преобретает тогда вид $\mathrm{Re}\, s = 1/2$, чем и объясняется его название в тексте. — *Прим. ред.*

ненулевым идеалам в D. Нетрудно показать, что $\zeta_D(s)$ сходится для $\operatorname{Re} s > 1$. Более того, можно показать, что $\zeta_D(s) = (1 - p^{-s})\,\zeta(E_p, s)$. См. также § 1 гл. 11.

Намеченная здесь точка зрения развита Артином в его диссертации [2].

Мы определили $\zeta(E_p, s)$ для простых чисел $p \nmid \Delta$. Если $p \mid \Delta$, то мы полагаем

$$\zeta(E_p, s) = \frac{1}{(1 - p^{-s})(1 - p^{1-s})}.$$

Это определение не лучшее, но его достаточно для наших целей.

Теперь, введя локальную дзета-функцию для всех простых чисел p, мы определяем *глобальную дзета-функцию* просто как произведение локальных дзета-функций:

$$\zeta(E, s) = \prod_p \zeta(E_p, s). \tag{x}$$

Из определения мы видим, что

$$\zeta(E, s) = \zeta(s)\,\zeta(s-1)\,L(E, s)^{-1},$$

где

$$L(E, s) = \prod_{p \nmid \Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}. \tag{xi}$$

Функция $L(E, s)$ называется *L-функцией* кривой E. Вспоминая результат Хассе о том, что $(1 - a_p p^{-s} + p^{1-2s}) = (1 - \pi p^{-s})(1 - \bar{\pi} p^{-s})$ с $|\pi| = |\bar{\pi}| = \sqrt{p}$, можно очень легко показать, что произведение из определения $L(E, s)$ сходится для $\operatorname{Re} s > 3/2$.

Хассе высказал гипотезу о том, что $\zeta(E, s)$ может быть аналитически продолжена на всю плоскость $\mathbf{C}$ [1]). Тот факт, что это

---

[1]) Это предположение может быть дополнено гипотезой о функциональном уравнении для L-ряда. Добавим с этой целью в произведение (xi) сомножители, отвечающие простым числам, делящим Δ. А именно если редукция $\bmod p$ кривой E имеет двойную особую точку с разделенными касательными, то возьмем сомножителем $(1 \pm p^{-s})^{-1}$, где знак выбирается в зависимости от того, будут касательные в особой точке рациональными над $\mathbf{F}_p$ или нет. Во всех остальных случаях положим соответствующий сомножитель равным 1. Тогда для нового L-ряда должно выполняться соотношение

$$(2\pi)^{-s}\,\Gamma(s)\,L(E, s) = \pm N^{1-s}\,(2\pi)^{-(2-s)}\,\Gamma(2-s)\,L(E, 2-s).$$

Здесь $N = \prod_{p \mid \Delta} p^{b_p}$ — кондуктор эллиптической кривой E, $b_p = 1$, если $E \bmod p$ имеет двойную особую точку, и $b_p = 2$ в оставшихся случаях (в предположении, что $p \neq 2, 3$; по поводу b_2 и b_3 см. [29*]).

Это соотношение полезно сравнить с функциональным уравнением для дзета-функции Дедекинда (см. [8*], [168] и примечание к гл. 16, § 6). — *Прим. ред.*

верно в частных случаях, впервые установил Вейль [81]. После этого Дойринг доказал этот результат для важного класса эллиптических кривых, которые обладают «комплексным умножением».

Результаты Дойринга изложены в [169], гл. 10. Таниями и позже Вейль высказали гипотезу о том, что каждая эллиптическая кривая над $\mathbf{Q}$ может быть параметризована эллиптическими модулярными формами. См. статью Суиннертона-Дайера в [226] по поводу точной формулировки этой гипотезы. Для таких кривых выполняется гипотеза Хассе [1]). Таким образом, предположение о справедливости гипотезы Хассе становится довольно убедительным.

Предположив, что $L(E, s)$ может быть продолжена на всю плоскость $\mathbf{C}$, имеет смысл говорить об ее аналитическом поведении в окрестности точки $s = 1$.

Основываясь на обширном эмпирическом материале о кривых вида $y^2 = x^3 - Dx$, Бёрч и Суиннертон-Дайер пришли к следующей замечательной гипотезе.

Гипотеза. *Предположим, что E — некоторая эллиптическая кривая, определенная над $\mathbf{Q}$. Тогда ранг группы E, r_E, равен порядку нуля L-функции $L(E, s)$ в $s = 1$.*

Эта гипотеза может быть дополнена. Предполагая, что эта гипотеза справедлива, мы можем определить ненулевую константу

$$B_E = \lim_{s \to 1} (s - 1)^{-r_E} L(E, s).$$

Бёрч и Суиннертон-Дайер дают выражение для B_E, которое зависит от тонких арифметических инвариантов кривой E. Обсуждение этого здесь увело бы нас слишком далеко. См. [109] и [227] (а также [21*], [29*]. — *Ред.*).

В важной статье [114], опубликованной в 1977 г., сделано значительное продвижение в направлении сформулированной гипотезы. Основной результат из нее был затем обобщен в [87]. Даже формулировка этого результата в полной общности увела бы нас в теорию комплексного умножения, поэтому мы ограничимся частным случаем.

---

[1]) По поводу аргументов в пользу этого предположения Таниямы—Вейля см. [29*], где содержатся, в частности, обширные численные результаты. Из работ [7*], [29*], с. 10, и [25*] вытекает, что, обратно, если для дзета-функции эллиптической кривой над $\mathbf{Q}$ (и некоторых ее обобщений, которые относятся к дзета-функции примерно так же, как L-функции Гекке поля алгебраических чисел к его дзета-функции Дедекинда) выполняется функциональное уравнение, то кривая E параметризуется модулярными функциями по Танияме—Вейлю. — *Прим. ред.*

Теорема 3. *Пусть E — какая-либо эллиптическая кривая, определенная над $\mathbf{Q}$, и предположим, что она обладает комплексным умножением. Если $L(E, 1) \neq 0$, то группа $E(\mathbf{Q})$ конечна* [1]).

Большинство обсуждавшихся нами работ написано на очень высоком уровне и лежат вне рамок этой книги. В следующих параграфах мы рассмотрим эллиптические кривые двух типов: $y^2 = x^3 + D$ и $y^2 = x^3 - Dx$.

Для этих кривых мы анализируем локальные и глобальные дзета-функции и показываем на основе фундаментального результата Гекке, что глобальная дзета-функция этих кривых может быть аналитически продолжена на всю плоскость $\mathbf{C}$. Это дает читателю по меньшей мере пример из обширной арифметической теории эллиптических кривых.

§ 3. $y^2 = x^3 + D$, локальный случай

Пусть D — ненулевое целое число. Мы будем рассматривать эллиптическую кривую E, определяемую уравнением $x_0x_2^2 = x_1^3 - Dx_0^3 = 0$, или в аффинных координатах $y^2 = x^3 + D$. Дискриминант Δ кривой E равен $-2^4 3^3 D^2$, так что мы будем рассматривать лишь простые числа $p \neq 2, 3$ и $p \nmid D$.

Кривая $y^2 = x^3 + \overline{D}$ над $\mathbf{F}_p$ имеет одну бесконечно удаленную точку. Таким образом, $N_p = 1 + N(y^2 = x^3 + \overline{D})$, где мы используем обозначения из гл. 8. При помощи сумм Якоби мы получим явную формулу для N_p. Начиная с этого места, будем писать D вместо $\overline{D}$, так что «для простоты записи» D будет обозначать класс вычетов D по модулю p.

Если $p \equiv 2$ (3), то $x \to x^3$ будет автоморфизмом группы $\mathbf{F}_p^*$. Нетрудно получить (см. упр. 1), что в этом случае $N_p = p + 1$.

Если $p \equiv 1$ (3), то пусть χ — характер порядка 3 и ρ — характер порядка 2 группы $\mathbf{F}_p^*$. Тогда

$$N(y^2 = x^3 + D) = \sum_{u+v=D} N(y^2 = u)\, N(x^3 = -v) =$$

$$= \sum_{u+v=D} (1 + \rho(u))(1 + \chi(-v) + \chi^2(-v)) =$$

$$= p + \sum_{u+v=D} \rho(u)\chi(v) + \sum_{u+v=D} \rho(u)\chi^2(v).$$

---

[1]) Гросс и Загир недавно доказали частный случай гипотезы Бёрча и Суиннертона-Дайера для эллиптических кривых E над $\mathbf{Q}$, обладающих модулярной параметризацией (см. выше). Если $L(E, s)$ имеет простой нуль в точке $s = 1$, то на E имеется рациональная точка бесконечного порядка, т. е. $r_E \geqslant 1$ [27*]. — *Прим. ред.*

Мы воспользовались тем, что $\chi(-1) = 1$. Производя замену переменных $u = Du'$ и $v = Dv'$, получаем

$$N_p = p + 1 + \rho\chi(D)\, J(\rho, \chi) + \overline{\rho\chi(D)}\, \overline{J(\rho, \chi)}, \qquad \text{(i)}$$

где черта обозначает комплексное сопряжение.

Для более глубокого анализа соотношения (i) будет полезна следующая лемма.

Лемма. *Пусть p — нечетное простое число, ρ — характер порядка 2 и ξ — любой нетривиальный характер группы $\mathbf{F}_p^*$. Тогда*

$$J(\rho, \xi) = \xi(4)\, J(\xi, \xi).$$

Доказательство. Имеем

$$J(\rho, \xi) = \sum_{u+v=1} \rho(u)\xi(v) =$$

$$= \sum_{u+v=1} (1 + \rho(u))\xi(v) = \sum_{u+v=1} N(t^2 = u)\xi(v) =$$

$$= \sum_t \xi(1-t)^2 = \xi(4) \sum_t \xi\left(\frac{1-t}{2}\right)\xi\left(\frac{1+t}{2}\right) = \xi(4)\, J(\xi, \xi). \square$$

Используя лемму, равенство (i) можно преобразовать в

$$N_p = p + 1 + \rho\chi(D)\, J(\chi, \chi) \pm \overline{\rho\chi(4D)\, J(\chi, \chi)}. \qquad \text{(ii)}$$

Мы хотим уточнить теперь характеры ρ и χ. Так как $p \equiv 1\ (3)$, то $p = \pi\bar{\pi}$ в $\mathbf{Z}[\omega]$ (напомним, что $\omega = e^{2\pi i/3}$), где π и $\bar{\pi}$ можно выбрать примарными, т. е. $\pi \equiv \bar{\pi}\ (3) \equiv 2\ (3)$. Пусть $(a/\pi)_6$ — символ вычета степени 6, и возьмем $\rho(a) = (a/\pi)_6^3$ и $\chi(a) = (a/\pi)_6^2 = (a/\pi)_3$. Тогда $\rho\chi(a) = \rho(a)\chi(a) = (a/\pi)_6^5 = \overline{(a/\pi)_6}$. Наконец, полагая $\chi_\pi(a) = (a/\pi)_3$, из леммы 1 § 4 гл. 9 получаем $J(\chi_\pi, \chi_\pi) = \pi$. Подставляя эти выражения в равенство (ii), приходим к такому результату:

Теорема 4. *Предположим, что $p \neq 2, 3$ и $p \nmid D$. Рассмотрим эллиптическую кривую $y^2 = x^3 + D$ над $\mathbf{F}_p$. Если $p \equiv 2\ (3)$, то $N_p = p + 1$. Если $p \equiv 1\ (3)$, то пусть $p = \pi\bar{\pi}$ с $\pi \in \mathbf{Z}[\omega]$ и $\pi \equiv 2\ (3)$. Тогда*

$$N_p = p + 1 + \overline{\left(\frac{4D}{\pi}\right)_6}\,\pi + \left(\frac{4D}{\pi}\right)_6 \bar{\pi}.$$

Теорема 4 полностью определяет локальную дзета-функцию кривой $y^2 = x^3 + D$.

В качестве примера рассмотрим кривую $y^2 = x^3 + 1$ над $\mathbf{F}_{13}$. Имеем $13 = (-1 + 3\omega)(-1 + 3\omega^2)$ и $-1 + 3\omega \equiv 2$ (3). Для применения формулы из теоремы 4 мы должны знать, что $(4/-1 + 3\omega)_6 = (2/-1 + 3\omega)_3$. Так как $2^{(13-1)/3} = 2^4 \equiv 3$ $(-1 + 3\omega) \equiv \omega^2 (-1 + 3\omega)$, то $(2/-1 + 3\omega)_3 = \omega^2$. Формула из теоремы 4 дает

$$N_{13} = 13 + 1 + \omega(-1 + 3\omega) + \omega^2(-1 + 3\omega^2) = 14 + 2(\omega^2 + \omega) = 14 - 2 = 12.$$

Нетрудно проверить, что точками на кривой $y^2 = x^3 + 1$ с координатами в поле $\mathbf{F}_{13}$ будут ∞, (4, 0), (10,0), (12, 0), (0, ± 1), (2, ± 3), (5, ± 3) и (6, ± 3).

§ 4. $y^2 = x^3 - Dx$, локальный случай

Пусть D — ненулевое целое число. Рассмотрим эллиптическую кривую E, определенную уравнением $x_0x_2^2 - x_1^3 + Dx_1x_0^2 = 0$, или в аффинных координатах $y^2 = x^3 - Dx$. Дискриминант кривой E есть $\Delta = 2^6D^3$. Мы будем рассматривать лишь простые числа $p \neq 2$ и $p \nmid D$.

Кривая $y^2 = x^3 - Dx$ над $\mathbf{F}_p$ (мы продолжаем писать D вместо $\overline{D}$) имеет одну бесконечно удаленную точку, так что $N_p = 1 + N(y^2 = x^3 - Dx)$. В этом случае методы гл. 8 не применимы непосредственно. Мы сначала преобразуем кривую $y^2 = x^3 - Dx$ в кривую $u^2 = v^4 + 4D$. Число же решений уравнения $u^2 = v^4 + 4D$ может быть подсчитано нашими прежними методами.

Пусть C и C' обозначают кривые $y^2 = x^3 - Dx$ и $u^2 = v^4 + 4D$ соответственно. Определим преобразование T следующим образом:

$$T(u, v) = \left(\frac{1}{2}(u + v^2), \frac{1}{2}v(u + v^2)\right).$$

Простое вычисление показывает, что T отображает C' в C. Точка (0, 0) на C не лежит в образе, так как равенство $4D = u^2 - v^4 = (u - v^2)(u + v^2)$ показывает, что $u + v^2 \neq 0$.

Определим преобразование S посредством формулы

$$S(x, y) = \left(2x - \frac{y^2}{x^2}, \frac{y}{x}\right).$$

Нетрудно показать, что S отображает $C - \{(0, 0)\}$ в C' и, кроме того, TS тождественно на $C - \{(0, 0)\}$ и ST тождественно на C'. Пусть $N' = N(u^2 = v^4 + 4D)$ и $N = N(y^2 = x^3 - Dx)$. Мы показали что $N - 1 = N'$.

Если $p \equiv 3$ (4), то -1 будет квадратным невычетом, так что каждый элемент $\mathbf{F}_p$ будет иметь вид $\pm w^2$. Таким образом, каждый квадрат автоматически является четвертой степенью. Следовательно,

$$N' = N(u^2 = v^4 + 4D) = N(u^2 = v^2 + 4D) = p - 1.$$

Таким образом, мы нашли, что при $p \equiv 3$ (4) будет $N_p = 1 + N = 2 + N' = 2 + p - 1 = p + 1$.

Предположим теперь, что $p \equiv 1$ (4). Пусть λ — характер порядка 4 поля $\mathbf{F}_p$, и положим $\rho = \lambda^2$. Тогда уже знакомым нам способом получаем

$$N(u^2 = v^4 + 4D) = \sum_{r+s=4D} N(u^2 = r)\, N(v^4 = -s) =$$

$$= p - 1 + \overline{\lambda(-4D)}\, J(\rho, \chi) + \lambda(-4D)\, \overline{J(\rho, \chi)}. \quad \text{(i)}$$

Мы использовали то, что при $p \equiv 1$ (4) будет $J(\rho, \rho) = -1$ (см. гл. 8, § 3 теорема 1). По лемме из предыдущего параграфа имеем $J(\rho, \lambda) = \lambda(4)\, J(\lambda, \lambda)$. Таким образом,

$$\overline{\lambda(-4D)}\, J(\rho, \lambda) = \overline{\lambda(D)}\, \lambda(-1)\, J(\lambda, \lambda).$$

Выберем теперь λ более конкретно. Так как $p \equiv 1$ (4), то $p = \pi\bar{\pi}$ в $\mathbf{Z}[i]$ с примарным π, т. е. $\pi \equiv 1$ $(2 + 2i)$. Отождествим $\mathbf{F}_p$ с $\mathbf{Z}[i]/\pi\mathbf{Z}[i]$ и выберем в качестве λ символ биквадратичного вычета, $\lambda(a) = (a/\pi)_4$. Тогда в силу предложения 9.9.4

$$-\lambda(-1)\, J(\lambda, \lambda) = \pi.$$

Подставляя все полученное в равенство (i), получаем следующую теорему.

Теорема 5. *Предположим, что $p \neq 2$ и $p \nmid D$. Рассмотрим эллиптическую кривую $y^2 = x^3 - Dx$ над $\mathbf{F}_p$. Если $p \equiv 3$ (4), то $N_p = p + 1$. Если $p \equiv 1$ (4), то пусть $p = \pi\bar{\pi}$ с $\pi \in \mathbf{Z}[i]$ и $\pi \equiv 1$ $(2 + 2i)$. Тогда*

$$N_p = p + 1 - \overline{\left(\frac{D}{\pi}\right)_4}\, \pi - \left(\frac{D}{\pi}\right)_4 \bar{\pi}.$$

В качестве примера рассмотрим $y^2 = x^3 - x$ над $\mathbf{F}_{13}$. Имеем

$$13 = (3 + 2i)(3 - 2i)$$

и $3 + 2i \equiv 1$ $(2 + 2i)$. По формуле из теоремы 4 получаем, что $N_{13} = 13 + 1 - (3 + 2i) - (3 - 2i) = 14 - 6 = 8$. Действительно, простое вычисление показывает, что точками на $y^2 = x^3 - x$ с координатами в $\mathbf{F}_{13}$ будут ∞, $(0, 0)$, $(1, 0)$, $(-1, 0)$, $(5, \pm 4)$ и $(-5, \pm 6)$.

§ 5. L-функции Гекке

В двух важных статьях, опубликованных в 1918 и 1920 гг., немецкий математик Гекке ввел новый класс характеров и L-функций. Их можно определить над произвольным полем алгебраических чисел. Мы сосредоточим наше внимание на алгебраических характерах Гекке над CM-полями определенного типа (терминология поясняется ниже). В приложениях, которые мы намереваемся привести, этого будет достаточно.

Пусть $K/\mathbf{Q}$ — некоторое поле алгебраических чисел. Изоморфизм σ поля K в $\mathbf{C}$ называется *вещественным*, если $\sigma(K) \subset \mathbf{R}$, в противном случае он называется *комплексным*. K называется *вполне вещественным*, если каждый изоморфизм поля K в $\mathbf{C}$ вещественный. K называется *вполне комплексным*, если каждый изоморфизм поля K в $\mathbf{C}$ комплексный. K называется *CM-полем*, если оно является вполне комплексным расширением некоторого своего вполне вещественного подполя K_0. Например, если $d \in \mathbf{Q}$ с $d > 0$, то $\mathbf{Q}(\sqrt{-d})$ есть CM-поле. Другие примеры дают круговые поля $\mathbf{Q}(\zeta_m)$. Вполне вещественным подполем в $\mathbf{Q}(\zeta_m)$ является $\mathbf{Q}(\zeta_m + \zeta_m^{-1})$.

Пусть $K \subset \mathbf{C}$ — такое CM-поле, что $K/\mathbf{Q}$ — нормальное расширение. Пусть j — ограничение комплексного сопряжения на K. Тогда нетрудно убедиться (упр. 2) в том, что j лежит в центре G группы Галуа поля $K/\mathbf{Q}$. Кроме того, K_0 — подполе инвариантных элементов при действии j. Мы предполагаем далее, что K удовлетворяет перечисленным условиям.

Пусть $\mathcal{O} \subset K$ — кольцо целых чисел и $M \subseteq \mathcal{O}$ — некоторый идеал. *Алгебраический характер Гекке по модулю M* есть функция χ из множества идеалов кольца $\mathcal{O}$ в $\mathbf{C}$, удовлетворяющая следующим условиям:

(i) $\chi(\mathcal{O}) = 1$;

(ii) $\chi(A) \neq 0$ в том и только том случае, когда A взаимно прост с M;

(iii) $\chi(AB) = \chi(A)\chi(B)$;

(iv) существует такой элемент $\theta = \sum n(\sigma)\sigma \in \mathbf{Z}[G]$, что если $\alpha \in \mathcal{O}$, $\alpha \equiv 1 \ (M)$, то $\chi((\alpha)) = \alpha^{\theta}$;

(v) существует такое целое число m, что $n(\sigma) + n(j\sigma) = m$ для всех $\sigma \in G$.

Последнее условие, как нетрудно видеть, эквивалентно условию $(1 + j)\theta = mN$, где $N = \sum \sigma$ — элемент нормы в $\mathbf{Z}[G]$.

Число m в условии (v) называется *весом* характера χ.

Следует заметить также, что по условию (iii) характер χ полностью определен своими значениями на простых идеалах, не делящих M.

Предложение 18.5.1. *Пусть* χ — *некоторый алгебраический характер Гекке веса* m. *Тогда при* $(A, M) = (1)$ *имеем* $|\chi(A)| = NA^{m/2}$.

Доказательство. Пусть I_M — множество идеалов в $\mathcal{O}$, взаимно простых с M. Мы вводим на I_M понятие эквивалентности следующим образом: при $A, B \in I_M$ полагаем $A \sim B$, если существуют такие $\alpha, \beta \in \mathcal{O}$, что $\alpha, \beta \equiv 1\ (M)$ и $(\alpha)\, A = (\beta)\, B$. Можно показать, что классов эквивалентности имеется конечное число и они образуют группу C_M. Произведение в этой группе переводит классы эквивалентности идеалов A и B в класс эквивалентности идеала AB. Если $M = \mathcal{O}$, то эта конструкция приводит к группе классов идеалов кольца $\mathcal{O}$ (см. гл. 12, § 1). Пусть h — число элементов в C_M.

Если $A \in I_M$, то существуют такие $\alpha, \beta \in \mathcal{O}$, $\alpha, \beta \equiv 1\ (M)$, что $(\alpha)\, A^h = (\beta)$. Таким образом, $\alpha^\theta \chi(A)^h = \beta^\theta$.

Возьмем комплексное сопряжение этого равенства и перемножим результаты:

$$(\alpha^\theta)^{1+j} |\chi(A)|^{2h} = (\beta^\theta)^{1+j},$$

или в силу (v)

$$(N\alpha)^m |\chi(A)|^{2h} = (N\beta)^m.$$

Так как $(\alpha)\, A^h = (\beta)$, то также

$$N\alpha N A^h = N\beta.$$

Сравнивая эти два равенства, получаем $|\chi(A)^{12h} = NA^{mh}$ и $|\chi(A)| = N(A)^{m/2}$. □

Это доказательство показывает, что значения $\chi(A)$ являются алгебраическими числами (на самом деле корнями степени h из элементов поля K). Это частично объясняет, почему χ называется алгебраическим характером Гекке.

Мы переходим теперь к определению L-функции, задаваемой некоторым алгебраическим характером Гекке χ. А именно, полагаем

$$L(s, \chi) = \prod_P (1 - \chi(P)\, NP^{-s})^{-1} = \sum_A \chi(A)\, NA^{-s}.$$

Произведение берется по всем простым идеалам в $\mathcal{O}$, а сумма — по всем идеалам в $\mathcal{O}$.

Простая оценка показывает, что произведение сходится абсолютно для $\operatorname{Re} s > 1 + m/2$ и равномерно для $\operatorname{Re} s \geqslant 1 + m/2 + \delta$ при любом $\delta > 0$. В самом деле, произведение абсолютно сходится в том и только том случае, когда $\sum_P |\chi(P)\, NP^{-s}|$ сходится.

В силу предложения 18.5.1 при вещественном s

$$|\chi(P)NP^{-s}| = NP^{(m/2)-s} \leqslant p^{-(s-m/2)},$$

где p — рациональное простое число, делящееся на P. Так как каждое рациональное простое число имеет, самое большее, $[K:\mathbf{Q}]$ делителей в $\mathcal{O}$, то

$$\sum |\chi(P)NP^{-s}| \leqslant [K:\mathbf{Q}] \sum_p p^{-(s-m/2)},$$

что сходится при $s > 1 + m/2$.

Используя тот факт, что произведение для $L(s, \chi)$ абсолютно сходится при $\operatorname{Re} s > 1 + m/2$, можно показать, что сумма тоже сходится в этой области и что они совпадают.

Основной факт об L-функциях Гекке, который нам понадобится, дается следующей теоремой. Ее длинное и трудное доказательство мы не приводим (см. [8*], [168], [44]. — *Ред.*).

Теорема 6. *Пусть χ — некоторый алгебраический характер Гекке и $L(s, \chi)$ — соответствующая L-функция. Если $\chi(A) \neq 1$ при некотором A, то $L(s, \chi)$ может быть аналитически продолжена до целой функции на всей плоскости* $\mathbf{C}$.

Следует заметить, что эта теорема справедлива для всех числовых полей и всех L-функций Гекке, а не только для тех, которые возникают из алгебраических характеров Гекке. Более того, Гекке получил очень важное функциональное уравнение для своих L-функций. Для случая, когда χ — алгебраический характер Гекке веса m, это функциональное уравнение связывает $L(s, \chi)$ с $L(m + 1 - s, \tilde{\chi})$.

Некоторые авторы производят нормализацию, полагая $\tilde{\chi}(A) = \chi(A)/NA^{m/2}$. Тогда $L(s, \tilde{\chi}) = \prod_p (1 - \tilde{\chi}(P)/NP^{-s})^{-1}$ сходится для $\operatorname{Re} s > 1$ (следует воспользоваться тем же самым рассуждением, что и для $L(s, \chi)$, вместе с фактом, что при $(A, M) = (1)$ имеем $|\tilde{\chi}(A)| = 1$). Мы будем работать непосредственно с характером Гекке χ.

В следующих двух параграфах мы покажем, что L-функции $L(E, s)$ для эллиптических кривых вида $y^2 = x^3 + D$ и $y^2 = x^3 - Dx$ будут L-функциями Гекке. В первом случае мы построим алгебраический характер Гекке на $\mathbf{Q}(\omega)$, а во втором — на $\mathbf{Q}(i)$.

Последнее замечание. В гл. 14 при помощи сумм Гаусса мы определили функцию $\Phi(A)$ на идеалах поля $\mathbf{Q}(\zeta_m)$, взаимно простых с m. Можно показать, что $\Phi(A)$ продолжается до алгебраического характера Гекке с модулем (m^2) и веса m. Это впервые было показано А. Вейлем в [81]. В более поздней статье [236]

он отмечает, что случай, когда m — нечетное простое число, рассматривался Эйзенштейном.

§ 6. $y^2 = x^3 - Dx$, глобальный случай

Мы приступаем теперь к анализу глобальной дзета-функции эллиптической кривой E, определенной уравнением $y^2 = x^3 - Dx$, $D \in \mathbf{Z}$. Достаточно рассмотреть соответствующую E L-функцию $L(E, s)$. Так как $\Delta = 2^6 D^3$ в этом случае, то мы имеем (см. равенство (x) § 2)

$$L(E, s) = \prod_{p \nmid 2D} (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

Числа a_p определены равенством $N_p = p + 1 - a_p$ и N_p определены в теореме 5 из § 4.

Построим такой алгебраический характер χ на $\mathbf{Z}[i]$ по модулю $(8D)$, что $L(E, s) = L(s, \chi)$.

Для этого χ достаточно определить $\chi(P)$ при простых идеалах P в $\mathbf{Z}[i]$. Если P делит $2D$, полагаем $\chi(P) = 0$. Предположим, что P не делит $2D$. Если $NP = p$, то $p \equiv 1\ (4)$ и $P = (\pi)$ с $\pi \equiv 1\ (2 + 2i)$. Пусть $\chi(P) = \overline{(D/\pi)}_4 \pi$. Если $NP = p^2$, то $p \equiv 3\ (4)$ и $P = (p)$. Положим $\chi(P) = -p$.

Лемма. *Предположим, что* $p \equiv 3\ (4)$. *Тогда* $(D/p)_4 = 1$.

Доказательство. Пусть P — простой идеал в $\mathbf{Z}[i]$, порожденный p. Тогда $(D/p)_4 = (D/P)_4 \equiv D^{(NP-1)/4}\ (P)$. Так как $NP = p^2$, то $(NP - 1)/4 = (p^2 - 1)/4 = (p - 1)(p + 1)/4$. В силу малой теоремы Ферма $D^{p-1} \equiv 1\ (p)$, откуда следует, что $(D/p)_4 \equiv 1\ (P)$, а потому $(D/p)_4 = 1$. □

Эта лемма позволяет определить $\chi(P)$ единым образом для всех простых идеалов P, не делящих $2D$. Если $P = (\pi)$ с $\pi \equiv 1\ (2 + 2i)$, то $\chi(P) = \overline{(D/\pi)}_4 \pi$.

Теорема 7. *Пусть E — эллиптическая кривая, определенная уравнением $y^2 = x^3 - Dx$ с $D \in \mathbf{Z}$. Введенный выше характер χ является алгебраическим характером Гекке веса 1 по модулю $(8D)$. Кроме того, $L(E, s) = L(s, \chi)$.*

Доказательство. Предположим сначала, что $p \equiv 3\ (4)$ и $p \nmid 2D$. По теореме 5 имеем $N_p = p + 1$, так что $a_p = 0$. Пусть $P = (p)$. Тогда $NP = p^2$ и $\chi(P) = -p$. Таким образом,

$$1 - a_p p^{-s} + p^{1-2s} = 1 + p^{1-2s} = 1 - \chi(P) NP^{-s}.$$

Предположим теперь, что $p \equiv 1\ (4)$ и $p \nmid 2D$. Запишем $p\mathbf{Z}[i] = P\bar{P}$, $P = (\pi)$ и $\pi \equiv 1\ (2+2i)$. Тогда $NP = p$ и в силу теоремы 5 $a_p = \overline{(D/\pi)}_4\,\pi + (D/\pi)_4\,\bar{\pi}$. Таким образом,

$$1 - a_p p^{-s} + p^{1-2s} = \left(1 - \overline{\left(\frac{D}{\pi}\right)}_4 \pi p^{-s}\right)\left(1 - \left(\frac{D}{\pi}\right)_4 \bar{\pi} p^{-s}\right) =$$

$$= (1 - \chi(P)\,NP^{-s})(1 - \chi(\bar{P})\,N\bar{P}^{-s}).$$

Мы воспользовались тем, что $\overline{(D/\bar{\pi})}_4 = (D/\pi)_4$. Объединяя полученные результаты, получаем

$$L(E, s) = \prod_P (1 - \chi(P)\,NP^{-s})^{-1} = \sum_A \chi(A)\,NA^{-s} = L(s, \chi).$$

Остается показать, что χ — алгебраический характер Гекке веса 1 по модулю $(8D)$.

Для идеала A, взаимно простого с $2D$, очевидно, $\chi(A) = \overline{(D/\alpha)}_4\,\alpha$, где α — однозначно определенный образующий элемент для A с $\alpha \equiv 1\ (2+2i)$. Теорема будет доказана, если мы сможем показать, что из $\alpha \equiv 1\ (8D)$ следует $(D/\alpha)_4 = 1$. Для этого мы рассмотрим отдельно случаи $D \equiv 1\ (4)$, $D \equiv 3\ (4)$ и D четное.

Если $D \equiv 1\ (4)$, то, согласно предложению 9.9.8, $(D/\alpha)_4 = (\alpha/D)_4$. Так как $\alpha \equiv 1\ (D)$, то $(\alpha/D)_4 = 1$ и этот случай разобран.

Прежде чем идти дальше, сделаем одно замечание о $(i/\alpha)_4$. Если $\alpha \equiv 1\ (8)$, то мы утверждаем, что $(i/\alpha)_4 = 1$. Чтобы убедиться в этом, заметим, что $(i/\alpha)_4 = i^{(N\alpha-1)/4}$. Если $\alpha = a + bi \equiv 1\ (8)$, то $a - 1 \equiv 0\ (8)$ и $b \equiv 0\ (8)$. Таким образом, $N\alpha - 1 = a^2 + b^2 - 1 = (a^2 - 1) + b^2 \equiv 0\ (16)$. Тем самым утверждение доказано.

Предположим теперь, что $D \equiv 3\ (4)$. Пусть $\alpha \equiv 1\ (8D)$. Воспользовавшись предложением 9.9.8 и замечанием, сделанным выше, получаем

$$(D/\alpha)_4 = (i^2 D/\alpha)_4 = (-D/\alpha)_4 = (\alpha/D)_4 = 1.$$

Остается рассмотреть случай четного D. Запишем $D = 2^t D_0$, где D_0 нечетно. Пусть $\alpha \equiv 1\ (8D)$. В силу того что было доказано до сих пор, $(D_0/\alpha)_4 = 1$. Таким образом, достаточно показать, что $(2/\alpha)_4 = 1$. Чтобы убедиться в этом, нам нужно получить одно дополнение к биквадратичному закону взаимности. А именно, предположим, что число $\alpha = a + bi$ примарно. Тогда

$$\left(\frac{1+i}{\alpha}\right)_4 = i^{(a-b-b^2-1)/4}.$$

Доказательство этого в случае, когда α — простой элемент, в общих чертах намечено в упражнениях к гл. 9. Нетрудно перейти также от простого α к примарному.

Если $\alpha \equiv 1\ (8D)$ и D четно, то $\alpha \equiv 1\ (16)$. Отсюда получаем $a - 1 \equiv 0\ (16)$ и $b \equiv 0\ (16)$, так что $(1 + i/\alpha)_4 = 1$. Поэтому

$$1 = \left(\frac{1+i}{\alpha}\right)_4^2 = \left(\frac{2i}{\alpha}\right)_4 = \left(\frac{2}{\alpha}\right)_4.$$

Доказательство окончено. □

§ 7. $y^2 = x^3 + D$, глобальный случай

При анализе L-функции эллиптической кривой, определенной уравнением $y^2 = x^3 + D$, $D \in \mathbf{Z}$, мы поступаем так же, как в последнем параграфе. Так как дискриминант Δ в этом случае равен $-2^4 3^3 D^2$, то

$$L(E, s) = \prod_{p \nmid 6D} (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

Числа a_p определяются равенством $N_p = p + 1 - a_p$, а N_p определяется теоремой 4 § 3.

Мы построим некоторый алгебраический характер Гекке χ на $\mathbf{Z}[\omega]$ веса 1 по модулю $(12D)$ и покажем, что $L(E, s) = L(s, \chi)$.

Пусть $P \subset \mathbf{Z}[\omega]$ — простой идеал. Если P делит $6D$, положим $\chi(P) = 0$. Предположим теперь, что $P \nmid 6D$. Если $NP = p$, то $p \equiv 1\ (3)$ и $P = (\pi)$ с примарным π, т. е. $\pi \equiv 2\ (3)$. Полагаем $\chi(P) = -\overline{(4D/\pi)_6}\,\pi$. Если $NP = p^2$, то $p \equiv 2\ (3)$ и $P = (p)$. Пусть $\chi(P) = -p$.

Лемма 1. *Предположим, что p — нечетное простое число и $p \equiv 2\ (3)$. Тогда $(4D/p)_6 = 1$.*

Доказательство. Из предположения следует, что $p + 1$ делится на 6. Как мы знаем, $(4D)^{p-1} \equiv 1\ (p)$. Возводя обе части этого сравнения в степень $(p+1)/6$, получаем результат. □

Лемма 1 позволяет дать определение $\chi(P)$ единым образом. Если $P \nmid 6D$, то запишем $P = (\pi)$, где $\pi \equiv 2\ (3)$. Тогда $\chi(P) = -\overline{(4D/\pi)_6}\,\pi$.

Лемма 2. *Предположим, что $\alpha \in \mathbf{Z}[\omega]$ и $(\alpha, 2D) = (1)$. Определим $(D/\alpha)_2$ как $(D/\alpha)_6^3$. Тогда $(D/\alpha)_2 = (D/N\alpha)$, где последний символ есть символ Якоби (см. гл. 5, § 2).*

Доказательство. Оба символа $(D/\alpha)_2$ и $(D/N\alpha)$ мультипликативны по α. Поэтому достаточно проверить равенство символов для случая, когда $\alpha = \pi$ — простой элемент.

Предположим, что $\pi = p \neq 2$ — рациональное простое число, причем $p \equiv 2\ (3)$. Тогда $Np = p^2$, так что $(D/Np) = (D/p)^2 = 1$.

С другой стороны,

$$\left(\frac{D}{p}\right)_2 = \left(\frac{D}{p}\right)_6^3 \equiv D^{(p^2-1)/2}\ (p) \equiv (D^{p-1})^{(p+1)/2}\ (p) \equiv 1\ (p).$$

Поэтому $(D/Np) = 1 = (D/p)_2$.

Предположим теперь, что π — комплексное простое число, так что $N\pi = p \equiv 1\ (3)$. Тогда

$$\left(\frac{D}{\pi}\right)_2 = \left(\frac{D}{\pi}\right)_6^3 \equiv D^{(p-1)/2}\ (\pi) \equiv \left(\frac{D}{p}\right)(\pi).$$

Так как $p = N\pi$, отсюда следует, что $(D/\pi)_2 = (D/N\pi)$ и доказательство закончено. □

Теорема 8. *Пусть E — эллиптическая кривая над $\mathbf{Q}$, определенная уравнением $y^2 = x^3 + D$, $D \in \mathbf{Z}$. Введенный выше характер будет алгебраическим характером Гекке веса 1 по модулю $(12D)$. Кроме того, $L(E, s) = L(s, \chi)$.*

Доказательство. Предположим сначала, что $p \equiv 2\ (3)$ и $p \nmid 6D$. По теореме 4 имеем $N_p = p + 1$, так что $a_p = 0$. Пусть $P = (p)$. Тогда P есть простой идеал в $\mathbf{Z}[\omega]$ и $\chi(P) = -p$. Таким образом,

$$1 - a_p p^{-s} + p^{1-2s} = 1 + p^{1-2s} = 1 - \chi(P)\, NP^{-s}.$$

Предположим теперь, что $p \equiv 1\ (3)$ и $p \nmid 6D$. Запишем $p\mathbf{Z}[\omega] = P\bar{P}$, где $P = (\pi)$ и $\pi \equiv 2\ (3)$. Тогда $NP = p$ и по теореме 4 имеем $a_p = -\overline{(4D/\pi)}_6\, \pi - (4D/\pi)_6\, \bar{\pi}$. Таким образом,

$$1 - a_p p^{-s} + p^{1-2s} = \left(1 + \left(\overline{\frac{4D}{\pi}}\right)_6 \pi p^{-s}\right)\left(1 + \left(\frac{4D}{\pi}\right)_6 \bar{\pi} p^{-s}\right) =$$

$$= (1 - \chi(P)\, NP^{-s})(1 - \chi(\bar{P})\, N\bar{P}^{-s}).$$

Мы воспользуемся тем, что $\overline{(4D/\bar{\pi})}_6 = (4D/\pi)_6$. Собирая все это вместе, получаем

$$L(E, s) = \prod_P (1 - \chi(P)\, NP^{-s})^{-1} = \sum_A \chi(A)\, NA^{-s} = L(s, \chi).$$

Остается показать, что χ будет алгебраическим характером Гекке веса 1 по модулю $(12D)$.

Очевидно, что для A, взаимно простого с $12D$, $\chi(A) = \overline{(4D/\alpha)}_6\, \alpha$, где α — однозначно определенный образующий идеала A, для которого $\alpha \equiv 1\ (3)$. Все, что нам нужно, это показать, что из $\alpha \equiv 1\ (12D)$ следует $(4D/\alpha)_6 = 1$.

Так как $1 = (4D/\alpha)_6\, (4D/\alpha)_6^2\, (4D/\alpha)_6^3$, достаточно показать, что из $\alpha \equiv 1\ (12D)$ следует $(4D/\alpha)_3 = 1$ и что в силу леммы 2 $(4D/N\alpha) = 1$. Эти два равенства мы и докажем поочередно.

Предположим, что $3 \nmid D$. Так как $\alpha \equiv 1\ (3)$ и α взаимно просто с $4D$, то в силу кубического закона взаимности (теорема 1 гл. 9) $(4D/\alpha)_3 = (-\alpha/4D)_3 = (\alpha/4D)_3 = 1$. Последнее равенство следует из сравнения $\alpha \equiv 1\ (4D)$.

Если $3 \mid D$, запишем $D = 3^t D_0$ с $3 \nmid D_0$. Тогда $(4D/\alpha)_3 = (3/\alpha)_3^t (4D_0/\alpha)_3 = (3/\alpha)_3^t$. Мы должны показать, что из $\alpha \equiv 1\ (12D)$ и $3 \mid D$ следует равенство $(3/\alpha)_3 = 1$. Из предположения имеем $\alpha \equiv 1\ (9)$. Нам нужны дополнения к кубическому закону взаимности, которые могут быть сформулированы следующим образом. Если $\gamma \in \mathbf{Z}[\omega]$ примарно, то $\gamma = a + b\omega \equiv 2\ (3)$. Положим $a = 3m - 1$ и $b = 3n$. Тогда

$$\left(\frac{\omega}{\gamma}\right)_3 = \omega^{m+n} \quad \text{и} \quad \left(\frac{1-\omega}{\gamma}\right)_3 = \omega^{2m}.$$

Набросок доказательства имеется в упражнениях к гл. 9. Далее, $3 = -\omega^2 (1-\omega)^2$, так что из $\alpha \equiv 1\ (9)$ следует равенство $(3/\alpha)_3 = 1$, что и было нужно.

Остается показать, что из $\alpha \equiv 1\ (12D)$ следует равенство $(4D/N\alpha) = 1$. Но из $\alpha \equiv 1\ (12D)$ получаем $N\alpha \equiv 1\ (4)$ и $N\alpha \equiv 1\ (D)$. Если D нечетно, то

$$\left(\frac{4D}{N\alpha}\right) = \left(\frac{D}{N\alpha}\right) = \left(\frac{N\alpha}{D}\right) = 1.$$

Мы воспользовались квадратичным законом взаимности. Если D четно, запишем $D = 2^t D_0$ с нечетным D_0. Тогда

$$\left(\frac{4D}{N\alpha}\right) = \left(\frac{2}{N\alpha}\right)^t \left(\frac{D_0}{N\alpha}\right) = \left(\frac{2}{N\alpha}\right)^t.$$

Последнее, что осталось доказать: из четности D и сравнения $\alpha \equiv 1\ (12D)$ следует равенство $(2/N\alpha) = 1$. Из предположения вытекает, что $\alpha \equiv 1\ (8)$, так что $N\alpha \equiv 1\ (8)$, а потому $(2/N\alpha) = 1$. □

Мы закончим замечанием, что теоремы 6, 7 и 8 показывают, что для эллиптических кривых E вида $y^2 = x^3 - Dx$ или $y^2 = x^3 + D$ L-функция $L(E, s)$ может быть аналитически продолжена на всю плоскость $\mathbf{C}$. Это доказывает гипотезу Хассе для этих кривых!

§ 8. Заключительные замечания

В этой главе мы рассмотрели частные типы эллиптических кривых, определенных над $\mathbf{Q}$, и исследовали их локальные и глобальные дзета-функции. Эти рассмотрения можно перенести на алгебраические многообразия, определенные над полями алгебраических чисел. Мы пройдем немного по этому пути, рассмотрев кривые, определенные многочленом с коэффициентами

в некотором поле алгебраических чисел. После приведения соответствующих определений мы исследуем кривые Ферма $x_0^l + x_1^l + x_2^l = 0$, l — нечетное простое число. В связи с этим мы познакомимся с одним классом алгебраических характеров Гекке, определенных суммами Якоби.

Пусть K — *поле алгебраических чисел* и $\mathcal{O} \subset K$ — *кольцо* его целых чисел. Пусть $f(x_0, x_1, x_2) \in \mathcal{O}[x_0, x_1, x_2]$ — неособый однородный многочлен положительной степени и C обозначает алгебраическую кривую, определенную уравнением $f(x_0, x_1, x_2) = 0$. Если P — простой идеал в $\mathcal{O}$, то можно редуцировать коэффициенты f *по модулю* P *и получить многочлен* $\bar{f} \in \mathcal{O}/P[x_0, x_1, x_2]$. Можно показать, что существует такое конечное множество простых идеалов $\mathcal{P}$, что для $P \notin \mathcal{P}$ редуцированный многочлен $\bar{f}$ будет неособым. Пусть C_P — кривая, определенная над $\mathcal{O}/P$ уравнением $\bar{f}(x_0, x_1, x_2) = 0$. В § 1 гл. 11 было показано, как кривой C_P *поставить в соответствие некоторую дзета-функцию.* А именно,

$$Z(C_P, u) = \exp \sum_{m=1}^{\infty} \frac{N_m(P)\, u^m}{m},$$

где $N_m(P)$ — число (*проективных*) решений уравнения $\bar{f}(x_0, x_1, x_2) = 0$ в расширении поля $\mathcal{O}/P$ степени m. Напомним, что это расширение единственно с точностью до изоморфизма, так что $N_m(P)$ определено корректно.

Используя теорему Римана — Роха, можно показать, что существует такой многочлен $H(C_P, u) \in \mathbf{Z}[u]$ со свободным членом 1, что

$$Z(C_P, u) = \frac{H(C_P, u)}{(1-u)(1-NPu)}. \tag{i}$$

При $P \in \mathcal{P}$ не так легко выбрать подходящее определение. Для наших целей мы просто полагаем $H(C_P, u) = 1$ при $P \in \mathcal{P}$.

Локальная дзета-функция кривой C в P получается, если в равенстве (i) положить $u = NP^{-s}$. А именно,

$$\zeta(C_P, s) = \frac{H(C_P, NP^{-s})}{(1-NP^{-s})(1-NP^{1-s})}. \tag{ii}$$

Это обобщает равенство (ix) § 2.

Глобальная дзета-функция кривой C определяется как

$$\zeta(C, s) = \prod_P \zeta(C_P, s). \tag{iii}$$

Произведение берется по всем ненулевым простым идеалам в $\mathcal{O}$.

Произведение $\prod_P (1 - NP^{-s})^{-1}$ называется *дзета-функцией поля* K и обозначается через $\zeta_K(s)$. Впервые эта функция иссле-

довалась Дедекиндом. Это произведение сходится при $\operatorname{Re}(s) > 1$ и, как показал Гекке, оно может быть продолжено до мероморфной функции на всей плоскости $\mathbf{C}$ и удовлетворяет некоторому функциональному уравнению. Единственный простой полюс имеется при $s = 1$.

Положим $L(C_P, s) = H(C_P, NP^{-s})^{-1}$ и $L(C, s) = \prod_P L(C_P, s)$. Тогда из равенств (ii) и (iii) получаем

$$\zeta(C, s) = \frac{\zeta_K(s)\,\zeta_K(s-1)}{L(C, s)}. \qquad \text{(iv)}$$

Отсюда видно, что если мы хотим исследовать, может ли $\zeta(C, s)$ быть аналитически продолжена на всю плоскость $\mathbf{C}$, достаточно рассмотреть $L(C, s)$.

Фиксируем некоторое нечетное простое число l. Начиная с этого места, мы будем рассматривать кривую C, определенную уравнением $x_0^l + x_1^l + x_2^l = 0$. Будет удобно считать кривую C определенной над полем $K = \mathbf{Q}(\zeta_l)$, а не над $\mathbf{Q}$. Пусть $\mathcal{O} = \mathbf{Z}[\zeta_l]$ — кольцо целых чисел в K.

Нетрудно убедиться в том, что исключительное множество $\mathcal{S}$ в этом случае состоит из единственного идеала $\mathcal{L} = (1 - \zeta_l)$. Если $P \neq \mathcal{L}$, то мы знаем, что l делит $NP - 1$. Именно этот факт делает K более удобным полем определения.

Предполагая, что $P \neq (1 - \zeta_l)$, применим теорему 2 § 3 гл. 11 к кривой C_P над $\mathcal{O}/P$. Имеем

$$H(C_P, u) = \prod_{\chi_0, \chi_1, \chi_2} (1 + NP^{-1} g(\chi_0)\, g(\chi_1)\, g(\chi_2)\, u), \qquad \text{(v)}$$

где произведение берется по таким тройкам характеров кольца $(\mathcal{O}/P)^*$ порядка l, что $\chi_0\chi_1\chi_2 = \varepsilon$ — тривиальный характер.

Так как $g(\chi_1)\, g(\chi_2) = J(\chi_1, \chi_2)\, g(\chi_1\chi_2)$ и $\chi_0\chi_1\chi_2 = \varepsilon$, то $g(\chi_0)\, g(\chi_1)\, g(\chi_2) = \chi_1\chi_2(-1)\, NPJ(\chi_1, \chi_2)$. Поскольку $-1 = (-1)^l$, то $\chi_1\chi_2(-1) = 1$. Подставляя полученные значения в (v), получаем

$$H(C_P, u) = \prod_{\chi_1, \chi_2} (1 + J(\chi_1, \chi_2)\, u), \qquad \text{(vi)}$$

где произведение берется по парам характеров порядка l с $\chi_1\chi_2 \neq \varepsilon$.

Пусть $\chi_P(\alpha) = (\alpha/P)_l^{-1}$ для $\alpha \in \mathcal{O}$. Это есть обратная величина к символу l-степенного вычета (см. гл. 14, § 2). Для $1 \leqslant a, b \leqslant l - 1$ и $a + b \neq l$ положим $\lambda_{a,b}(P) = -J(\chi_P^a, \chi_P^b)$. В этих обозначениях

$$H(C_P, u) = \prod_{\substack{a,\ b=1 \\ a+b \neq l}}^{l-1} (1 - \lambda_{a,b}(P)\, u), \qquad \text{(vii)}$$

так что

$$L(C_P, s) = \prod_{\substack{a,\ b=1 \\ a+b\neq l}}^{l-1} (1 - \lambda_{a\,b}(P)\, NP^{-s})^{-1}. \qquad \text{(viii)}$$

Определим $\lambda_{a,\,b}(\mathscr{L}) = 0$ и $L(s, \lambda_{a,b}) = \prod_P (1 - \lambda_{a,\,b}(P)\, NP^{-s})^{-1}$. Как мы показали,

$$L(C, s) = \prod_{\substack{a,\ b=1 \\ a+b\neq l}}^{l-1} L(s, \lambda_{a,\,b}).$$

В этом месте разумно выразить надежду, что $\lambda_{a,\,b}$ продолжается до алгебраического характера Гекке. На самом деле так оно и есть! $\lambda_{a,\,b}$ является алгебраическим характером Гекке веса 1 по модулю (l^3). Соответствующий элемент из группового кольца равен

$$\sum_{t=1}^{l-1} \left(\left\langle \frac{at}{l} \right\rangle + \left\langle \frac{bt}{l} \right\rangle - \left\langle \frac{(a+b)\,t}{l} \right\rangle \right) \sigma_t^{-1}.$$

Доказательство этих фактов будет намечено в упражнениях. Здесь мы лишь отметим, что, так как $L(C, s)$ является произведением L-функций Гекке, фундаментальный результат Гекке, теорема 6, показывает, что $L(C, s)$ может быть аналитически продолжена до целой функции на всей плоскости $\mathbf{C}$ и, более того, удовлетворяет некоторому функциональному уравнению, которое связывает $L(C, s)$ с $L(C, 2 - s)$.

Замечания

Понятие локальной и глобальной дзета-функций, соответствующих некоторой алгебраической кривой над полем алгебраических чисел, было введено Хассе. В конце 30-х годов Хассе предложил одному из своих студентов показать, что глобальная дзета-функция может быть аналитически продолжена на всю плоскость $\mathbf{C}$ и удовлетворяет некоторому функциональному уравнению. Де Рам попросил Вейля высказать свое мнение об этой проблеме. В то время Вейль не видел причин, почему глобальная дзета-функция должна обладать свойствами, которые ей приписал Хассе. Более того, он считал эту проблему слишком трудной для начинающего. По этому вопросу и по поводу других разъясняющих комментариев см. [241], т. II, с. 529—530.

Несмотря на первоначальный пессимизм, в ходе работы с частными случаями, сначала с кривой $y^2 = x^4 + 1$ (она эквивалентна кривой $y^2 = x^3 - x/4$) у Вейля возникло доверие к гипо-

тезе Хассе. Кульминацией его исследований по этим вопросам стала его знаменитая статья [81]. В ней Вейль рассматривает кривые вида $y^e = \gamma x^f + \delta$, где $2 \leqslant e \leqslant f$ и $\gamma\delta \neq 0$. В конце статьи он отмечает, что случаи $e = 2$ и $f = 3$ или 4 соответствуют эллиптическим кривым с комплексным умножением. По существу, это кривые, которые мы рассматривали в настоящей главе. Он пишет: «...было бы очень интересно исследовать с той же самой точки зрения более общие эллиптические кривые с комплексным умножением». Это предложение было с полным успехом реализовано Дойрингом.

Между прочим, стоит заметить, что то, что мы называли характерами Гекке, сам Гекке называл «Grössencharaktere». В старой литературе алгебраические характеры Гекке назывались характерами типа A_0.

В своей статье 1954 г. ([241], т. II, с. 550—558) (см. также [6*]. — *Ред.*) Вейль определяет локальную и глобальную дзета-функции для неособого алгебраического многообразия над полем алгебраических чисел. Он ставит вопрос о том, могут ли эти функции быть аналитически продолжены на всю плоскость $\mathbf{C}$ и удовлетворяют ли они функциональному уравнению подходящего типа. Проверив, что эти свойства выполняются для многих примеров, он пишет: «Очень соблазнительно предположить, что это всегда так, но я мало надеюсь на скорое доказательство этого». Гипотеза эта известна теперь как гипотеза Хассе — Вейля. Несмотря на то, что в этом направлении имеется большой прогресс, которым мы обязаны самому Вейлю, Танияме, Шимуре и другим, гипотеза Хассе — Вейля все еще остается открытой.

Обстоятельный обзор по поводу различных дзета- и L-функций, которые были определены и изучались начиная с XIX в., см. в статье о дзета-функциях в «Encyclopedic Dictionary of Mathematics» (v. II, sec. 436, M. I. T. Press, 1977).

Упражнения

1. Пусть p — простое число $p \equiv 2$ (3), и рассмотрим кривую E_p, определенную над $\mathbf{F}_p$ уравнением $y^2 = x^3 + a$, $a \in \mathbf{F}_p$. Показать, что $N(y^2 = x^3 + a) = p + 1$ (число проективных точек).

2. Пусть $K \subset \mathbf{C}$ — нормальное CM-поле и j — ограничение на K комплексного сопряжения. Показать, что подполе инвариантных элементов относительно j является единственным вполне вещественным подполем в K степени $[K : \mathbf{Q}]/2$ и $j\sigma = \sigma j$ для всех σ в группе Галуа поля K над $\mathbf{Q}$.

3. Пусть $A, B \in \mathbf{Z}$, $\Delta = 16(4A^3 - 27B^2) \neq 0$ и E — эллиптическая кривая, определенная уравнением $y^2 = x^3 - Ax - B$. Если p — простое число и $p \nmid \Delta$, то пусть N_p обозначает число проективных точек на редуцированной кривой E_p над $\mathbf{F}_p$. Простое число p называется *аномальным для* E, если

$$\sum_{x=0}^{p-1} ((x^3 - Ax - B)/p) \equiv -1 \ (p).$$

Положим

$$f_p = -\sum_{x=0}^{p-1} ((x^3 - Ax - B)/p).$$

Показать, что

(a) p аномально для E тогда и только тогда, когда $p \mid N_p$.

(b) Предположим, что для E_p выполняется гипотеза Римана (см. гл. 11, § 3). Если $p > 5$, то

$$f_p = 1 \Longleftrightarrow p \text{ аномально для } E.$$

(c) Пусть $B = 0$, $p \equiv 1$ (4) и $p \nmid \Delta$. Тогда f_p четно. Если $p > 5$, то p не аномально.

(d) Если $B = 0$, то

$$5 \text{ аномально} \Longleftrightarrow A \equiv 2 \text{ (5)}.$$

Это упражнение взято из [202].

4. Рассмотрим абелеву группу рациональных точек на эллиптической кривой E, определенной уравнением $y^2 = x^3 + c$. Если $p \nmid 6c$, то известно, что подгруппа кручения (т. е. точек конечного порядка) кривой E изоморфна подгруппе группы кручения кривой E, редуцированной по модулю p. Воспользоваться упр. 1 и теоремой Дирихле о плотности простых чисел в арифметической прогрессии для доказательства того, что подгруппа кручения определенной выше кривой может иметь лишь 1, 2, 3, 4 или 6 элементов. Это упражнение взято из [201].

В следующих упражнениях используются обозначения из гл. 14, § 3. Кроме того, $G = \mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z}$ и T обозначает подмножество в G, состоящее из (a, b), где $a \neq 0$, $b \neq 0$, $a + b \neq 0$.

5. Обобщить упр. 13 из гл. 6 следующим образом. Если $x = (x_1, x_2)$, $y = (y_1, y_2) \in G$, то пусть $\langle x, y \rangle = x_1 y_1 + x_2 y_2$. Для $\mathbf{C}$-значного отображения f, определенного на G, положим $\hat{f}(x) = (1/m^2) \sum_y f(y)\, \zeta_m^{-\langle x, y \rangle}$, $y \in G$. Показать, что

(a) $f(x) = \sum_y \hat{f}(y)\, \zeta_m^{\langle x, y \rangle}$.

(b) $\sum_x |\hat{f}(x)|^2 = (1/m^2) \sum_x |f(x)|^2$.

(c) Предположим, что f отображает G в единичную окружность и $\hat{f}$ принимает целые значения. Показать, что $f(x, y) = f(0, 0)\, \zeta_m^{ax+by}$ для подходящего элемента (a, b). Получить отсюда, что если $f(0, 0) = f(1, 0) = f(0, 1) = 1$, то f тождественно равна 1.

6. Пусть $(a, b) \in G$, $P \subset D_m$ — некоторый простой идеал и $m \notin P$. Определим $\lambda_{a,b}(P)$ следующим образом:

(i) если $(a, b) \in T$, то $\lambda_{a,b}(P) = -J(\chi_P^a, \chi_P^b)$;

(ii) если $(a, b) \neq (0, 0)$, $a + b = 0$, то положим $\lambda_{a,b}(P) = +\chi_P^a(-1)$;

(iii) если $a + b \neq 0$ и $a = 0$ или $b = 0$, то положим $\lambda_{a,b}(P) = 1$;

(iv) $\lambda_{0,0}(P) = -(N(P) - 2)$.

Показать, что если изменить соглашение гл. 8, касающееся тривиальных характеров, положив $\varepsilon(0) = 0$, то $\lambda_{a,b}(P) = -J(\chi_P^a, \chi_P^b)$ для всех $(a, b) \in G$.

7. Для $(c, d) \in G$ определим $N_{c,d}$ как число решений (x, y), $x, y \in \mathbf{F}_q$ ($q = N(P)$) уравнений $x + y = 1$, $\chi_P(y) = \zeta_m^d$ и $\chi_P(x) = \zeta_m^c$. Показать, что $J(\chi_P^a, \chi_P^b) = \sum_{c,d} N_{c,d} \zeta_m^{ac+bd}$. Получить отсюда, что $-N_{c,d} = \hat{\lambda}_{c,d}(P)$.

8. Продолжить $\lambda_{a,b}(P)$ по мультипликативности на все идеалы $\mathfrak{A} \subset D_m$, $m \notin \mathfrak{A}$. Показать, что

(a) $\lambda_{0,0}(\mathfrak{A})\, N(\mathfrak{A}) \equiv 1 \ (m^2)$;

(b) если $\alpha \in D_m$, $\alpha \neq 0$, $(a, b) \in T$, то $\lambda_{a,b}((\alpha)) = u(a, b)\, \alpha^{\nu(a,b)}$, где $u(a, b) \in D_m$, $|u(a, b)| = 1$ и

$$\nu(a, b) = \sum_{(i, m)=1} \left(\left\langle \frac{at}{m} \right\rangle + \left\langle \frac{bt}{m} \right\rangle - \left\langle \frac{(a+b)t}{m} \right\rangle \right) \sigma_t^{-1};$$

(c) $\hat{\lambda}_{a,b}(\mathfrak{A}) \in \mathbf{Z}$.

9. Предположим, что $\alpha \equiv 1 \ (m^2)$. Определим $u(a, b)$ для фиксированного α согласно упр. 8, если $(a, b) \in T$. Если $(a, b) \notin T$, $(a, b) \neq (0, 0)$, то положим $u(a, b) = \lambda_{a,b}((\alpha))$ и $u(0, 0) = 1$. Показать, что

(a) $u(a, b) \equiv \lambda_{a,b}((\alpha)) \ (m^2)$ для всех $(a, b) \in G$;

(b) $\hat{u}(a, b) \in D_m$ для всех $(a, b) \in G$;

(c) $\hat{u}(a, b) \in \mathbf{Z}$ для всех $(a, b) \in G$;

(d) применить п. (c) упр. 5 для доказательства того, что $u(a, b) = 1$ при всех $(a, b) \in G$ и получить отсюда, что $\lambda_{a,b}$ является алгебраическим характером Гекке для D_m с определяющим модулем m^2.

Упражнения 5—9 заимствованы из [171], гл. 1, § 4.

10. Привести пример неабелева CM-поля.

УКАЗАНИЯ К ОТДЕЛЬНЫМ УПРАЖНЕНИЯМ

Глава 1

6. Воспользоваться упр. 4.

8. Проделать его для случая $d = 1$, а затем для общего случая воспользоваться упр. 7.

9. Воспользоваться упр. 4.

15. Возможно обобщение: a будет n-й степенью тогда и только тогда, когда $n \mid \operatorname{ord}_p a$ для всех p.

16. Воспользоваться упр. 15.

17. Воспользовавшись упр. 15, показать, что из $a^2 = 2b^2$ следует, что 2 будет квадратом некоторого целого числа.

23. Начать с представления $4\,(a/2)^2 = (c - b)\,(c + b)$.

28. Показать, что $n^5 - n$ делится на 2, 3 и 5. Затем воспользоваться упр. 9.

30. Пусть s — наибольшее целое число, для которого $2^s \leqslant n$, и рассмотрим $\sum_{k=1}^{n} 2^{s-1}/k$. Показать, что эта сумма может быть записана в виде $a/b + 1/2$ с нечетным b. Затем воспользоваться упр. 29.

31. $2 = (1 + i)\,(1 - i) = -i\,(1 + i)^2$.

34. Так как $\omega^2 = -1 - \omega$, то $(1 - \omega)^2 = 1 - 2\omega + \omega^2 = -3\omega$, так что $3 = -\omega^2\,(1 - \omega)^2$.

Глава 2

1. Нужно следовать классическому доказательству Евклида.

2. Воспользоваться тем, что $\operatorname{ord}_p (a + b) \geqslant \min (\operatorname{ord}_p a,\ \operatorname{ord}_p b)$.

3. Если бы $p_1, p_2, \ldots, p_t$ были всеми простыми числами, то выполнялось бы равенство $\varphi\,(p_1 p_2 \ldots p_t) = 1$. Воспользовавшись теперь формулой для φ, получить противоречие.

5. Рассмотреть последовательность $2^2 + 1,\ 2^4 + 1,\ 2^8 + 1, \ldots$. Согласно предыдущему упражнению, никакое простое число не может делить два члена этой последовательности.

6. Прямой счет! Рассмотреть множество пар (s, t) с $p^s t \leqslant n$.

12. Во всех случаях слагаемые мультипликативны. Поэтому следует сначала произвести вычисления для степеней простых чисел и воспользоваться затем мультипликативностью.

17. Воспользоваться формулой для $\sigma\,(n)$.

20. Если $d \mid n$, то n/d также делит n.

22. Если $(t, n) = 1$, то $(n - t, n) = 1$, а потому можно так выделить пары взаимно простых с n чисел, что они будут давать в сумме n.

Глава 3

1. Предположить, что $p_1, p_2, \ldots, p_t$ все сравнимы с -1 по модулю 6. Рассмотреть $N = 6p_1 p_2 \ldots p_t - 1$.

3. 10^k сравнимо с 1 по модулю 3 и 9 и сравнимо с $(-1)^k$ по модулю 11.

5. Если решение существует, то $x^3 \equiv 2\ (7)$ имеет решение. Показать, что последнее сравнение не имеет решения.

10. Если n не равно степени простого числа, записать $n = ab$ с $(a, b) = 1$. Если $n = p^s$ с $s > 2$, то $(n-1)!$ делится на $p \cdot p^{s-1} = p^s = n$. Если $n = p^2$ и $p \neq 2$, то $(n-1)!$ делится на $p \cdot 2p = 2n$.

13. По индукции показать, что $n^p \equiv n\ (p)$ для всех n. Если $(n, p) = 1$, то можно сократить n и получить формулу Ферма.

17. Пусть x_i — решение сравнения $f(x) \equiv 0 \left(p_i^{a_i}\right)$; решить систему $x \equiv x_i \left(p_i^{a_i}\right)$.

23. Так как $i \equiv -1\ (1+i)$, то $a + bi \equiv a - b\,(1+i)$. Записать $a - b = 2c + d$, где $d = 0$ или 1. Тогда $a + bi \equiv d\,(1+i)$.

25. Записав $\alpha = 1 + \beta\lambda$, возведя в куб обе части этого равенства и перейдя к сравнению по модулю λ^4, получить, что $\alpha^3 \equiv 1 + (\beta^3 - \omega^2\beta)\,\lambda^3\ (\lambda^4)$. Затем показать, что член в скобках делится на λ.

Глава 4

4. Если $(-a)^n \equiv 1$ и n четно, то $p - 1 \mid n$. Если n нечетно, то $p - 1 \mid 2n$, откуда следует, что $2 \mid n$ (противоречие).

6. Упражнение не совсем простое. Если 3 — не примитивный элемент, то показать, что 3 сравнимо с квадратом. С помощью упражнения 4 показать, что существует такое целое число a, что $-3 \equiv a^2\ (p)$. Решить теперь сравнение $2u \equiv -1 + a\ (p)$ и показать, что u имеет порядок 3. Это означает, что $p \equiv 1\ (3)$, а это не так.

7. Воспользоваться тем фактом, что 2 не является квадратом по модулю p.

9. См. упр. 22 из гл. 2; воспользоваться тем, что $g^{(p-1)/2} \equiv -1\ (p)$ для примитивного корня g.

11. Представить числа между 1 и $p - 1$ в виде степеней примитивного корня и воспользоваться формулой для суммы геометрической прогрессии.

14. Если $(ab)^s = e$, то $a^{ns} = 1$, откуда следует, что $m \mid ns$. Таким образом, $m \mid s$. Аналогично $n \mid s$. Таким образом, $mn \mid s$.

18. Выбрать некоторый примитивный элемент (например, 2) и построить элементы порядка 7.

22. Сначала показать, что $1 + a + a^2 \equiv 0\ (p)$.

23. Воспользоваться предложением 4.2.1.

Глава 5

3. Воспользоваться тождеством $4\,(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac)$.

9. Используя сравнение $k \equiv -(p-k)\ (p)$, сначала показать, что $2 \cdot 4 \cdot \ldots \cdot (p-1) \equiv (-1)^{(p-1)/2}\ 1 \cdot 3 \cdot 5 \cdot \ldots \cdot (p-2)\ (p)$.

10. Воспользоваться упр. 9.

13. Если $x^4 - x^2 + 1 \equiv 0\ (p)$, то $(2x^2 - 1)^2 \equiv -3\ (p)$ и $(x^2 - 1)^2 \equiv -x^2\ (p)$. При помощи квадратичного закона взаимности получить отсюда, что $p \equiv 1\ (3)$ и $p \equiv 1\ (4)$.

18. Пусть $D = p_1 p_2 \ldots p_m$, и предположим, что n — невычет по модулю p_1. Найти целое число b, для которого $b \equiv 1\ (p_i)$ и $b \equiv n\ (p_1)$ для $1 < i \leqslant m$. Затем воспользовавшись определением символа Якоби, показать, что $(b/D) = -1$.

23. Если p — простое число в $\mathbf{Z}[i]$, то, так как $s^2 + 1 = (s+i)(s-i)$, либо $p \mid s + i$, либо $p \mid s - i$, однако ни одна из этих возможностей не имеет места.

28. Для доказательства (b) заметить, что $a + b$ нечетно, так что из $2p = (a+b)^2 + (a-b)^2$ вытекает, что $(2p/a+b) = 1$. Далее следует воспользоваться свойствами символа Якоби.

29. Случаи $p \equiv 1\ (4)$ и $p \equiv 3\ (4)$ полезно рассмотреть отдельно.

30. Для вычисления написанной суммы воспользоваться тем, что

$$(n(n+1)/p) = ((2n+1)^2 - 1/p).$$

Глава 6

1. Найти уравнение степени 4.

2. Если $a_0\alpha^s + a_1\alpha^{s-1} + \ldots + a_s = 0$, где $a_i \in \mathbf{Z}$, то умножить обе части этого равенства на a_0^{s-1} и убедиться в том, что $a_0\alpha$ — целое алгебраическое число.

3. Предположим, что α и β удовлетворяют приведенным уравнениям с целыми коэффициентами степеней m и n соответственно. Пусть γ — корень уравнения $x^2 + \alpha x + \beta$; показать, что $\mathbf{Z}$-модуль, порожденный $\alpha^i\beta^j\gamma^k$, где $0 \leqslant i < m$, $0 \leqslant j < n$ и $k = 0$ или 1, отображается в себя при умножении на γ.

10. Воспользоваться тем, что $g_a = (a/p)\, g$ и $\sum_a (a/p) = 0$.

11. Напомним, что $1 + (t/p)$ равно числу решений сравнения $x^2 \equiv t\ (p)$ и что $\sum_t \zeta^t = 0$.

13. Воспользоваться упр. 12.

16. Показать, что в противном случае $f'(\alpha) = 0$, и применить предложение 6.1.7.

23. С помощью упр. 4 показать, что достаточно убедиться в том, что $f(x)$ неприводим в $\mathbf{Z}[x]$. Затем записать $f(x) = g(x)\, h(x)$, произвести редукцию по модулю p и воспользоваться тем, что $F_p[x]$ — область с однозначным разложением на множители.

Глава 7

3. Так как $q \equiv 1\ (n)$, существует n решений уравнения $x^n = 1$. Если $\beta^n = \alpha$, то другие решения уравнения $x^n = \alpha$ задаются $\gamma\beta$, где γ пробегает решения уравнения $x^n = 1$.

5. $q^n - 1 = (q-1)\left(q^{n-1} + \cdots + q + 1\right)$. Так как $q \equiv 1\ (n)$, то $q^{n-1} + \ldots + q + 1 \equiv n\ (n) \equiv 0\ (n)$. Таким образом, $n(q-1)$ делит $q^n - 1$.

7. Пусть $m = [K : F]$. Элемент α является квадратом в K в том и только том случае, когда $\alpha^{(q^m-1)/2} = 1$. Если α — не квадрат в F, то $\alpha^{(q-1)/2} = -1$. Показать, что $\alpha^{(q^m-1)/2} = (-1)^m$. Эта формула и приводит к нужному результату.

9. Воспользоваться методом упр. 7.

14. Это можно доказать точно так же, как и для F_p. Предположим, что $q = p^m$. Пусть $f(x) \in F_p[x]$ неприводим и степени mn и $g(x)$ — неприводимый делитель многочлена $f(x)$ в $F_q[x]$. Пусть α — корень многочлена $g(x)$; показать, что $F_q \subset F_p(\alpha)$. Сделать отсюда вывод о том, что $F_q(\alpha) = F_p(\alpha)$ и что $[F_q(\alpha) : F_q] = n$. Отсюда следует, что $g(x)$ имеет степень n.

15. Если $x^n - 1$ разлагается на линейные множители в E, где $[E : F] = f$, то E имеет q^f элементов и $n \mid q^f - 1$, так как корни многочлена $x^n - 1$ образуют подгруппу в E^* порядка n.

23. Если β — какой-либо корень многочлена $x^p - x - \alpha$, то его корнями будут и $\beta + 1, \beta + 2, \ldots, \beta + (p-1)$. Воспользовавшись этим, можно доказать утверждение о неприводимости. Для доказательства последнего утверждения заметим, что из $\beta^p = \beta + \alpha$ следует $\beta^{p^2} = \beta^p + \alpha^p = \beta + \alpha + \alpha^p$ и т. д. Таким образом, $\beta^{p^n} = \beta + \mathrm{tr}(\alpha)$, а потому $\beta \in F$ тогда и только тогда, когда $\mathrm{tr}(\alpha) = 0$.

Глава 8

1. Воспользоваться следствием предложения 8.1.3 и предложением 8.1.4.

4. Произвести подстановку $t = (k/2)(u + 1)$ и воспользоваться упр. 3.

6. Получается из упр. 5 вместе с частью (d) теоремы 1 или непосредственно из упр. 4 при помощи подстановки $k = 1$.

8. Воспользовавшись предложением 8.1.5, следовать доказательству упр. 3.
14. Воспользоваться предложением 8.3.3.
19. Показать сначала, что число решений задается формулой $p^{r-1} + J_0(\chi, \chi, \ldots, \chi)$, где χ — характер порядка 2 и в J_0 имеется r компонент. Затем воспользоваться предложением 8.5.1 и теоремой 3. Заметим, в частности, что если r нечетно, то ответом будет просто p^{r-1}.
28. Для (a): записать

$$\sum_{x=1}^{p-1} x\chi(x) = \sum_{x=1}^{(p-1)/2} x\chi(x) + \sum_{x=1}^{(p-1)/2} (p-x)\chi(p-x).$$

Для (b): записать

$$\sum_{x=1}^{p-1} x\chi(x) = \sum_{x=1}^{(p-1)/2} 2x\chi(2x) + \sum_{x=1}^{(p-1)/2} (p-2x)\chi(p-2x).$$

Для (c) и (d): приравнять (a) и (b).

Глава 9

3. Воспользоваться тем, что $N\gamma = a^2 - ab + b^2 \equiv 3(m+n) + 1$ (9).
4. Записать γ в виде $3(m+n) - 1 - 3n\lambda$. Таким образом, $\gamma \equiv 3(m+n) - 1$ (3λ).
5. Напомним, что $3 = -\omega^2\lambda^2$.
7. $2 + 3\omega$, $-7 - 3\omega$ и $-4 - 3\omega$.
10. $D/5D$ имеет 25 элементов. Следовательно, $x^{24} - 1$ полностью разлагается на линейные множители в D.
13. Воспользовавшись упр. 9, показать, что перечисленные элементы представляют все кубы в $D/5D$.
15. Напомним, что каждый элемент в $D/\pi D$ представляется некоторым рациональным целым числом.
19. Воспользоваться упр. 18, кубическим законом взаимности и индукцией по числу примарных простых делителей γ.
23. Пусть $p = \pi\bar{\pi}$, где π примарно. В силу упр. 15 сравнение $x^3 \equiv 3$ (p) разрешимо тогда и только тогда, когда $\chi_\pi(3) = 1$. Согласно упр. 5, $\chi_\pi(3) = \omega^{2n}$, где $\pi = a + b\omega$ и $b = 3n$. Отсюда следует, что сравнение $x^3 \equiv 3$ (p) разрешимо тогда и только тогда, когда $9 \mid b$.
24. (a) Воспользоваться кубическим законом взаимности с $\pi \equiv b\omega$ (a).
(d) Записав $(a+b) = (a+b)\,\omega\cdot\omega^{-1}$, обратить внимание на то, что $a + b\omega \equiv a(1-\omega)$ (π).
25. (a) Воспользовавшись упр. 18 и следствием предложения 9.3.4, показать, что $\chi_{a+b}(b) = 1$. Заметим, что $\pi \equiv -b(1-\omega)(a+b)$.
(b) $\chi_{a+b}(1-\omega) = (\chi_{a+b}(1-\omega)^2)^2 = (\chi_{a+b}(-3\omega))^2$ и т. д.
39. Объединить упр. 6 и 27 гл. 8 с предложением 9.6.1.
40. См. указание к предыдущему упражнению.
43. Воспользоваться упр. 23 из гл. 6.

Глава 10

2. Отобразить $[x_0, x_1, \ldots, x_{n-1}]$ в $[0, x_0, x_1, \ldots, x_{n-1}]$.
3. Так как число точек в $A^n(F)$ равно q^n, разложение $P^n(F)$ показывает, что число точек в $P^n(F)$ равно q^n плюс число точек в $P^{n-1}(F)$. Далее следует применить индукцию.
4. Без ограничения общности можно предположить, что $a_0 \neq 0$. Если $[x_0, x_1, \ldots, x_n]$ — какое-либо решение, то отобразить его в точку $[x_1, x_2, \ldots, x_n]$ из $P^{n-1}(F)$. Показать, что это отображение корректно определено, взаимно однозначно и эпиморфно.

5. Произвести подстановку, избавиться от однородности и воспользоваться тем, что многочлен степени n имеет не больше n корней.

9. k-я частная производная равна $ma_k x_k^{m-1}$. Так как каждый коэффициент a_k отличен от 0 и m взаимно просто с характеристикой, единственный общий нуль для всех частных производных имеет координаты, все равные нулю. Это, однако, не соответствует никакой точке проективного пространства.

12. Приведенное к однородному виду уравнение таково: $t^2x^2 + t^2y^2 + x^2y^2 = 0$. Полагая $t = 0$, убеждаемся в том, что точками на бесконечности будут (0, 0, 1) и (0, 1, 0). Вычисление частных производных и подстановка показывают, что обе эти точки особые.

14. Рассмотреть соответствующее однородное уравнение и вычислить три частные производные. Предположив, что общее решение существует, показать, что $4a^3 + 27b^2 = 0$.

19. След тождественно равен нулю на F_p тогда и только тогда, когда $p \mid n$.

20. Рассмотреть отображение $h(x) = x^p - x$ из F_q в F_q. Доказать, что оно будет гомоморфизмом и что его образ имеет q/p элементов. Доказать также, что образ h содержится в ядре отображения следа. Показать, что в ядре последнего отображения имеется не больше q/p элементов.

21. Подсчитать число таких отображений.

23. Произвести подстановку и вычисление.

Глава 11

4. В F_q существует $2q + 1$ точек на бесконечности и q^2 конечных точек. Поэтому $N_s = 3p^{2s} - p^s - 1$.

7. Число прямых в $P^n(F)$ равно числу плоскостей в $A^{n+1}(F)$, которые проходят через начало координат. Ответом будет $(q^{n+1} - 1)(q^{n+1} - q)(q^2 - 1)^{-1} \cdot (q^2 - q)^{-1}$.

9. Существует одна бесконечно удаленная точка. При $x = 0$ имеется лишь одна точка (0, 0) на кривой. При $x \neq 0$ положить $t = y/x$ и рассмотреть $t^2 = x + 1$. Последнее уравнение имеет $p - 2$ решений с $x \neq 0$. Вместе получается p решений в F_p. Аналогично в F_q имеется q решений. Таким образом, ответом будет $(1 - pu)^{-1}$.

12. Для начала вычислить число решений уравнения $u^2 - v^2 = 4D$.

16. Важные факты: $N_{F_s/F}$ является эпиморфизмом; группа мультипликативных характеров конечного поля циклическая.

18. Воспользоваться соотношением между суммами Гаусса и Якоби и соотношением Хассе—Дэвенпорта.

19. После разложения членов произведения в геометрические прогрессии результат сводится к тому факту, что каждый приведенный многочлен является произведением приведенных неприводимых многочленов, причем последнее представление единственно.

20. Воспользоваться тождеством $1 - T^s = \prod_{k=0}^{s-1} (1 - \zeta^k T)$, где $\zeta = e^{2\pi i/s}$.

Глава 12

7. $21 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$.

9. Записать $\det(\omega_i^{(j)})$ в виде $P - N$, где P — сумма членов, соответствующих четным перестановкам, а N — соответствующая сумма для нечетных перестановок. Затем обратить внимание на то, что $(P - N)^2 = (P + N)^2 - 4PN$. Стандартное рассуждение показывает, что $P + N$ и PN — целые числа.

9. Воспользоваться предложением 12.1.4 и элементарными симметрическими функциями.

14. Рассмотреть $\zeta + \zeta^{-1}$, где ζ — некоторый примитивный корень из единицы степени 7.

21—23. См. часть 2 § 5.

26. Выбрать некоторый примитивный корень g для поля вычетов. Поднять его в D и рассмотреть соответствующий минимальный многочлен над инвариантным подполем для группы разложения (см. [207], с. 223).

Глава 13

1. Показать, что $\varphi(n)$ четно при $n > 2$.

2. Воспользоваться предложением 13.1.3.

3. $\mathbf{Q}(\sqrt{p}) = \mathbf{Q}(\zeta_p)$.

24. Дискриминант квадратичного поля по модулю 4 равен 0 или 1.

27. Порядок σ_p не может быть равен 4. См. теорему 2.

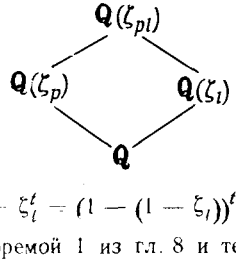
Глава 14

1. (a) Воспользоваться определением $J(\chi, \psi)$, формулой бинома и упр. 11 из гл. 4. См. также лемму 1 из гл. 9.

12. См. упр. 17 (e).

14. Пусть P — некоторый простой идеал, делящий p. Показать, что $(\alpha/P)(\alpha/\overline{P}) = 1$. См. [166], предложение 1034.

17. (b) Исследовать ветвление l в диаграмме



(c) Заметим, что $\zeta_l^{\sigma t} - \zeta_l^t = (1 - (1 - \zeta_l))^t$.

(e) Воспользоваться теоремой 1 из гл. 8 и тем, что $g(\chi_P^t) = g(\chi_P)^{\sigma t}$.

Глава 15

2. Воспользоваться теоремой 3.

3. Воспользоваться теоремой 3 и предложением 15.2.4.

9. Как функция комплексной переменной $(e^t - 1)^{-1}$ аналитична для $|t| < 2\pi$.

13. Воспользоваться упр. 12.

21. Положить $F = 2$ в упр. 19.

Глава 16

4. Для другой оценки отметить, что $\int_0^1 t^{3k}(1-t)\,dt = 1/[(3k+1)(3k+2)]$.

7. Показать, что если $p \nmid m$ и $p \mid \Phi_m(N)$ для некоторого целого числа N, то $p \equiv 1\ (m)$.

11. Для целого числа m выбрать простое число $p \equiv 1\ (m)$ и рассмотреть подполя поля $\mathbf{Q}(\zeta_p)$.

12. Если $p \equiv t\ (m)$, то $p \mid f(\zeta^p) = f(\zeta)^t$, где ζ — примитивный корень степени m из единицы и $f(x) \in \mathbf{Z}[x]$, $f(\zeta) = 0$.

14. Воспользоваться теоремой 1 из гл. 6.

Глава 17

2. $y^2 + 4 = x^3 - 27$.

3. Следовать доказательству предложения 17.8.1 ([60], теорема 121).

8. $(y + 2i)(y - 2i) = x^3$.

12. Рассмотреть $(x_1 + y_1\sqrt{d})^2$ для некоторого решения (x_1, y_1) уравнения $x^2 - dy^2 = -1$.

13. $1^3 + 2^3 + \cdots + n^3 = (n(n+1)/2)^2$.

16. Рассмотреть отображение

$$(x_1, x_2, x_3, x_4) \to \left(\frac{x_1 + x_2}{2}, \frac{x_1 - x_2}{2}, \frac{x_3 + x_4}{2}, \frac{x_3 - x_4}{2}\right).$$

18. $\binom{4}{2} = 6$.

19. См. указание к упр. 16.

Глава 18

4. Если t — порядок подгруппы ветвления для E, то при $p \equiv 2$ (3) имеем $p \equiv -1$ (t). Плотность множества простых чисел $p \equiv -1$ (t) равна $1/\varphi(t)$, в то время как плотность простых чисел $p \equiv 2$ (3) равна $1/2$.

8. (a) Сначала провести доказательство для $\mathfrak{P} = P$, воспользовавшись тем, что $(N(P) - 2)\,N(P) = (N(P) - 1)^2 - 1$.

(b) См. упр. 4 из гл. 14. Для $|u(a, b)| = 1$ применить σ_{-1} (см. лемму 4 § 5 гл. 14).

(c) Показать, что $\hat{u}$ инвариантен при действии подходящей группы Галуа.

12. (a) См. гл. 11.

(b) См. упр. 4.

(c) См. упр. 17.

ЛИТЕРАТУРА

Основная литература

1. Albert A. Fundamental concepts of higher algebra. — Chicago: University of Chicago Press, 1956.

2. Artin E. The collected papers of Emil Artin. — Reading, Mass.: Addison-Wesley, 1965.

3. Ax J. Zeros of polynomials over finite fields. — Amer. J. Math., 1964, v. 86, p. 255—261.

4. Bachman P. Niedere Zahlentheorie, Vol. 1. — Leipzig, 1902, p. 83.

5. Bachman P. Die Lehre von der Kreisteilung. — Leipzig, 1872.

6. Bachman P. Über Gauss' Zahltheoretische Arbeiten. — Gött. Nachr., 1911., p. 455—508.

7. Beck A., Bleicher M. N., Crowe D. W. Excursions into mathematics. — New York: Worth, 1969.

8. Bilharz H. Primdivisor mit vorgegebener Primitivwurzel. — Math. Ann., 1937, B. 114, S. 476—492.

9. Боревич З. И., Шафаревич И. Р. Теория чисел. — М.: Наука, 1985.

10. Carlitz L. The arithmetic of polynomials in a Galois field. — Amer. J. Math., 1932, v. 54, p. 39—50.

11. Carlitz L. Some applications of a theorem of Chevalley. — Duke Math. J., 1951, v. 18, p. 811—819.

12. Carlitz L. Some problems involving primitive roots in a finite field. — Proc. Nat. Acad. Sci. U. S. A., 1952, v. 38, p. 314—318.

13. Carlitz L. Kloosterman sums and finite field extensions. — Acta Arithmetica, 1969, v. 16, p. 179—193.

14. Cartier P. Sur une généralisation des symboles de Legendre—Jacobi. — L'Enseignement Math., 1970, v. 15, p. 31—48.

15. Cassels J. W. S. On Kummer sums. — Proc. London Math. Soc., 1970, v. 21, no. 3, p. 19—27. [Имеется перевод: Математика, 1972, 16 : 1, с. 157—164.]

16. Chevalley C. Démonstration d'une hypothèse de M. Artin. — Abhand. Math. Sem. Hamburg, 1936, v. 11, p. 73—75.

17. Chowla S. The last entry in Gauss' diary. — Proc. Nat. Acad Sci. U. S. A., 1949, v. 35, p. 244—246.

18. Chowla S. The Riemann hypothesis and Hilbert's tenth problem. — New York: Gordon & Breach, 1963.

19. Chowla S. A note on the construction of finite Galois fields $GF(p^n)$. — J. Math. Anal. Appl., 1966, v. 15, p. 53—54.

20. Chowla S. An algebraic proof of the law of quadratic reciprocity. — Norske Vid. Selsk. Forh. (Trondheim), 1966, v. 39, p. 59.

21. Davenport H. On the distribution of quadratic residues mod p. — London Math. Soc. J., 1930—1931, v. 5—6, p. 49—54.

22. Davenport H. The higher arithmetic. — London: Hutchinson, 1968. [Имеется перевод: Дэвенпорт Г. Высшая арифметика. — М.: Наука, 1965.]

23. Davenport H., Hasse H. Die Nullstellen der Kongruenz Zetafunktion in gewissen zyklischen Fällen. — J. Reine und Angew. Math., 1935, B. 172, S. 151—182.

24. Deuring M. The zeta functions of algebraic curves and varieties. — Indian J. Math., 1955, p. 89—101.

25. Dickson L. Linear algebraic groups and an exposition of the Galois field theory. — New York: Dover, 1958.

26. Dwork B. On the rationality of the zeta function. — Amer. J. Math., 1959, v. 82, p. 631—648.

27. Eisenstein G. Beiträge zur Kreisteilung. — J. Reine und Angew. Math., 1844, S. 269—278.

28. Eisenstein G. Beweis des Reciprocitätssatzes für die kubischen Reste. — J. Reine und Angew. Math., 1844, S. 289—310.

29. Eisenstein G. Nachtrag zum kubischen Reciprocitätssatze. — J. Reine und Angew. Math., 1844, B. 28, S. 28—35.

30. Eisenstein G. Beiträge zur Theorie der elliptischen Funktionen. — J. Reine und Angew., 1847, B. 35, S. 135—274.

31. Erdös P. Some recent advances and current problems in number theory. — Lectures in modern mathematics, Vol. 3, New York: Wiley, 1965.

32. Frankel A. Integers and the theory of numbers. — Scripta Math. Studies, 1955, v. 5.

33. Galois E. Oeuvres mathématiques. — Paris: Gauthier-Villars, 1897. [Имеется перевод: Галуа Э. Сочинения. — М. — Л.: ОНТИ. 1936.]

34. Gauss C. F. Arithmetische Untersuchungen. — New York: Chelsea, 1965. [Имеется перевод: Гаусс К. Ф. Труды по теории чисел. — М.: АН СССР, 1959.]

35. Goldstein L. Density questions in algebraic number theory. — Amer. Math. Monthly, April 1971, v. 78, p. 342—351.

36. Graham R. On quadruples of consecutive k-th power residues. — Proc. Amer. Math. Soc., 1964, p. 196—197.

37. Greenberg M. Forms in many variables. — Mento Park, Calif.: W. A. Benjamin, 1969.

38. Hardy G. H. Prime numbers. — Manchester : British Association, 1915, pp. 350—354, and Collected papers, Vol. 2.

39. Hardy G. H. An introduction to the theory of numbers. — Bull. Amer. Math. Soc., 1929, v. 35, p. 778—818.

40. *Hardy G. H., Wright E. M. An introduction to the theory of numbers.* 4th ed. — New. York: Oxford University Press, 1960.

41. Hasse H. Vorlesungen über Zahlentheorie. — Berlin: Springer-Verlag, 1964. [Имеется перевод: Хассе Г. Лекции по теории чисел. — М.: ИЛ, 1953.]

42. Hasse H. The Riemann hypothesis in function fields. — Philadelphia: Pennsylvania State University Press, 1969.

43. Hausner A. On the law of quadratic reciprocity. — Archiv der Math., 1961, v. 12, p. 182—183.

44. Hecke E. Algebraische Zahlentheorie. — Leipzig, 1929. Reprint by Chelsea Publishing Company, Inc., New York. [Имеется перевод: Гекке Э. Лекции по теории алгебраических чисел. — М.—Л.: Гостехиздат. 1940.]

45. Holzer L. Zahlentheorie. — Leipzig: Teubner Verlagsgesellschaft, 1958.

46. Hooley C. On Artin's conjecture. — J. Reine und Angew. Math., 1967, B. 225, S. 209—220.

47. *Jacobi C. Über die Kreisteilung.* — J. *Reine und Angew. Math.*, 1846, S. 254—274.

48. Jacobsthal E. Über die Darstellung der Primzahlen der Form $4n + 1$ als Summe zweier Quadrate. — J. Riene und Angew. Math., 1907, B. 132, S. 238—245.

49. Jordan C. Traité des substitutions. — Paris, 1870.

50. Kornblum H. Über die Primfunktionen in einer Arithmetischen Progression. — Math. Z., 1919, B. 5, S. 100—111.

51. Kummer E. Über die allgemeinen Reciprocitätsgesetz. — Math. Abh. Akad. Wiss. zu Berlin, 1859, S. 19—160.

52. Landau E. Elementary number theory. — 2nd ed., New York: Chelsea, 1966.

53. Lang S. Some theorems and conjectures on diophantine equations. — Bull. Amer. Math. Soc., 1960, v. 66, p. 240—249.

54. Lehmer D. H. A note on primitives. — Scripta Mathematica, 1963, v. 26, p. 117—119.

55. Lehmer E. On the quintic character of 2 and 3. — Duke Math. J., 1951, v. 18, p. 11—18.

56. Lehmer E. Criteria for cubic and quartic residuacity. — Mathematika, 1958, v. 6, p. 20—29.

57. Leonard P. On constructing quartic extensions of $GF(p)$. — Norske Vid. Selsk. Forh. (Trondheim), 1967, v 40, p. 41—52.

58. Mann H. B. Introduction to number theory. — Columbus, Ohio: Ohio State University Press, 1955.

59. Mills W. H. Bounded consecutive residues and related problems. — Proc. Symp. Pure Math., 1965, v. 8.

60. Nagell T. Introduction to number theory. — New York: Wiley, 1951. См. также: Chelsea Publishing Company Inc., New York.

61. Niven I., Zuckerman H. S. An introduction to the theory of numbers. — 2nd ed., New York: Wiley, 1966.

62. Pisot C. Introduction à la théorie des nombres algébriques. — L'Enseignement Math., 1962, v, 8, no. 2, p. 238—251.

63. Pollard H., Diamond H. The theory of algebraic numbers. — New York: Wiley, 1950, 2nd ed., 1975.

64. Rademacher H. Lectures on elementary number theory. — Lexington, Mass.: Xerox College Publishing, 1964.

65. Rademacher H., Toeplitz O. The enjoyment of Mathematics. — Princeton University Press, 1951.

66. Rieger G. Die Zahlentheorie bei C. F. Gauss. — Gauss Gedenkband, Berlin: Haude and Sperner, 1960.

67. Samuel P. Unique factorization. — Amer. Math. Monthly, 1968, v. 75, p. 945—952.

68. Samuel P. Théorie algébrique des nombres. — Paris: Hermann & Cie, 1967.

69. Serr J.-P. Compléments d'arithmétiques, Rédigés par J. P. Ramis et G. Ruget. — Paris: Ecoles Normales Supérieures, 1964. См. также: Springer-Verlag, 1973. [Имеется перевод: Серр. Ж. П. Курс арифметики. — М.: Мир, 1972.]

70. Shanks D. Solved and unsolved problems in number theory. — New York: Spartan Books, 1962.

71. Sierpinski W. A selection of problems in the theory of numbers. — Oxford: Pergamon Press, 1964.

72. Smith H. J. S. Report on the theory of numbers. — 1894. См. также: Chelsea Publishing Company, Inc., New York, 1965.

73. Stark H. An introduction to number theory. — Cambridge, Mass.: M. I. T. Press, 1979.

74. Storer T. Cyclotomy and difference sets. — Chicago: Markham, 1967.

75. Swan R. Factorization of polynomials over finite fields. — Pacific J. Math., 1962, v. 12, p. 1099—1106.

76. Vegh E. Primitive roots modulo a prime as consecutive terms of an arithmetic progression. — J. Reine und Angew. Math., 1969, B. 235, S. 185—188.

77. Виноградов И. М. Основы теории чисел. — М.: Наука, 1981.

78. Warning E. Bemerkung zur vorstehenden Arbeit von Herrn Chevalley. — Agh. Math. Sem. Hamburg, 1936, B. 11, p. 76—83.

79. Waterhouse W. The sign of the Gauss sum. — J. Number Theory, 1970, v. 2, no. 3, p. 363.

80. Weil A. Number of solutions of equations in a finite field. — Bull. Amer. Math. Soc., 1949, B. 55, p. 497—508.

81. Weil A. Jacobi sums as «Grössencharaktere». — Trans. Amer. Math. Soc., 1952, v. 73, p. 487—495.

82. Yamamoto K. On a conjecture of Hasse concerning multiplicative relations of Gauss sums. — J. Combin. Theory, 1966, v. 1, p. 476—489.

83. Yokoyama A. On the Gaussian sum and the Jacobi sum with its applications. — Tohoku Maths. J. (2), 1964, v. 16, p. 142—153.

Дополнительная литература

84. Adams W. W., Goldstein L. J. Introduction to number theory. — Englewood Cliffs, N. J.: Prentice-Hall, 1976.

85. Ahlfors L. Complex analysis. — 2nd ed., New York: McGraw-Hill, 1966.

86. Ankeny N. C., Artin E., Chowla S. The class numbers of real quadratic fields. — Ann. Math. (2), 1952, v. 56, p. 479—493.

87. Arthaud N. On Birch and Swinnerton-Dyer's conjecture for elliptic curves with complex multiplication. — Comp. Math., 1978, v. 37, fasc. 2, p. 209—232.

88. Ayoub R. Euler and zeta function. — Amer. Math. Monthly, 1974, v. 81, p. 1067—1086.

89. Baker A. Transcendental number theory. — Cambridge: Cambridge University Press, 1975.

90. Baker A. On the class number of imaginary quadratic fields. — Bull. Amer. Math. Soc., 1971, v. 77, p. 678—684.

91. Bergmann G. Über Eulers Beweis des grossen Fermatschen Satzes für den Exponenten 3. — Math. Ann., 1966, B. 164, S. 159—175.

92. Berndt B. C. Sums of Gauss, Jacobi and Jacobsthal. — J. Number Theory, 1979, v. 11, p. 349—398.

93. Berndt B. C., Evans R. The determination of Gauss sums. — Bull. Amer. Math. Soc., 1981, v. 5 (2), p. 107—129.

94. Berndt B. C. Classical theorems on quadratic residues. — L'Enseignement Math., 1976, v. 22, fasc. 3—4.

95. Berndt B. C., Evans R. Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer. — Ill. Math., 1979, v. 23, no. 3, p. 374—437.

96. Birch B. J., Swinnerton-Dyer H. P. F. Notes on elliptic curves, I. — J. Reine und Angew. Math., 1963, v. 212, p. 7—25; II, 1965, v. 218, p. 79—108.

97. Birch B. J. Conjectures on elliptic curves. — In: Theory of Numbers. — Amer. Math. Soc., Proc. of Symposium in Pure Math., Vol. 8, Pasadena, 1963.

98. Bombieri E. Counting points on curves over finite fields (d'après S. A. Stepanov). — Sem. Bourbaki, Vol. 1972—73, Exposé 430. Lecture Notes in Mathematics, Vol. 383, p. 234—241. New York: Springer-Verlag, 1974.

99. Brown E. The first proof of the quadratic reciprocity law, revisited. — Amer. Math. Monthly, 1981, v. 88, p. 257—264.

100. Brumer A., Kramer K. The rank of elliptic curves. — Duke Math. J., 1977, v. 44, p. 715—742.

101. Bühler W. K. Gauss. — New York: Springer-Verlag, 1981.

102. Burde K. Ein rationales biquadratisches Reciprozitätsgesetz. — J. Reine und Angew. Math., 1969, B. 235, S. 175—184.

103. Butts H. S., Wade L., Two criteria for Dedekind domains. — Amer. Math. Monthly, 1966, v. 73, p. 14—21.

104. Carlitz L. Arithmetic properties of generalized Bernoulli numbers. — J. Reine und Angew. Math., 1959, B. 201—202, S. 173—182.

105. Carlitz L. A note on irregular primes. — Proc. Amer. Math. Soc., 1954. v. 5, p. 329—331.

106. Carlitz L. A characterization of algebraic number fields with class number two. — Proc. Amer. Math. Soc., 1960. v. 11, p. 391—392.

107. Cassels J. W. S. Arithmetic on an elliptic curve. — Proceedings of the International Congress of Mathematics, Stockholm, 1962, p. 234—246.

108. Cassels J. W. S. On Kummer sums. — Proc. London, Math. Soc. (3), 1970, v. 21, p. 19—27. [Эта ссылка совпадает с [15].]

109. Cassels J. W. S. Diophantine equations with special reference to elliptic curves. — J. London Math. Soc., 1966, v. 41, p. 193—291; [Имеется перевод: Математика, 1968, 12 : 1, с. 113 — 160; 1968, 12 : 2, с. 5—48.]

110. Cassels J. W. S., Fröhlich A. Algebraic number theory. — Proceedings of an International Congress by the London Mathematical Society, 1967. Washington, D. C.: Thompson. [Имеется перевод: Алгебраическая теория чисел. Под ред. Дж. Касселса и А. Фрёлиха. — М.: Мир. 1969.]

111. Châtelet F. Les corps quadratiques. — Monographies de l'Enseignement Mathématique, vol. 9. Genève: 1962.

112. Chandrasekharan K. Introduction to analytic number theory. — New York: Springer-Verlag, 1968. [Имеется перевод: Чандрасекхаран К. Введение в аналитическую теорию чисел. — М.: Мир, 1974.]

113. Chowla S. On Gaussian sums. — Proc. Nat. Acad. Sci. U. S. A., 1962, v. 48, p. 1127—1128.

114. Coates J., Wiles A. On the conjecture of Birch and Swinnerton-Dyer. — Invent. Math., 1977, v. 39, p. 223—251.

115. Cohn H. A second course in number theory. — New York: Wiley, 1962.

116. Collison M. J. The origins of the cubic biquadratic reciprocity laws. — Arch. Hist. Exact Sci., 1977, no. 1, p. 63—69.

117. Czogla A. Arithmetic chracterization of algebraic number fields with small class numbers. — Math. Z., 1981. S. 247—253.

118. Davenport H. The work of K. E. Roth. — Proc. Int. Cong. Math., 1958, LVII—LX. Cambridge: Cambridge University Press, 1960.

119. Davenport H. Multiplicative number theory. — New York: Springer-Verlag, 1980. [Имеется перевод: Дэвенпорт Г. Мультипликативная теория чисел. — М.: Наука, 1971.]

120. Davis D., Shisha O. Simple proofs of the fundamental theorem of arithmetic. — Math. Mag., 1980, v. 54, no. 1, p. 18.

121. Dedekind R. Mathamatische Werke, Vols I and II, New York: Chelsea, 1969.

122. Dirichlet P. G. L. Sur l'équation $t^2 + u^2 + v^2 + w^2 = 4m$. — In: Dirichlet's Werke, Vol. 2, pp. 201—208. — New York: Chelsea, 1969.

123. Dirichlet P. G. L. Beweis des Satzes, dass jede unbegrenzte arithmetische Progression ... . In: Mathematische Werke, pp. 313—342. — New York: Chelsea, 1969.

124. Dirichlet P. G. L. Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres. — In: Dirichlet's Werke, pp. 401—496.— New York: Chelsea, 1969.

125. Dirichlet P. G. L. Werke. 2 vols. in one. — New York: Chelsea, 1969.

126. Dirichlet P. G. L. Sur la manière de résoudre l'équation $t^2 - pu^2 = 1$ au moyen des fonctions circulaires. — In: Dirichlet's Werke, pp. 345—350. New York: Chelsea, 1969.

127. Dirichlet P. G. L. Dedekind, Vorlesungen über Zahlentheorie. — New York: Chelsea, 1968. [Имеется перевод: Дирихле П. Г. Л. Лекции по теории чисел. В обработке и с дополнениями Р. Дедекинда. — М.—Л.: ОНТИ, 1938.]

128. Edwards H. M. Fermat's last theorem. A genetic introduction to algebraic number theory. — New York: Springer-Verlag, 1977. [Имеется перевод: Эдвардс Г. М. Последняя теорема Ферма. Генетическое введение в алгебрическую теорию чисел. — М.: Мир, 1980.]

129. Edwards H. M. The background of Kummers proof of Fermat's last theorem for regular exponent. — Arch. Hist. Exact Sci., 1974, v. 14, p. 219—326. См. также дополнение к последней работе: там же, 1977, v. 17, p. 371—394.

130. Eisenstein G. Einfacher Beweis und Verallgemeinerung des Fundamentaltheorems für die biquadratischen Reste. — In: Mathematische Werke, Band I, pp. 223—245. New York: Chelsea, 1975.

131. Eisenstein G. Lois de réciprocité. — In: Mathematische Werke, Band I, pp. 53—67. New York: Chelsea, 1975.

132. Eisenstein G. Beweis des allgemeinsten Reciprocitätsgesetze zwischen reelen und complexen Zahlen. — In: Mathematische Werke, Band II, pp. 189—198. New York: Chelsea, 1975.

133. Erdös P. On a new method in elementary number theory which leads to an elementary proof of the prime number theorem. — Proc. Nat. Acad. Sci. U. S. A., 1949, v. 35, 374—384.

134. Flanders H. Generalization of a theorem of Ankeny and Rogers. — Ann. Math., 1953, v. 57, p. 392—400.

135. Fulton W. Algebraic curves. — New York: W. A. Benjamin, 1969.

136. Gauss C. F. Disquisitiones Arithmeticae. — Transl. by A. A. Clarke. New Haven, Conn.: Yale University Press, 1966. [Имеется перевод: Гаусс К.Ф. Труды по теории чисел. — М.: изд. АН СССР, 1959.]

137. Gauss C. F. Mathematische Tagebuch, 1796—1814. — Edited by K.-R.Biermann. Ostwalds Klassiker 256.

138. Gerstenhaber M. The 152nd proof of the law of quadratic reciprocity. — Amer. Math. Monthly, 1963, v. 70, p. 397—398.

139. Goldstein L. J. A history of the prime number theorem. — Amer. Math. Monthly, 1973, v. 80, p. 599—615.

140. Goldstein L. J. Analytic number theory. — Princeton, N. J.: Prentice-Hall, 1971.

141. Goss D. A simple approach to the analytic continuation and values at negative integer for Riemann's zeta function. — Proc. Amer. Math. Soc., 1981, v. 81, no. 4, p. 513—517.

142. Gross B. H., Rohrlich D. E. Some results on the Mordell—Weil group of the Jacobian of the Fermat curve. — Invent. Math., 1978, v. 44, p. 201—224.

143. Hall T. Carl Friedrich Gauss, a biography. — Transl. by A. Froderberg. Cambridge, Mass: M. I. T. Press, 1970.

144. Hartshorne R. Algebraic geometry. — New York: Springer-Verlag, 1977. [Имеется перевод: Хартсхорн Р. Алгебраическая геометрия. — М.: Мир, 1981.]

145. Hartung P. G. On the Pellian equation. — J. Number Theory, 1980, v. 12, p. 110—112.

146. Heath T. L. Diophantus of Alexandria: A study in the history of greek algebra. — New York: Dover, 1964.

147. Heath T. L., Brown D. R., Patterson S. J. The distribution of Kummer sums at prime arguments. — J. Reine und Angew. Math. 1979, v. 310, p. 111—136.

148. Heffter L. Ludwig Stickelberger. — Deutsche Math. Jahr., 1937, B. 47, S. 79—86.

149. Herbrand J. Sur les classes des corp circulaires. — J. Math. Pures et Appl., 1932, vii, p. 417—441.

150. Herstein I. Topics in algebra. — Lexington, Mass: Xerox College, 1975.

151. Hilbert D. Die Theorie der algebraischen Zahlkörper. — In: Gesammelte Abhandlungen, Vol. 1, p. 63—363. New York: Chelsea, 1965.

152. Hofmann J. E. Über Zahlentheoretische Methoden Fermats und Eulers, ihre Zusammenhänge und ihre Bedeutung. — Arch. Hist. Exact Sci., 1960—62, p. 122—159.

153. Hurwitz A. Einige Eigenschaften der Dirichlet'schen Funktion $F(s) = \Sigma(D/n)\,1/n^s$, etc ... . -- In. Hurwitz A. Mathematische Werke, Band I, pp. 72—88, Basel and Stuttgart: Birkhäuser-Verlag, 1963.

154. Hurwitz A. Mathematische Werke, Band II. — Basel und Stuttgart: Birkhäuser-Verlag, 1963.

155. Iwasawa K. Lectures on *p*-adic *L*-functions. — Ann. Math. Studies, Princeton Press, 1974.

156. Iwasawa K. A note on Jacobi sums. — Symp. Math., 1975, v. 15, p. 447—459.

157. Iwasawa K. A note on cyclotomic fields. — Ivent. Math., 1976, v. 36, p. 115—123.

158. Iyanaga S. (Ed.) Theory of numbers. — Amsterdam: North-Holland, 1975.

159. Johnson W. Irregular primes and cyclotomic invariants. — Math. Comp., 1975, v. 29, p. 113—120.

160. Joly J. R. Equations et variétés algébriques sur un corps fini. — L'Enseignement Math., 1973, v. 19, p. 1—117.

161. Katz N. An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields. — Proc. of Symposia in Pure Math., Vol. 28, p. 275—305. Providence, R. I.: Amer. Math. Society, 1976.

162. Koblitz N. *P*-adic numbers, *p*-adic analysis, and zeta-functions. — New York: Springer-Verlag, 1977. [Имеется перевод: Коблиц Н. *p*-адические числа, *p*-адический анализ и дзета-функции. — М.: Мир, 1982.]

163. Kummer E. E. De residuis cubicis disquisitiones nonnullae analyticae. — J. Reine und Angew. Math., 1846, B. 32, S. 341—359. (Collected Papers, Vol. 1, p. 145—163. New York: Springer-Verlag, 1975.)

164. Kummer E. E. Collected Papers, Vol. 1. — New York: Springer-Verlag, 1975.

165. Landau E. Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale ... . — New York: Chelsea, 1949.

166. Landau E. Vorlesungen über Zahlentheorie, Vols. 1—3. — Leipzig, 1927.

167. Lang S. Cyclotomic fields. — New York: Springer-Verlag, 1978.

168. Lang S. Algebraic number theory. — Reading, Mass.: Addison-Wesley, 1970.

169. Lang S. Elliptic functions. — Reading, Mass.: Addison-Wesley, 1970. [Имеется перевод: Ленг С. Эллиптические функции. — М.: Наука, 1984.]

170. Lang S. Diophantine geometry. — New York: Wiley-Intercsience, 1962. [Имеется перевод: Ленг С. Основы диофантовой геометрии. — М.: Наука, 1986.]

171. Lang S. Cyclotomic fields, II. — New York: Springer-Verlag, 1980.

172. Lang S. Review of L. J. Mordell's diophantine equations. — Bull. Amer. Math. Soc., 1970, v. 76, p. 1230—1234.

173. Lang S. Higher dimensional diophantine problems. — Bull. Amer. Math. Soc., 1974, v. 80, no. 5, p. 779—787.

174. Lehmer E. On Euler's criterion. — J. Aust. Math. Soc., 1959/61, part 1, p. 67—70.

175. Lehmer E. Rational reciprocity laws. — Amer. Math. Monthly, 1978, v. 85, p. 467—472.

176. Lehmer E. On the location of Gauss sums. — Math. Comp., 1956, v. 10, p. 194—202.

177. Leonard P. A., Williams S. Jacobi sums and a theorem Brewer. — Rocky Mountain. J. Math., Spring, 1975, v. 5, no. 2.

178. Leopoldt A. W. Eine Verallgemeinerung der Bernoullischen Zahlen. — Abhandl. Math. Sem. Hamburg, 1958, v. 22, p. 131—140.

179. LeVeque W. J. Fundamentals of number theory. — Reading, Mass.: Addison-Wesley, 1977.

180. LeVeque W. J. A brief survey of diophantine equations. — M. A. A. Studies in Mathematics, 1969, v. 6, p. 4—24.

181. von Lienen H. Reele kubische und biquadratische Legendre symbole. — J. Reine und Angew. Math., 1979, B. 305, S. 140—154.

182. Loxton J. H. Some conjectures concerning Gauss sums. — J. Reine und Angew. Math., 1978, B. 297, S. 153—158.

183. Marcus D. A. Number fields. — New York: Springer-Verlag, 1977.

184. Masley J. M. Where are number fields with small class number? — Le cture Notes in Mathematics, Vol. 751, p. 221—242. New York: Springer-Verlag-1979.

185. Masley J. M. Class groups of abelian number fields. — Proc. Queen's Number Theory Conference, 1979. Edited by P. Ribenboim. Kingston, Ontario: Queen's University.

186. Matthews C. R. Gauss sums and elliptic functions. I: The Kummer sum. — Invent. Math., 1979. v. 52, p. 163—185; II; The quartic case, 1979, v. 54, p. 23—52.

187. Mazur B. Rational points on modular curves. — In: Modular functions of one variable, V. Lecture Notes in Mathematics, Vol. 601. New York: Springer-Verlag, 1976.

188. Metsänkylä T. Distribution of irregular prime numbers. — J. Reine und Angew. Math., 1976, B. 282, S. 126—130.

189. Mordell L. J. Diophantine equations. — New York: Academic Press, 1969.

190. Mordell L. J. Review of S. Lang's diophantine geometry. — Bull. Amer. Math. Soc., 1964, v. 70, p. 491—498.

191. Mordell L. J. The infinity of rational solutions of $y^2 = x^3 + k$. — London Math. Soc., 1966, v. 41, p. 523—525.

192. Morlaye B. Démonstration élémentaire d'un théorème de Davenport et Hasse. — L'Enseignement Math., 1973, v. 18, 269—276.

193. Moser L. A theorem on quadratic residues. — Proc. Amer. Math. Soc., 1951, v. 2, p. 503—504.

194. Muskat J. B. Reciprocity and Jacobi sums. — Pacific J. Math., 1967, v. 20, p. 275—280.

195. Nagell T. Sur les restes et nonrestes cubiques. — Arkiv. Math., 1952, v. 1, p. 579—586.

196. Narkiewicz W. Elementary and analytic theory of algebraic numbers. — Warsaw: Polish Scientific Publications, 1974.

197. Neumann J. von, Goldstine H. H. A numerical study of a conjecture of Kummer. — MTAC, 1953, v. 7, p. 133—134.

198. Newman D. J. Simple analytic proof of the prime number theorem. — Amer. Math. Monthly, 1980, v. 87, p. 693—696.

199. Nielson N. Traité élémentaire des nombres Bernoulli. — Paris: 1923.

200. Olson L. D. The trace of Frobenius for elliptic curves with complex multiplication. — Lecture Notes in Mathematics, v. 732, p. 454—476. New York: Springer-Verlag, 1979.

201. Olson L. D. Points of finite order on elliptic curves with complex multiplication. — Manuscripta Math., 1974, v. 14, p. 195—205.

202. Olson L. D. Hasse invariants and anomalous primes for elliptic curves with complex multiplication. — J. Number Theory, 1976, v. 8, p. 397—414.

203. Poincaré H. Sur les propriétés des courbes algebriques planes. — J. Liouville (v), 1901, v. 7, p. 161—233.

204. Rademacher H. Topics in analytic number theory. — Die Grundlehren der mathematischen Wissenschaften. New York: Springer-Verlag, 1964.

205. Reichardt H. Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen. — J. Reine Angew. Math., 1942, B. 184, S. 12—18.

206. Ribenboim P. 13 lectures on Fermat's Last Theorem. — New York: Springer-Verlag, 1979.

207. Ribenboim P. Algebraic numbers. — New York: Wiley, 1972.

208. Ribet K. A modular construction of unramified p-extensions of $Q(\mu_p)$. — Invent. Math., 1976, v. 34, p. 151—162.

209. Rieger C. J. Die Zahlentheorie bei C. F. Gauss. — In: C. F. Gauss, Leben und Werk, SS. 38—77. Berlin: Haude & Spenersche Verlagsbuchhandlung, 1960.

210. Robert A. Elliptic curves. Lecture Notes in Mathematics, vol. 326. — New York: Springer-Verlag, 1973.

211. Rozen M. I., Kraft J. Eisenstein reciprocity and n-th power residues. — Amer. Math. Monthly, 1981, v. 88, p. 269—270.

212. Rosen M. I. Abel's theorem on the lemniscate. — Amer. Math. Monthly, 1981, v. 88, p. 387—395.

213. Samuel P. Théorie algébrique des nombres. — Hermann: Paris, 1967.

214. Samuel P., Zariski O. Commutative algebra, vol. 1. — New York: Springer-Verlag, 1975—1976. [Имеется перевод: Зарисский О., Самюэль П. Коммутативная алгебра. — М.: ИЛ, 1963. т. 1—2.]

215. Selberg A. An elementary proof of the prime number theorem. — Ann. Math., 1949, v. 50, p. 305—319.

216. Selmer E. S. The diophantine equation $ax^3 + by^3 + cz^3 = 0$. — Acta Math., 1951, v. 85, p. 203—362.

217. Schmidt W. M. Diophantine approximation. — Lecture Notes in Mathematics, vol. 785. New York: Springer-Verlag, 1980.

218. Schmidt W. M. Equations over finite fields: an elementary approach. — Lecture Notes in Mathematics, vol. 536. New York: Springer-Verlag, 1976.

219. Шафаревич И. Р. Основы алгебраической геометрии. — М.: Наука, 1972.

220. Smith D. E. Source book in mathematics, vols. 1 and 2. New York: Dover, 1959.

221. Stark H. M. On the Riemann hypothesis in hyperelliptic function fields. — A. M. S. Proc. Symp. Pure Math., 1973, v. 24, p. 285—302.

222. Степанов С. А. Рациональные точки алгебраических кривых над конечными полями. — Актуальные проблемы аналитической теории чисел. — Минск, Наука и техника, 1974, с. 224—241.

223. Stephens N. M. The diophantine equation $x^3 + y^3 = dz^3$ and the conjectures of Birch and Swinnerton-Dyer. — J. Reine und Angew. Math., B. 231.

224. Stickelberger L. Über eine Verallgemeinerung von der Kreistheilung. — Math. Ann., 1890, B. 37, p. 321—367.

225. Stolarsky K. B. Algebraic numbers and diophantine approximation. — New York: Dekker, 1974.

226. Swinnerton-Dyer H. P. F. The conjectures of Birch and Swinnerton-Dyer and of Tate. — In: Proceedings of a Conference on Local Fields. Berlin—Heidelberg—New York: Springer-Verlag, 1967. [Имеется перевод: Математика, 1969, 13 : 5, 3—25.]

227. Tate J. The arithmetic of elliptic curves. — Invent. Math., 1974, v. 23, p. 179—206.

228. Thomas A. D. Zeta functions: An introduction to algebraic geometry.— London—San Francisco: Pitman, 1977.

229. Trost E. Primzahlen. — Basel and Stuttgart: Birkhäuser-Verlag, 1953. [Имеется перевод: Трост Э. Простые числа. — М.: Гос. изд. физ.-матем. лит. 1959.]

230. Uspensky J. V., Heaslet M. A. Elementary number theory. — New York: McGraw-Hill, 1939.

231. Vandiver H. S. Fermat's last theorem. — Amer. Math. Monthly, 1946, v. 53, p. 555—578.

232. Vandiver H. S. On developments in an arithmetic theory of the Bernoulli and allied numbers. — Scripta Math., 1961, v. 25, p. 273—303.

233. van der Poorten A. A proof that Euler missed ... Apery's proof of the irrationality of $\zeta(3)$: An informal report. — The Mathematical Intellingencer, 1978, v. 1, no 1, p. 195—203.

234. Wagstaff S. The irregular primes to 125000. — Math. Comp., 1978, v. 32, no 142, p. 583—591.

235. Weil A. Two lectures on number theory: Past and present. — L'Enseignement Math., 1973, v. XX, p. 81—110. Weil A. Oeuvres Scientifiques, vol. III, pp. 279—302. New York: Springer-Verlag, 1979.

236. Weil A. Sommes de Jacobi et caractères de Hecke. — Gött. Nach. (1974), 1—14. См. также: Weil A. Oeuvres Scientifiques, vol. III, pp. 329—342. — New York: Springer-Verlag, 1979.

237. Weil A. Sur les sommes de trois et quatre carrés. — L'Enseignement Math., 1974, v. 20, p. 303—310. См. также: Weil A. Oeuvres Scientifiques, vol. III. — New York: Springer-Verlag, 1979.

238. Weil A. La cyclotomie jadis et naguère. — L'Enseignement Math., 1974, v. 20, p. 247—263. См. также: Weil A. Oeuvres Scientifiques, vol. III, p. 311—327. — New York: Springer-Verlag, 1979.

239. Weil A. Review of «Mathematische Werke, by Gotthold Eisenstein». — In: Weil A. Oeuvres Scientifiques, vol. III, p. 398—403. — New York: Springer-Verlag, 1979.

240. Weil A. Fermat et l'équation de Pell. — In: Oeuvres Scientifiques, vol. III, p. 413—419. New York: Springer-Verlag, 1979.

241. Weil A. Oeuvres Scientifiques, Collected Papers, 3 vols. Corrected second printing. — New York: Springer-Verlag, 1980.

242. Wiles A. Modular curves and the class group of $Q(\zeta_p)$. — Invent. Math., 1980. v. 58, p. 1—35.

243. Williams K. S. On Euler's criterion for cubic nonresidues. — Proc. Amer. Math. Soc., 1975, v. 49, p. 277—283.

244. Williams K. S. Note on Burde's rational biquadratic reciprocity law. — Canad. Math. Bull., 1977, (1) v. 20, p. 145—146.

245. Williams K. S. On Eisenstein's supplement to the law of cubic reciprocity. — Bull. Cal. Math. Soc., 1977, v. 69, p. 311—314.

246. Wyman B. F. What is a reciprocity law? Amer. Math. Monthly, 1972, v. 79, p. 571—586.

247. Yokoi H. On the distribution of irregular primes. — J. Number Theory, 1975, v. 7, p. 71—76.

248. Zeta functions. — In: Encyclopedic Dictionary of Mathematics, Edited by S. Iyanaga, Y. Kawada. Cambridge, Mass: M. I. T. Press, 1977, p. i372—i393.

Литература, добавленная при переводе

1*. Акс Дж., Кохэн С. Диофантовы проблемы над локальными полями. — Математика, 1965, 9 : 5, с. 3—27.

2*. Алгебра и теория чисел: избранные доклады семинара Бурбаки. — М.: Мир, 1987.

3*. Башмакова И. Г., Славутин Е. И. История диофантова анализа (от Диофанта до Ферма). — М.: Наука, 1984.

4*. Ван-дер-Варден Б. Л., Алгебра. — М.: Наука, 1979.

5*. Вейль А. Теория чисел и алгебраическая геометрия. — Математика, 1958, 2 : 4, с. 49—58.

6*. Вейль А. Абстрактная алгебраическая геометрия в сравнении с классической. — Математика, 1958, 2 : 4, с. 59—66.

7*. Вейль А. Об определении рядов Дирихле через функциональные уравнения. — Математика, 1970, 14 : 6, с. 133—145.

8*. Вейль А. Основы теории чисел. — М.: Мир, 1972.

9*. Венков А. Б., Проскурин Н. В. Автоморфные функции и проблема Куммера. — Успехи мат. наук, 1982, т. 37, № 3, с. 134—165.

10*. Венков Б. А. Элементарная теория чисел. — М.—Л.: ОНТИ, 1937.

11*. Делинь П. Гипотеза Вейля, — Успехи матем. наук, 1976, т. 39, № 5, с. 159—190.

12*. Диксон Л. Е. Введение в теорию чисел. — Тбилиси, 1941.

13*. Диофант. Арифметика и книга о многоугольных числах. — М.: Наука, 1974.

14*. Живые числа. — М.: Мир, 1985.

15*. Ленг С. Алгебра. — М.: Мир, 1968.
16*. Милн Дж. Этальные когомологии. — М.: Мир. 1983.
17*. Милнор Дж. Введение в алгебраическую K-теорию. — М.: Мир, 1974.
18*. Прахар К. Распределение простых чисел. — М.: Мир, 1967.
19*. Привалов И. И. Введение в теорию функций комплексного переменного.— М.: Наука.
20*. Проблемы теории диофантовых приближений. — М.: Мир, 1974.
21*. Тейт Дж. Алгебраические классы когомологий. — Успехи матем. наук, 1965, т. 20, № 6, с. 27—40.
22*. Хассе Х. Лекции по теории чисел. — М.: ИЛ, 1953.
23*. Шафаревич И. Р. Новое доказательство теоремы Кронекера—Вебера. — Труды Матем. ин-та АН СССР, 1951, т. 38, с. 382—387.
24*. Шафаревич И. Р. Дзета-функция. — М.: МГУ, 1969.
25*. Faltings G. Endlichkeitssatze für abelschen Varietäten über Zahlkörpern.— Inventiones math., 1983, v. 73, n. 3, p. 349—366.
26*. Fouvry E. Theoreme de Brun—Titchmarsh; application au theoreme de Fermat. — Inventiones math., 1985, v. 79, n°2, p. 383—407. Adleman L. M., Heath—Brown D. R. The first case of Fermat's last theorem.— Inventiones math., 1985, v. 79, n° 2, p. 409—416.
27*. Gross B. Zagier D. The heights of Heegner points and the derivatives of L-functions. — Inventiones math., 1986.
28*. Mestre J.-F. Formules explicites et minorations de conducteurs de variétés algébriques. — Compos. math., 1986.
29*. Modular functions of one variable IV. — Lecture Notes in Mathematics, no 476, Berlin: Springer, 1975.
30*. Serre J.-P. Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. — C. R. Acad. Sci., 1983, Ser. 1, t. 296, p. 397—402.
31*. Washington L. C. Introduction to cyclotomic fields. — New York: Springer, 1982.
32*. Arithmetic geometry. — N. Y., 1986.
33*. Masur B. Arithmetic on curves. — Bull. Amer. Math. Soc., 1986, v. 14, no 2, p. 207—259.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ОГЛАВЛЕНИЕ