Дж.В.С.Касселс

ВВЕДЕНИЕ В ТЕОРИЮ ДИОФАНТОВЫХ ПРИБЛИЖЕНИИ

ИЗДАТЕЛЬСТВО ИНОСТРАННОЙ ЛИТЕРАТУРЫ, Москва 1961

Книга Касселса является одной из немногих в мировой литературе, а на русском языке чуть ли не единственной монографией по одному из важных разделов современной теории чисел — теории диофантовых приближений. В этой теории изучаются, в частности, вопросы наилучшего приближения иррациональных чисел рациональными: тонкое строение "арифметической прямой" и "арифметического пространства". Теория диофантовых приближений находит многочисленные приложения в других разделах математики, например в теории функций, в теории динамических систем и др.

Очень ясно и сжато написанная книга Касселса будет полезна студентам, аспирантам и научным работникам-математикам.

ОГЛАВЛЕНИЕ

УКАЗАТЕЛЬ

ПРЕДИСЛОВИЕ

Цель этой монографии — дать представление об основных технических приемах и о некоторых наиболее замечательных результатах теории диофантовых приближений. Монография рассчитана на студентов старших курсов, владеющих элементами теории чисел. От читателя не требуется никаких специальных знаний, кроме основ теории интеграла Лебега, необходимых для понимания гл. VII, и элементов алгебраической теории чисел, необходимых для понимания гл. VIII (но не гл. VI). Все, что требуется из геометрии чисел, излагается подробно в приложении В, к которому читатель может обращаться по мере надобности.

Библиографические замечания и советы по дальнейшему чтению даются в конце каждой главы, а изредка встречающиеся комментарии предназначены для более искушенного читателя. Вообще я упоминал только сравнительно новые и наиболее доступные работы, из которых можно было бы получить дальнейшие ссылки. Результаты, полученные до 1936 г., излагаются в содержательной и незаменимой книге Коксмы (1936)[1]. Там, где не дается никаких ссылок, не следует полагать, что мы претендуем на оригинальность: многие результаты являются общим достоянием, и я включил их, не помня источника.

Специалист заметит пробелы. В частности, очень мало говорится о совместном приближении набора иррациональных чисел и ничего о точных константах. Небольшое число имеющихся точных результатов связано с глубокими исследованиями, например с давенпортовским значением критического детерминанта $|X|(Y^2+Z^2)\leqslant 1$ и с совсем иными техническими приемами, отличными от тех, которые мы приводим

---

[1]) Ссылки см. на стр. 196—201.

в этой книге (я совсем не пользуюсь словом „решетка"). Современное состояние вопроса см. у Давенпорта (1954). Однако в приложении В читатель найдет предпосылки для понимания теоремы Малера о компактности для решеток [Малер (1946)], которая является важным орудием при изучении совместных приближений, а также и во многих других вопросах.

Существуют аналоги многих результатов этой книги, в которых роль действительных чисел играют p-адические числа [см. Лутц (1951) и цитированную там литературу].

Мне приятно выразить здесь благодарность профессорам Давенпорту, Малеру, Морделлу и г-ну Берчу, прочитавшим и первоначальную рукопись и корректуры; проф. Холлу и г-ну Суиннертону-Дайеру, прочитавшим корректуры: их проницательная критика как формы, так и содержания привела к тому, что в окончательном виде книга мало напоминает первоначальный вариант. Проф. Роджерс и г-н Берч разрешили мне использовать неопубликованные работы, относящиеся соответственно к цепочкам Маркова и теоремам переноса, а д-р Рот предоставил в мое распоряжение до опубликования рукопись с кардинальным улучшением теоремы Туэ — Зигеля.

Касселс

Тринити Колледж,
Кембридж, 1956

ОБОЗНАЧЕНИЯ

1. Под „числом“ понимается „действительное число“, если противное не оговорено или не подразумевается по контексту.

2. Для числа θ вводятся следующие стандартные обозначения:

$[\theta]$ — целая часть числа θ, т. е. такое целое, что $[\theta] \leqslant \theta < [\theta]+1$;

$\{\theta\}$ — дробная доля числа θ, т. е. $[\theta]+\{\theta\}=\theta$;

$\|\theta\|$ — расстояние до ближайшего целого, т. е.

$$\|\theta\|=\min(\{\theta\},\ 1-\{\theta\})=\min|\theta-n| \quad (n=0,\ \pm 1,\ \pm 2,\ldots).$$

Ясно, что $\|\theta_1+\theta_2\| \leqslant \|\theta_1\|+\|\theta_2\|$ и $\|n\theta\| \leqslant |n|\,\|\theta\|$ для всех целых n.

Скобки [ ], { } употребляются только в указанном выше смысле, кроме тех случаев, когда нет опасности смешения.

3. Векторы (упорядоченные системы чисел) обозначаются жирными буквами, а их координаты — соответствующими обыкновенными буквами, например $\boldsymbol{\alpha}=(\alpha_1,\ \ldots,\ \alpha_n)$, $\mathbf{z}=(z_1,\ \ldots,\ z_m)$. Если требуется обозначить последовательность векторов (с одинаковым числом координат) путем приписывания индексов, то это делается так:

$$\mathbf{z}^{(r)}=(z_{r1},\ \ldots,\ z_{rm}) \qquad (r=1,\ 2,\ \ldots).$$

Нулевой вектор $(0,\ \ldots,\ 0)$ обозначается через $\mathbf{0}$. Для сложения и умножения векторов употребляются обычные обозначения:

$$\lambda\mathbf{z}=(\lambda z_1,\ \ldots,\ \lambda z_m),$$

$$\mathbf{z}^{(1)}+\mathbf{z}^{(2)}=(z_{11}+z_{21},\ \ldots,\ z_{1m}+z_{2m}).$$

Если $\mathbf{u}=(u_1,\ \ldots,\ u_m)$ и $\mathbf{z}=(z_1,\ \ldots,\ z_m)$, то полагаем

$$\mathbf{uz}=u_1z_1+\ \ldots\ +u_mz_m.$$

Мы не стремимся устанавливать различие между ковариантными и контравариантными векторами даже там, где это могло бы быть уместно. Мы часто представляем себе векторы как точки соответствующего эвклидова пространства и пользуемся естественным языком для выражения их связей друг с другом.

4. $a \mid b$ для целых a, b означает „a делит b". Аналогично $a \nmid b$ означает „a не делит b". Наибольший общий делитель и наименьшее общее кратное системы целых чисел $a_1, \ldots, a_m$ обозначаются через н. о. д. $(a_1, \ldots, a_m)$ или н. о. д. (a_j) и н. о. к. $(a_1, \ldots, a_m)$ или н. о. к. (a_j) соответственно.

5. Символ $\in$ мы заимствуем из логики. Если A есть множество каких-нибудь элементов и a — некоторый элемент, то $a \in A$ означает, что „a принадлежит A". Например, если A — множество рациональных чисел и a — некоторое число, то $a \in A$ означает, что „a — рациональное число". Смысл знака $\notin$ противоположен смыслу знака $\in$.

6. Наименьшая верхняя грань и наибольшая нижняя грань множества A действительных чисел a обозначаются соответственно через $\sup\limits_{a \in A} a$, $\inf\limits_{a \in A} a$. Верхний и нижний пределы последовательности a_j действительных чисел обозначаются соответственно через $\limsup a_j$ и $\liminf a_j$. Так,

$$\liminf a_j = \lim_{J \to \infty} \left(\inf_{j \geqslant J} a_j \right).$$

7. Теоремы и леммы нумеруются последовательно в каждой главе, а уравнения и т. д. — в каждом параграфе. Ссылка (7) означает „выражение (7) из данного параграфа", а ссылка (2.7) означает „выражение (7) из § 2".

8. Список работ, на которые имеются ссылки, приведен на стр. 196. Ссылка на работу дается посредством указания имени автора и года. Например, Перрон (1913). Работы, вышедшие в одном и том же году, различаются добавлением букв (a, b).

9. Предметный указатель дан на стр. 213. Соответствующие определения выделены в тексте курсивом.

Глава I

ОДНОРОДНЫЕ ПРИБЛИЖЕНИЯ

§ 1. Введение. В этой и следующей главах мы выясним, насколько точно (в соответствующем смысле) иррациональное число θ может быть приближено рациональными дробями p/q. Здесь p, q — целые, и, не ограничивая общности, можно считать $q > 0$. Так как при фиксированном q минимум разности $|\theta - p/q| = q^{-1}|q\theta - p|$ равен $q^{-1}\|q\theta\|$ [1]), то можно рассматривать $\|q\theta\|$ вместо $|\theta - p/q|$. Это, естественно, приводит к теории непрерывных дробей, являющейся полезным орудием исследования.

Следующая теорема является простым, но полезным результатом.

Теорема I. *Пусть θ и $Q > 1$ — действительные числа. Тогда существует целое q, такое, что*

$$0 < q < Q, \quad \|q\theta\| \leqslant Q^{-1}.$$

Замечание 1. Число θ не обязательно иррационально. Таким образом, эта теорема дает сведения о приближении рациональных чисел рациональными же числами с меньшими знаменателями.

Замечание 2. Если Q — целое и $\theta = Q^{-1}$, то $\|q\theta\| \geqslant Q^{-1}$ для $0 < q < Q$. Следовательно, знак $\leqslant$ в теореме не может быть заменен знаком $<$.

Первое доказательство (Дирихле). Допустим сначала, что Q — целое. Рассмотрим распределение $Q+1$ чисел [2])

$$0,\ 1,\ \{q\theta\} \qquad (0 < q < Q), \tag{1}$$

[1]) Обозначение см. на стр. 7.
[2]) Обозначение см. на стр. 7.

удовлетворяющих неравенству $0 \leqslant x \leqslant 1$, среди Q подинтервалов

$$\frac{u}{Q} \leqslant x < \frac{u+1}{Q}, \quad 0 \leqslant u < Q, \tag{2}$$

где вместо знака $<$ берется знак $\leqslant$, когда $u = Q - 1$. По меньшей мере один из подинтервалов (2) должен содержать две точки из $Q+1$ точек (1). Значит, можно найти целые r_1, r_2, s_1, s_2, такие, что

$$|(r_1\theta - s_1) - (r_2\theta - s_2)| \leqslant Q^{-1},$$

где без ограничения общности можно считать $r_2 < r_1$. Беря $q = r_1 - r_2$, получаем утверждение теоремы.

Справедливость теоремы при Q не целом следует сразу из ее справедливости для $[Q]+1$.

Второе доказательство. Доказываемая теорема является по существу частным случаем теоремы Минковского о линейных формах (теорема III приложения В). Согласно этой теореме, существуют целые p, q, не равные нулю одновременно, такие, что

$$|\theta q - p| \leqslant Q^{-1}, \quad |q| < Q.$$

Если бы $q = 0$, то мы имели бы $|p| = |\theta q - p| \leqslant Q^{-1} < 1$ и $p = 0$. Следовательно, можно считать, что $q > 0$, беря, если в этом есть надобность, $-p$, $-q$ вместо p, q.

§ 2. Непрерывные дроби. По теореме I неравенство

$$q\|q\theta\| < 1 \tag{1}$$

при иррациональном θ имеет бесконечно много целых решений $q > 0$. Теория непрерывных дробей дает более подробные сведения и позволяет, в частности, заменить в неравенстве (1) единицу на $5^{-1/2}$. Непрерывные дроби играют основную роль во многих исследованиях, хотя в этой книге мы и не будем ими широко пользоваться.

Дробь p/q $(q > 0)$ называется *наилучшим приближением* числа θ, если

$$\|q\theta\| = |q\theta - p|$$

и если

$$\|q'\theta\| > \|q\theta\| \quad \text{для} \quad 0 < q' < q.$$

Ясно, что $q=q_1=1$ дает наилучшее приближение с некоторым $p=p_1$ и

$$|q_1\theta-p_1|=\|\theta\|\leqslant\frac{1}{2}.$$

Если $\|q_1\theta\|=0$, т. е. θ — целое число, то процесс останавливается. В противном случае найдется значение q, такое, что $\|q\theta\|<\|q_1\theta\|$ (например, по теореме I при $Q>\|q_1\theta\|^{-1}$). Пусть q_2 — наименьшее q, обладающее этим свойством, так что $|q_2\theta-p_2|=\|q_2\theta\|<\|q_1\theta\|$ при некотором p_2, но $\|q\theta\|\geqslant\|q_1\theta\|$ при $0<q<q_2$. Если $\|q_2\theta\|=0$, то процесс останавливается. В противном же случае процесс можно продолжить и получить последовательность целых[1])

$$q_1=1<q_2<q_3<\ldots$$

и $p_1, p_2, \ldots$, таких, что

$$\|q_n\theta\|=|q_n\theta-p_n|, \tag{2}$$

$$\|q_{n+1}\theta\|<\|q_n\theta\|, \tag{3}$$

$$\|q\theta\|\geqslant\|q_n\theta\| \quad \text{для} \quad 0<q<q_{n+1}. \tag{4}$$

Согласно (4) и теореме I при $Q=q_{n+1}$, имеем

$$q_n\|q_n\theta\|<q_{n+1}\|q_n\theta\|\leqslant 1. \tag{5}$$

Если бы $q_{n+1}\theta-p_{n+1}$ и $q_n\theta-p_n$ имели одинаковый знак, то мы должны были бы иметь

$$|q'\theta-p'|<|q_n\theta-p_n|,$$

где $p'=p_{n+1}-p_n$, $0<q'=q_{n+1}-q_n<q_{n+1}$, вопреки (4). Следовательно,

$$(q_n\theta-p_n)(q_{n+1}\theta-p_{n+1})\leqslant 0. \tag{6}$$

Лемма 1. А. *Дроби p_n/q_n образуют все наилучшие приближения числа θ, расположенные в порядке возрастания q_n.*

В. *Если θ рационально, то $\theta=p_N/q_N$ при некотором N.*

С. *Если θ иррационально, то $p_n/q_n\to\theta$.*

---

[1]) Позднее мы слегка изменим эти обозначения (стр. 14).

Доказательство. A. Согласно построению, p_{n+1}/q_{n+1} есть наилучшее приближение p/q с наименьшим $q > q_n$.

B. Если $\theta = u/v$ $(v > 0)$ с взаимно простыми u, v, то, очевидно, u/v есть наилучшее приближение.

C. $|\theta - p_n/q_n| < q_n^{-2}$ согласно (5).

Лемма 2.

$$q_{n+1}p_n - q_np_{n+1} = \pm 1.$$

Доказательство. Левая часть есть целое число, и

$$q_{n+1}p_n - q_np_{n+1} = q_n(q_{n+1}\theta - p_{n+1}) - q_{n+1}(q_n\theta - p_n). \quad (7)$$

Следовательно, по (5), (6) имеем

$$|q_{n+1}p_n - q_np_{n+1}| = q_n\|q_{n+1}\theta\| + q_{n+1}\|q_n\theta\| > 0$$

и

$$< 2q_{n+1}\|q_n\theta\| \leqslant 2. \quad (7')$$

Следствие 1. *$q_{n+1}p_n - q_np_{n+1}$ имеет знак, противоположный знаку $q_n\theta - p_n$.*

Следствие 2. $q_{n+1}p_n - q_np_{n+1} = -(q_np_{n-1} - q_{n-1}p_n)$.

Следствие 3. $q_n\|q_{n+1}\theta\| + q_{n+1}\|q_n\theta\| = 1$.

Доказательства вытекают из (6), (7), и (7′).

Лемма 3. *Для $n \geqslant 2$ существует целое $a_n \geqslant 1$, такое, что*

$$q_{n+1} = a_nq_n + q_{n-1}, \quad (8)$$

$$p_{n+1} = a_np_n + p_{n-1}, \quad (9)$$

$$|q_{n-1}\theta - p_{n-1}| = a_n|q_n\theta - p_n| + |q_{n+1}\theta - p_{n+1}|. \quad (10)$$

Доказательство. По следствию 2 леммы 2 имеем

$$p_n(q_{n+1} - q_{n-1}) = q_n(p_{n+1} - p_{n-1}).$$

Следовательно, $q_{n+1} - q_{n-1} = a_nq_n$, $p_{n+1} - p_{n-1} = a_np_n$ при некотором целом a_n, так как p_n, q_n взаимно просты, согласно лемме 2 (или по определению наилучшего приближения). Так как $q_{n+1} > q_{n-1}$, то $a_n > 0$. Наконец, равенство (10) следует из равенств (8) и (9) и неравенства (6).

Равенство (10) дает простой способ нахождения p_{n+1}, q_{n+1}, если известны p_ν, q_ν $(\nu \leqslant n)$. Если θ рационально и

$\|q_n\theta\| = 0$, то процесс останавливается на p_n, q_n, в противном же случае [1])

$$a_n = \left[\frac{\|q_{n-1}\theta\|}{\|q_n\theta\|}\right]$$

согласно (2) и (10), так как $\|q_{n+1}\theta\| < \|q_n\theta\|$. После этого p_{n+1}, q_{n+1} могут быть найдены по формулам (8), (9).

Чтобы начать этот процесс, мы должны знать q_2 (полагаем $q_1 = 1$). Ради простоты мы будем теперь предполагать, что

$$0 < \theta < 1,$$

так как прибавление к θ целого числа не влияет на q_n и тривиально влияет на p_n. Предположим сначала, что

$$0 < \theta \leqslant \frac{1}{2}.$$

Тогда

$$q_1\theta - p_1 = \theta > 0, \quad q_1 = 1, \quad p_1 = 0.$$

Значит, по лемме 2 и по ее первому следствию имеем $p_2 = 1$. Таким образом, лемма 3 сохраняет силу и при $n = 1$, если положить

$$p_0 = 1, \quad q_0 = 0, \quad a_1 = q_2.$$

В частности, при $n = 1$ равенство (10) принимает вид

$$1 = a_1\theta + \|q_2\theta\|,$$

а отсюда $a_1 = [\theta^{-1}]$. Предположим теперь, что

$$\frac{1}{2} < \theta < 1.$$

Тогда $q_1\theta - p_1 = \theta - 1 < 0$, $q_1 = p_1 = 1$, а по лемме 2 и ее первому следствию $q_2 - p_2 = 1$. Чтобы начало схемы вычислений леммы 3 оставалось таким же, как и ранее, мы должны взять

$$\begin{aligned} &p_{-1} = 1, \quad q_{-1} = 0, \\ &p_0 = 0, \qquad q_0 = 1, \quad a_0 = 1, \\ &p_1 = 1, \qquad q_1 = 1, \quad a_1 = q_2 - 1 = p_2. \end{aligned}$$

[1]) Обозначение см. на стр. 7.

Тогда при $n=0$, 1 равенство (10) принимает вид

$$1=\theta+|\theta-1| \qquad (n=0),$$

$$\theta=a_1|\theta-1|+|q_2\theta-p_2| \qquad (n=1),$$

где

$$1>\theta=|q_0\theta-p_0|>|\theta-1|=|q_1\theta-p_1|>|q_2\theta-p_2|.$$

Теперь уместно изменить обозначения, если $1/2<\theta<1$, чтобы иметь одинаковое начало вычислений[1]).

Теорема II. *Пусть* $0<\theta<1$ *и пусть целые* p_n, q_n, a_n *определяются так:*

(A)
$$\left.\begin{aligned} p_0=1, \quad q_0=0,\\ p_1=0, \quad q_1=1,\end{aligned}\right\}$$

(B)
$$\left.\begin{aligned} p_{n+1}=a_np_n+p_{n-1},\\ q_{n+1}=a_nq_n+q_{n-1}\end{aligned}\right\} \quad (n\geqslant 1),$$

где

$$a_n=\left[\frac{|q_{n-1}\theta-p_{n-1}|}{|q_n\theta-p_n|}\right],$$

если $q_n\theta\neq p_n$; *в случае* $q_n\theta=p_n$ *процесс останавливается на* p_n, q_n. *Тогда дроби* p_n/q_n *являются наилучшими приближениями числа* θ *для* $n\geqslant 1$, *если* $a_1>1$, *и для* $n\geqslant 2$, *если* $a_1=1$. *Далее,*

$$(-1)^{n+1}(q_n\theta-p_n)\geqslant 0$$

и

$$q_{n+1}p_n-q_np_{n+1}=(-1)^n.$$

Доказательство непосредственно следует из предыдущего. Чтобы получить знаки в последних двух выражениях, надо использовать значения этих выражений при $n=1$ и неравенство (6) или следствие 2 леммы 2. Дроби p_n/q_n обычно называют *подходящими дробями числа* θ (независимо от того, являются они наилучшими приближениями или нет), а a_n — *неполными частными*.

---

[1]) Некоторые авторы употребляют несколько отличные обозначения (см. замечания в конце главы).

Так как числа a_n определяются числом θ, а число θ по лемме 1 определяется числами a_n, то можно писать, не опасаясь смешения, что

$$\theta = [a_1, a_2, a_3, \ldots],$$

если θ иррационально, и

$$\theta = [a_1, \ldots, a_N],$$

если $\theta = p_{N+1}/q_{N+1}$.

Положим

$$\theta_0 = 1, \quad \theta_n = \frac{|q_n\theta - p_n|}{|q_{n-1}\theta - p_{n-1}|} \quad (n \geqslant 1),$$

так что

$$\theta_1 = \theta, \quad 0 \leqslant \theta_n < 1 \quad (n \geqslant 1). \tag{11}$$

Тогда (10) примет вид

$$\theta_n^{-1} = a_n + \theta_{n+1}. \tag{12}$$

В частности, $\theta_{N+1} = 0$, если $\theta = p_{N+1}/q_{N+1}$. Таким образом, рациональное θ представляется в виде

$$\theta = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{N-1} + \cfrac{1}{a_N}}}}}, \tag{13}$$

что и объясняет название „непрерывная дробь“. Согласно (11), (12), $a_N^{-1} = \theta_N < 1$, т. е. $a_N \neq 1$. Полезно, однако, определить

$$[a_1, \ldots, a_{N-1}, 1] = [a_1, \ldots, a_{N-1} + 1]; \tag{14}$$

но лишь второе выражение определяет дроби p_n/q_n, являющиеся наилучшими приближениями (если же пользоваться первым выражением, то p_N/q_N не является наилучшим приближением).

Так как числа a_n определяются равенством (12), то, очевидно,

$$\theta_n = [a_n, a_{n+1}, \ldots] \quad \text{или} \quad [a_n, a_{n+1}, \ldots, a_N].$$

Аналогично, положим

$$\varphi_n = \frac{q_n}{q_{n+1}} \qquad (n \geqslant 0),$$

так что

$$0 \leqslant \varphi_n \leqslant 1,$$

где знак равенства имеет место в очевидных случаях. Тогда

$$q_{n+1} = a_n q_n + q_{n-1}$$

запишется в виде

$$\varphi_n^{-1} = a_n + \varphi_{n-1}.$$

Следовательно, как и для θ_n, имеем

$$\varphi_n = [a_n, a_{n-1}, \ldots, a_1].$$

Мы можем теперь выразить $q_n \| q_n \theta \|$ через θ_n и φ_n. По следствию 3 леммы 2

$$1 = q_{n+1} \| q_n \theta \| + q_n \| q_{n+1} \theta \| = (\varphi_n^{-1} + \theta_{n+1}) q_n \| q_n \theta \| =$$
$$= (\varphi_{n-1} + a_n + \theta_{n+1}) q_n \| q_n \theta \|.$$

Значит,

$$q_n \| q_n \theta \| = (a_n + \theta_{n+1} + \varphi_{n-1})^{-1} \tag{15}$$

и

$$q_{n+1} \| q_n \theta \| = (1 + \theta_{n+1} \varphi_n)^{-1} > \frac{1}{2}. \tag{16}$$

Мы уже видели, что каждое θ, $(0 < \theta < 1)$ определяет последовательность $a_1, a_2, \ldots$ положительных целых чисел. Теперь покажем обратное, т. е. что каждая последовательность целых положительных чисел определяет число θ. Для этого нам понадобится нетрудная

Лемма 4. *Пусть $n \geqslant 1$ и пусть*

$$\theta = [a_1, \ldots, a_n, a_{n+1}, a_{n+2}, \ldots],$$
$$\theta' = [a_1, \ldots, a_n, b_{n+1}, b_{n+2}, \ldots],$$

где правые части могут содержать конечное число элементов. Тогда

$$|\theta - \theta'| < 2^{-(n-2)}. \tag{17}$$

Замечание. В действительности нам нужен лишь тот факт, что правая часть (17) стремится к 0 при $n \to \infty$.

Доказательство. Пусть p_ν, q_ν $(0 \leqslant \nu \leqslant n+1)$ определяются равенствами (A) и (B) теоремы II. Тогда по теореме II дробь p_{n+1}/q_{n+1} является наилучшим приближением и для θ и для θ', а $q_{n+1}\theta - p_{n+1}$, $q_{n+1}\theta' - p_{n+1}$ имеют одинаковый знак. Но согласно (5) $|q_{n+1}\theta - p_{n+1}| < q_{n+1}^{-1}$, $|q_{n+1}\theta' - p_{n+1}| < q_{n+1}^{-1}$ и, значит, $|\theta - \theta'| < q_{n+1}^{-2}$. Так как $q_{n+1} = a_n q_n + q_{n-1} > 2q_{n-1}$, то по индукции $q_{n+1} > 2^{1/2\,(n-2)}$.

Теорема III. *Пусть $a_1, a_2, \ldots, a_N$ (или $a_1, a_2, \ldots$) — конечная (или бесконечная) последовательность целых положительных чисел. Тогда существует число θ, такое, что $\theta = [a_1, \ldots, a_N]$ (или $\theta = [a_1, a_2, \ldots]$). Если $a_N = 1$, то надо воспользоваться определением* (14).

Доказательство. В случае конечной последовательности чисел a_n положим $\theta_{N+1} = 0$ и определим последовательно

$$\theta_N, \ \theta_{N-1}, \ \ldots, \ \theta_1 = \theta,$$

согласно (12). Ясно, что $0 < \theta_n \leqslant 1$ для $1 \leqslant n \leqslant N$ и $\theta_n = 1$, если только $n = N$, $a_N = 1$. Следовательно, $\theta = [a_1, \ldots, a_N]$.

В случае бесконечной последовательности чисел a_n обозначим

$$\theta^{(N)} = [a_1, \ldots, a_N].$$

Это число, как мы теперь знаем, существует. По лемме 4

$$\lim |\theta^{(N)} - \theta^{(M)}| = 0 \qquad (N \to \infty, \ M \to \infty),$$

а, значит,

$$\theta = \lim \theta^{(N)} \geqslant 0$$

существует. Аналогично

$$\theta_n = \lim \theta_n^{(N)} \geqslant 0, \qquad \theta_n^{(N)} = [a_n, \ldots, a_N]$$

существует. Теперь

$$\left(\theta_n^{(N)}\right)^{-1} = a_n + \theta_{n+1}^{(N)},$$

если $N > n+1$. Значит, в пределе при $N \to \infty$ для всех n имеем $\theta_n^{-1} = a_n + \theta_{n+1}$, что и требовалось доказать.

§ 3. Эквивалентность. Два действительных числа θ, θ' называются *эквивалентными*, если существуют целые числа r, s, t, u, такие, что

$$\theta=\frac{r\theta'+s}{t\theta'+u}, \quad ru-ts=\pm 1.$$

Так как

$$\theta'=\frac{-u\theta+s}{t\theta-r},$$

то эквивалентная связь обладает свойством симметрии. Далее, если θ эквивалентно θ', а θ' эквивалентно θ'', то θ эквивалентно θ'', в чем легко убедиться непосредственным вычислением.

Согласно равенству (12), имеем $\theta_n=(a_n+\theta_{n+1})^{-1}$. Следовательно, числа $\theta=\theta_1, \theta_2, \ldots$ эквивалентны друг другу. Вообще, если

$$\theta=[a_1, \ldots, a_l, c_1, c_2, \ldots],$$
$$\theta'=[b_1, \ldots, b_m, c_1, c_2, \ldots],$$

то каждое из этих чисел эквивалентно

$$\theta_{l+1}=\theta'_{m+1}=[c_1, c_2, \ldots],$$

и, значит, они эквивалентны друг другу. В частности, любые два рациональных числа эквивалентны. Теперь докажем следующую теорему.

Теорема IV. *Для того чтобы два числа* θ, θ' $(0<\theta, \theta'<1)$ *были эквивалентны, необходимо и достаточно, чтобы*

$$\theta=[a_1, a_2, \ldots, a_l, c_1, c_2, \ldots],$$
$$\theta'=[b_1, b_2, \ldots, b_m, c_1, c_2, \ldots]$$

при соответствующих l, m *и* $a_1, \ldots, a_l, b_1, \ldots, b_m, c_1, c_2, \ldots$

Доказательство. Остается только показать, что если θ, θ' — числа иррациональные и эквивалентные, то они могут быть представлены в указанной форме. Пусть

$$\theta=\frac{r\theta'+s}{t\theta'+u}, \quad ru-st=\pm 1. \tag{1}$$

Тогда

$$q\theta-p=\frac{q'\theta'-p'}{t\theta'+u}, \tag{2}$$

где

$$q' = qr - pt, \quad p' = -qs + pu. \tag{3}$$

Так как $ru - st = \pm 1$, то, решая (3), получаем

$$\pm q = q'u + p't, \quad \pm p = q's + p'r. \tag{4}$$

В дальнейшем пары символов со штрихами и без штрихов всегда будут связаны как (p, q) и (p', q') в (3), (4).

Первое равенство (3) можно записать так:

$$q' = q(r - t\theta) + t(q\theta - p). \tag{5}$$

Можно считать, что

$$r - t\theta > 0$$

(в противном случае можно одновременно изменить знаки чисел r, s, t, u). Тогда из (5) следует, что знак целого q' такой же, как и знак целого q, если только

$$|q\theta - p| < \frac{r - t\theta}{|t|}; \tag{6}$$

заметим, что правая часть (6) не зависит от p и q.

Пусть теперь p_n/q_n, p_{n+1}/q_{n+1} являются двумя последовательными наилучшими приближениями числа θ, и пусть p'_n, q'_n, p'_{n+1}, q'_{n+1} определяются равенствами (3) и (4) (как указано выше). Покажем, что p'_n/q'_n, p'_{n+1}/q'_{n+1} при достаточно большом n являются двумя последовательными наилучшими приближениями числа θ'.

Прежде всего заметим, что и $(p, q) = (p_n, q_n)$ и $(p, q) = (p_{n+1}, q_{n+1})$ удовлетворяют (6) при достаточно большом n и, значит, $q'_n > 0$, $q'_{n+1} > 0$. Аналогично $q'_{n+1} - q'_n > 0$ при достаточно большом n, так как тогда

$$(p, q) = (p_{n+1} - p_n, q_{n+1} - q_n)$$

удовлетворяет неравенству (6) и $q_{n+1} - q_n > 0$. Следовательно,

$$0 < q'_n < q'_{n+1}. \tag{7}$$

Согласно (2),

$$|q'_n\theta' - p'_n| = |t\theta' + u|\,|q_n\theta - p_n| >$$
$$> |t\theta' + u|\,|q_{n+1}\theta - p_{n+1}| = |q'_{n+1}\theta' - p'_{n+1}|. \tag{8}$$

Предположим теперь, что существует пара целых чисел (x', y'), такая, что

$$0 < y' < q'_{n+1}, \quad |y'\theta' - x'| \leqslant |q'_n\theta' - p'_n|. \tag{9}$$

Пусть паре (x, y) соответствует пара (x', y') по (3), (4). Как и при выводе (8), находим из (9), что

$$|y\theta - x| \leqslant |q_n\theta - p_n|. \tag{10}$$

Следовательно, и $(p, q) = (x, y)$ и $(p, q) = (p_{n+1} - x, q_{n+1} - y)$ удовлетворяют (6), если n достаточно велико, а тогда

$$0 < y < q_{n+1} \tag{11}$$

по (9) [ср. доказательство (7)]. Из (10) и (11) следует, что $(x, y) = (p_n, q_n)$, так как p_n/q_n, p_{n+1}/q_{n+1} — два последовательных наилучших приближения. Значит, $(x', y') = (p'_n, q'_n)$ является единственным целым решением неравенства (9). А это вместе с (7), (8) показывает, что p'_n/q'_n, p'_{n+1}/q'_{n+1} являются двумя последовательными наилучшими приближениями числа θ'.

При всех $n \geqslant$ некоторого N дроби p'_n/q'_n, взятые в соответствующем порядке, являются, таким образом, последовательными наилучшимип приближениями числа θ'. Но p'_n/q'_n — не обязательно n-е наилучшее приближение. Если $\theta = [a_1, a_2, \ldots]$, то

$$q'_{n+1} = rq_{n+1} - tp_{n+1} = a_n q'_n + q'_{n-1}.$$

Следовательно, при некоторых s и $b_1, \ldots, b_s$ число $\theta' = [b_1, \ldots, b_s, a_{N+1}, a_{N+2}, \ldots]$, что и требовалось доказать.

Для иррационального θ положим [1])

$$\nu(\theta) = \liminf q\,\|q\theta\|,$$

так что $0 \leqslant \nu(\theta) \leqslant 1$ по теореме I. Неравенство $q\,\|q\theta\| < \nu'$ имеет бесконечно много целых решений $q > 0$, если $\nu' > \nu(\theta)$, и только конечное число решений, если $\nu' < \nu(\theta)$. По (2.4) ясно, что

$$\nu(\theta) = \liminf q_n\,\|q_n\theta\|.$$

[1]) Обозначение „lim inf“ см. на стр. 8.

Следствие. *Если* θ *эквивалентно* θ', *то* $\nu(\theta)=\nu(\theta')$.

Доказательство. Положим, что существует бесконечно много решений неравенства

$$q\,|q\theta-p|<\varkappa \tag{12}$$

при некотором $\varkappa$ и пусть p', q' определяются по (3) и (4). Меняя ролями θ и θ' в (2), получаем

$$q'\theta'-p'=\pm\frac{q\theta-p}{r-t\theta},$$

где знак $\pm$ определяется из (1) и (4). Согласно этому равенству и равенству (5),

$$q'\,|q'\theta'-p'|\leqslant q\,|q\theta-p|+\frac{|t|}{|r-t\theta|}\,|q\theta-p|^2\leqslant$$
$$\leqslant\varkappa+\frac{|t|}{|r-t\theta|}\cdot\left(\frac{\varkappa}{q}\right)^2<\varkappa'$$

для любого фиксированного $\varkappa'>\varkappa$ при условии, что q достаточно велико. Значит,

$$q'\,|q'\theta'-p'|<\varkappa'$$

имеет бесконечно много решений для любого $\varkappa'>\varkappa$, а это значит, что $\nu(\theta')\leqslant\nu(\theta)$. Аналогично $\nu(\theta)\leqslant\nu(\theta')$.

Это следствие легко получается также из (2.15) и леммы 4.

§ 4. Применение к приближениям. С помощью непрерывных дробей легко доказывается следующая

Теорема V. *Пусть θ — иррациональное число. Тогда существует бесконечно много q, таких, что*

$$q\,\|q\theta\|<5^{-1/2}.$$

Если θ эквивалентно $1/2\left(5^{-1/2}-1\right)$, то постоянная $5^{-1/2}$ не может быть заменена никаким меньшим числом. Если же θ не эквивалентно $1/2\left(5^{1/2}-1\right)$, то существует бесконечно много q, таких, что

$$q\,\|q\theta\|<2^{-3/2}.$$

Доказательство. Мы можем ограничиться рассмотрением наилучших приближений. Обозначим

$$A_n=q_n\,\|q_n\theta\|.$$

По следствию 3 леммы 2 имеем $q_n\|q_{n-1}\theta\|+q_{n-1}\|q_n\theta\|=1$, и, таким образом,

$$\lambda^2 A_n-\lambda+A_{n-1}=0, \quad \lambda=\frac{q_{n-1}}{q_n}. \tag{1}$$

Аналогично

$$\mu^2 A_n-\mu+A_{n+1}=0, \quad \mu=\frac{q_{n+1}}{q_n}. \tag{2}$$

Здесь

$$\mu-\lambda=\frac{q_{n+1}-q_{n-1}}{q_n}=a_n. \tag{3}$$

Исключим λ, μ из (1), (2), (3). Для этого вычтем (2) из (1) и воспользуемся (3):

$$a_n A_n(\lambda+\mu)=a_n+A_{n-1}-A_{n+1}. \tag{4}$$

Возведем в квадрат (3) и (4) и сложим

$$2a_n^2A_n^2(\lambda^2+\mu^2)=a_n^4A_n^2+(a_n+A_{n-1}-A_{n+1})^2. \tag{5}$$

Наконец, складывая (1), (2) и используя (4), (5), получаем

$$a_n^2A_n^2+2A_n(A_{n-1}+A_{n+1})=1-a_n^{-2}(A_{n-1}-A_{n+1})^2\leqslant 1. \tag{6}$$

Наименьшее значение левой части (6) равно

$$(a_n^2+4)\min(A_{n-1}^2,\ A_n^2,\ A_{n+1}^2),$$

а потому или

$$\min(A_{n-1},\ A_n,\ A_{n+1})<5^{-1/2}, \tag{7}$$

или $a_n=1$, $A_{n-1}=A_n=A_{n+1}=5^{-1/2}$. Но вторая возможность не имеет места, так как из (1) следует, что рациональное число $\lambda=q_{n-1}/q_n$ равняется тогда иррациональному числу $1/2(5^{1/2}\pm 1)$. Итак, равенство (7) справедливо всегда.

Если $a_n\geqslant 2$, то аналогично

$$\min(A_{n-1},\ A_n,\ A_{n+1})<2^{-3/2}.$$

Таким образом, существует бесконечно много решений неравенства

$$A_n<2^{-3/2},$$

кроме, быть может, случая, когда $a_n = 1$ (все $n \geqslant$ некоторого N). Эти исключительные θ, согласно теореме IV, эквивалентны

$$\xi = [1,\ 1,\ 1,\ \ldots].$$

Так как $\xi^{-1} = 1 + \xi$ и $0 < \xi < 1$, то

$$\xi = \frac{5^{1/2} - 1}{2}.$$

Остается только проверить, что если $\theta = \xi$ и $\varkappa < 5^{-1/2}$, то существует лишь конечное число решений неравенства $q\|q\theta\| < \varkappa$. Мы можем ограничиться рассмотрением наилучших приближений p_n/q_n. По (2.15)

$$q_n\|q_n\theta\| = (1 + \theta_{n+1} + \varphi_{n-1})^{-1},$$

где

$$\theta_{n+1} = [1,\ 1,\ \ldots] = \xi$$

и

$$\varphi_{n-1} = [\underbrace{1,\ \ldots,\ 1}_{n-1 \text{ знаков}}] \to \xi \qquad (n \to \infty)$$

по лемме 4. Следовательно,

$$q_n\|q_n\theta\| \to (1 + 2\xi)^{-1} = 5^{-1/2},$$

что и требовалось доказать.

В следующей главе мы докажем другими средствами утверждение более сильное, чем в теореме V.

§ 5. Совместные приближения. Иногда бывает желательно аппроксимировать множество чисел $\theta_1, \ldots, \theta_n$ дробями

$$\frac{p_1}{q}, \ \ldots, \ \frac{p_n}{q}$$

с общим знаменателем q, или, что то же самое, сделать $\|q\theta_1\|, \ldots, \|q\theta_n\|$ одновременно малыми. На этот счет имеется один вполне общий результат.

Теорема VI. *Пусть даны n линейных форм с m переменными:*

$$L_j(\mathbf{x}) = \sum_i \theta_{ji} x_i \qquad (1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n).$$

Тогда для каждого действительного $X > 1$ *существует целый вектор* $\mathbf{x} \neq \mathbf{0}$, *такой, что*

$$\|L_j(\mathbf{x})\| < X^{-m/n}, \quad |x_i| \leqslant X \qquad (1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n).$$

Доказательство. Как и во втором доказательстве теоремы I, достаточно найти целые $x_1, \ldots, x_m, y_1, \ldots, y_n$, не равные одновременно нулю, такие, что

$$|L_j(\mathbf{x}) - y_j| < X^{-m/n} \qquad (1 \leqslant j \leqslant n),$$

$$|x_i| \leqslant X \quad (1 \leqslant i \leqslant m).$$

Детерминант этой системы из $m+n$ линейных форм с $m+n$ переменными равен 1, а так как произведение правых частей тоже равно 1, то теорема VI следует из теоремы Минковского о линейных формах (теорема III приложения В).

В частности, беря $m = 1$, получаем

$$q^{1/n} \max(\|q\theta_1\|, \ldots, \|q\theta_n\|) < 1$$

для бесконечного числа целых $q > 0$. Этот результат может быть несколько улучшен.

Теорема VII. *Существует бесконечно много целых решений неравенства*

$$q^{1/n} \max(\|q\theta_1\|, \ldots, \|q\theta_n\|) < \frac{n}{n+1}.$$

Замечание. Как мы уже видели, если $n = 1$, то дробь $n/(n+1) = 1/2$ может быть заменена числом $5^{-1/2}$, но не меньшим. Наилучшие постоянные при $n > 1$ не известны.

Доказательство. Возьмем произвольное $t > 1$. По теореме IV приложения В существуют целые $x_1, \ldots, x_n, y$, не равные нулю одновременно, такие, что

$$t^{-n}|y| + t|\theta_j y_j - x_j| \leqslant (n+1)^{1/(n+1)} \qquad (1 \leqslant j \leqslant n), \quad (1)$$

так как определяемая этими неравенствами $(n+1)$-мерная область имеет объем 2^{n+1} [в чем легко убедиться, полагая $z_j = t(\theta_j y - x_j)$ $(1 \leqslant j \leqslant n)$; $z_{n+1} = t^{-n} y$]. Далее, если $y = 0$, то и $x_1 = \ldots = x_n = 0$ при достаточно большом t и, значит, можно считать, что $y > 0$. Тогда, пользуясь тем, что среднее арифметическое не меньше среднего геометрического, из неравенства (1) получаем $y^{1/n}|\theta_j y - x_j| \leqslant \leqslant n/(n+1)$, записав сперва левую часть (1) в виде

$$t^{-n}y + \underbrace{n^{-1}t|\theta_j y - x_j| + \ldots + n^{-1}t|\theta_j y - x_j|}_{n \text{ слагаемых}}.$$

Наконец, если хотя бы одно из чисел $\theta_1, \ldots, \theta_n$ иррационально, то при $t \to \infty$ получаем бесконечно много различных решений. Если все $\theta_1, \ldots, \theta_n$ — рациональные числа, то существует целое $Q > 0$, такое, что все $Q\theta_j$ — целые. Тогда все положительные кратные q числа Q, очевидно, удовлетворяют условиям теоремы.

Существует аналог теоремы VII для

$$u^n \| u_1\theta_1 + \ldots + u_n\theta_n \|; \quad u = \max(|u_1|, \ldots, |u_n|),$$

где $\theta_1, \ldots, \theta_n$ заданы, а $u_1, \ldots, u_n$ — целые, не все равные нулю.

Теорема VI в некотором смысле не улучшаема. Это видно из следующей теоремы, для доказательства которой необходимы некоторые знания из алгебраической теории чисел. Однако результаты конца этой главы в дальнейшем не потребуются. Другое доказательство в случае, когда $m = 1$ или $n = 1$, см. в гл. V, теорема III.

Теорема VIII. *Для любых целых положительных m, n существуют постоянная $\gamma > 0$ и линейные формы $L_j(\mathbf{x})$ $(1 \leqslant j \leqslant n)$, такие, что*

$$\left(\max_i |x_i|\right)^m \left(\max_j \|L_j(\mathbf{x})\|\right)^n \geqslant \gamma$$

при всех целых $\mathbf{x} = (x_1, \ldots, x_m) \neq \mathbf{0}$.

Доказательство. Положим $l = m + n$ (> 1). Существуют системы действительных сопряженных алгебраических целых $\varphi_1, \ldots, \varphi_l$ степени l (см. ниже). Обозначим

$$Q_k(\mathbf{x}, \mathbf{y}) = \sum_{j=1}^{n} \varphi_k^{j-1} y_j + \sum_{i=1}^{m} \varphi_k^{n+i-1} x_i \qquad (1 \leqslant k \leqslant l). \qquad (2)$$

При целых $\mathbf{x}$, $\mathbf{y}$, не равных одновременно нулю, $Q_k(\mathbf{x}, \mathbf{y})$ — сопряженные алгебраические целые, не равные нулю.

В частности, $\prod_k Q_k(\mathbf{x}, \mathbf{y})$ — целое рациональное, отличное от нуля. Поэтому

$$\prod_k |Q_k(\mathbf{x}, \mathbf{y})| \geqslant 1. \tag{3}$$

Но при $k = 1, 2, \ldots, n$ равенства (2) можно записать в виде

$$Q_k(\mathbf{x}, \mathbf{y}) = \sum_{j=1}^{n} \varphi_k^{j-1}(y_j - L_j(\mathbf{x})) \quad (k \leqslant n), \tag{4}$$

где $L_j(\mathbf{x})$ — некоторые линейные формы. В самом деле, чтобы найти $L_j(\mathbf{x})$, можно приравнять $Q_1, \ldots, Q_n$ к нулю и полученную систему решить относительно $y_1, \ldots, y_n$, которые будут зависеть от $\mathbf{x}$. При $k > n$ имеем

$$Q_k(\mathbf{x}, \mathbf{y}) = \sum_{j=1}^{n} \varphi_k^{j-1}(y_j - L_j(\mathbf{x})) + \sum_{i=1}^{m} \omega_{ki} x_i \quad (k > n), \tag{5}$$

где ω_{ki} — некоторые постоянные.

Пусть теперь $\mathbf{x} \neq \mathbf{0}$ — целый вектор и положим

$$X = \max_i |x_i|, \quad C = \max_j \|L_j(\mathbf{x})\|.$$

Пусть $y_1, \ldots, y_n$ — целые, такие, что

$$\|L_j(\mathbf{x})\| = |L_j(\mathbf{x}) - y_j|.$$

Тогда по (4)

$$|Q_k(\mathbf{x}, \mathbf{y})| \leqslant \gamma_1 C \quad (k \leqslant n), \tag{6}$$

где γ_1 (как и $\gamma_2, \ldots$ ниже) зависит только от φ_k, но не от $\mathbf{x}$. Аналогично по (5)

$$|Q_k(\mathbf{x}, \mathbf{y})| \leqslant \gamma_2 C + \gamma_3 X \leqslant \gamma_4 X \quad (k > n), \tag{7}$$

так как $C < 1 \leqslant X$. Из (6), (7) имеем

$$\left|\prod_k Q_k(\mathbf{x}, \mathbf{y})\right| \leqslant \gamma_1^n \gamma_4^m C^n X^m. \tag{8}$$

Выбрав $\gamma = \gamma_1^{-n} \gamma_4^{-m}$, получим из (3) и (8) утверждение теоремы.

[В качестве φ_j можно взять корни уравнения

$$(\varphi - a_1 q) \ldots (\varphi - a_l q) - 1 = 0, \tag{9}$$

где $a_1, \ldots, a_l$ — любые различные целые рациональные и q достаточно велико. При достаточно большом q это уравнение имеет l действительных корней φ_k, где

$$0 < |\varphi_k - a_k q| < K_1 q^{-l+1}, \tag{10}$$

и K_1 (как и K_2 ниже) зависит от $a_1, \ldots, a_l$, но не от q. Ясно, что φ_k — целые алгебраические. Если бы они были не все сопряженные, то после соответствующей перестановки $a_1, \ldots, a_l$ мы могли бы считать, что

$$\varphi_1, \ldots, \varphi_L \quad (L < l)$$

есть система сопряженных. Значит, $\prod\limits_{\lambda \leqslant L} (a_1 q - \varphi_\lambda)$ было бы целым рациональным. Но по (10), при достаточно большом q,

$$0 < \left| \prod_{\lambda \leqslant L} (a_1 q - \varphi_\lambda) \right| < K_2 q^{L-l} < 1,$$

что невозможно[1]).]

ЗАМЕЧАНИЯ

§ 1. Другое доказательство теоремы I опирается на ряды Фарея (Харди и Райт (1938), гл. III).

§ 2. Рассмотренные непрерывные дроби называются „регулярными“ непрерывными дробями. Они обладают двумя полезными свойствами: 1) последовательность чисел a_n, связывающих последовательные подходящие дроби, совершенно произвольна, 2) подходящие дроби p_n/q_n характеризуются простым внутренним свойством — свойством существования „наилучшего приближения“. Никакой другой алгоритм непрерывных дробей не обладает обоими свойствами. Например, „диагональные непрерывные дроби“ не обладают первым свойством, а „непрерывные дроби, построенные до ближайшего целого“, не обладают вторым свойством.

---

[1]) Этим доказана неприводимость уравнения (9) при достаточно большом q. — *Прим. перев.*

Вся схема рассуждений может быть перенесена и на произведение $\xi\eta$ двух линейных форм: $\xi = \alpha x + \beta y$ и $\eta = \gamma x + \delta y$ (α, β, γ, δ — действительные числа, x, y пробегают все целые числа). Пара целых чисел x_n, y_n дает „наилучшее приближение“, если не существует решения в целых числах $(x, y) \neq (0, 0)$ неравенств

$$|\xi(x, y)| < |\xi(x_n, y_n)|, \quad |\eta(x, y)| < |\eta(x_n, y_n)|.$$

Некоторые авторы берут p_{n-1}, q_{n-1} вместо наших p_n, q_n. Однако наше обозначение допускает бо́льшую симметрию между формами ξ, η в только что рассмотренном обобщении; эта симметрия отражается в симметрии равенства (2.15) относительно θ_{n+1} и φ_{n-1}.

Два более обширных изложения теории с различных точек зрения см. у Хинчина (1935) и Перрона (1913), а распространение на квадратичные поля см. у Пуату (1953).

§ 4. Это доказательство принадлежит проф. Давенпорту. „Асимметрическое“ обобщение см. у Сегре (1945), Барнса и Суиннертона-Дайера (1955), Торнхейма (1955).

§ 5. Современное состояние вопроса освещено у Давенпорта (1954).

Глава II

ЦЕПОЧКИ МАРКОВА[1])

§ 1. Введение. Как показал Марков, теорема V гл. I поддается расширению. Для всех иррациональных θ неравенство

$$q\|q\theta\| < 5^{-1/2} \tag{1}$$

имеет бесконечно много решений. Если θ эквивалентно $\frac{1}{2}(5^{1/2} - 1) = \theta_1$, т. е. корню уравнения

$$\theta_1^2 + \theta_1 - 1 = 0, \tag{2}$$

то постоянная $5^{-1/2}$ не может быть улучшена. Если же θ не эквивалентно θ_1, то существует бесконечно много решений неравенства

$$q\|q\theta\| < 2^{-3/2}, \tag{3}$$

где постоянная опять не может быть улучшена, если θ эквивалентно корню уравнения

$$\theta_2^2 + 2\theta_2 - 1 = 0. \tag{4}$$

В противном случае существует бесконечно много решений неравенства

$$q\|q\theta\| < \frac{5}{(221)^{1/2}}, \tag{5}$$

где постоянная не может быть улучшена для θ, эквивалентного корню уравнения

$$5\theta_3^2 + 11\theta_3 - 5 = 0. \tag{6}$$

---

[1]) Результаты этой главы нигде в дальнейшем не используются. Поэтому при первом чтении ее можно опустить.

Если же θ не эквивалентно корням уравнений (2), (4) и (6), то опять существует бесконечно много решений неравенства

$$q\|q\theta\| < \frac{13}{(1517)^{1/2}}, \tag{7}$$

где постоянная не может быть улучшена для θ, эквивалентного корню уравнения

$$13\theta_4^2 + 29\theta_4 - 13 = 0. \tag{8}$$

И так до бесконечности. Последовательность чисел $5^{-1/2}$, $2^{-3/2}$, $5/(221)^{1/2}$, $13/(1517)^{1/2}$, ... сходится к $1/3$.

Оказывается, существует тесно связанная с этим цепь теорем, относящихся к *неопределенным квадратичным формам*, т. е. к выражениям вида

$$f(x, y) = \alpha x^2 + \beta xy + \gamma y^2, \tag{9}$$

представляющимся произведением двух различных линейных действительных форм. Тогда *дискриминант*

$$\delta(f) = \delta = \beta^2 - 4\alpha\gamma \tag{10}$$

строго положителен. Две квадратичные формы, $f(x, y)$, $f'(x, y)$, называются *эквивалентными*, если существуют целые a, b, c, d, такие, что

$$\left.\begin{aligned} f'(ax + by,\ cx + dy) &= f(x, y), \\ ad - bc &= \pm 1 \end{aligned}\right\} \tag{11}$$

тождественно относительно x, y. Очевидно, соотношение эквивалентности симметрично относительно форм f и f'. Далее, легко показать, что если f эквивалентна f', а f' эквивалентна f'', то f эквивалентно f''. Таким образом, мы имеем обычное понятие эквивалентности. Нетрудно показать, что две эквивалентные формы имеют равные дискриминанты.

Эквивалентность форм связана с ранее введенной эквивалентностью действительных чисел. Если $f(\theta, 1) = 0$ и (11) имеет место, то

$$f'(a\theta + b,\ c\theta + d) = f(\theta, 1) = 0,$$

т. е. $f'(\theta', 1) = 0$, где $\theta' = (a\theta + b)/(c\theta + d)$. Таким образом, число θ эквивалентно одному из корней уравнения $f'(\theta', 1) = 0$;

Обозначим [1])

$$\mu(f) = \inf |f(x, y)|$$

(x, y — целые, не равные одновременно нулю).

Так как по (11) две эквивалентные формы принимают одинаковые значения, когда x, y пробегают все целые числа, то

$$\mu(f) = \mu(f') \quad (f' \text{ эквивалентна } f).$$

Далее, если $\lambda \neq 0$ — действительное число, то

$$\mu(\lambda f) = |\lambda| \mu(f), \quad \delta(\lambda f) = \lambda^2 \delta(f).$$

Значит, $\mu(f)\delta^{-1/2}(f)$ не изменится при замене f эквивалентной формой или при умножении f на постоянную.

Теперь имеется следующая цепочка теорем:

$$\mu(f) \leqslant 5^{-1/2} \delta^{1/2}(f),$$

где знак равенства имеет место только для форм, эквивалентных кратному формы $x^2 + xy - y^2$. В противном случае

$$\mu(f) \leqslant 2^{-3/2} \delta^{1/2}(f),$$

где равенство имеет место только для форм, эквивалентных кратному формы $x^2 + 2xy - y^2$ и т. д. Числа $5^{-1/2}$, $2^{-3/2}$, ... — те же, что и в цепочке теорем о приближениях; и если формы здесь обозначаются через $f(x, y)$, то θ в теореме о приближении определяется уравнением $f(\theta, 1) = 0$.

Цепочку теорем для форм доказать значительно легче, если предположить, что $\mu(f)$ *достигается*, т. е. что существуют целые x_0, y_0, такие, что

$$|f(x_0, y_0)| = \mu(f).$$

Если считать, что в этом специальном случае цепочка теорем для форм доказана, то можно получить общими техническими приемами („изоляция") и цепочку теорем для форм в общем случае и цепочку для приближений.

В § 2 мы рассмотрим теорию квадратичных форм и ее связь с приближениями. В частности, мы докажем теорему, на которую опирается техника изоляции. В § 3, 4 мы определяем

[1]) Обозначение „inf" см. на стр. 8.

и исследуем специальные квадратичные формы, которые встречаются в цепочках теорем. Наконец, в § 5, 6 мы формулируем и доказываем две цепочки теорем.

§ 2. Неопределенные бинарные квадратичные формы. В этом параграфе под

$$f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$$

понимается неопределенная квадратичная форма с дискриминантом

$$\delta = \beta^2 - 4\alpha\gamma > 0.$$

Обозначим через θ, φ корни уравнения $f(x, 1) = 0$. Тогда

$$f(x, y) = \alpha L(x, y) M(x, y),$$

где

$$L(x, y) = x - \theta y, \quad M(x, y) = x - \varphi y$$

и

$$|\alpha(\theta - \varphi)| = \delta^{1/2}.$$

Лемма 1. *Предположим, что существуют целые взаимно простые числа a, b, такие, что $f(a, b) = \alpha' \neq 0$. Тогда найдутся целые c, d, удовлетворяющие условию $ad - bc = 1$, для которых*

$$f(ax + cy, bx + dy) = \alpha' x^2 + \beta' xy + \gamma' y^2,$$

где

$$|\beta'| \leqslant |\alpha'|.$$

Доказательство. Так как a, b — взаимно простые, то найдутся целые числа c', d', удовлетворяющие условию $ad' - bc' = 1$. Тогда

$$f(ax + c'y, bx + d'y) = \alpha' x^2 + \beta'' xy + \gamma'' y^2$$

при некоторых β'', γ''. Всегда найдется целое n, такое, что

$$|\beta'' + 2n\alpha'| \leqslant |\alpha'|.$$

Очевидно, $c = c' + na$, $d = d' + nb$ обеспечивают справедливость леммы 1.

Следствие. *Если $\alpha' > 0$, то $f(x, y)$ эквивалентна форме $\alpha' x^2 + \beta''' xy + \gamma''' y^2$, причем $2\alpha' \leqslant \beta''' \leqslant 3\alpha'$.*

Доказательство. Обозначим $\alpha' x^2 + \beta' xy + \gamma' y^2 = f'(x, y)$. Если $\beta' \geqslant 0$, то берем $f'(x+y, y)$; если $\beta' < 0$, то берем $f'(x+y, -y)$.

Лемма 2 (лемма о компактности). *Пусть*

$$f_j(x, y) = \alpha_j x^2 + \beta_j xy + \gamma_j y^2 \quad (1 \leqslant j < \infty).$$

Предположим, что при всех достаточно больших j

$$0 < K_1 \leqslant |\alpha_j| \leqslant K_2, \quad |\beta_j| \leqslant K_3 |\alpha_j|,$$

где K_1, K_2, K_3 не зависят от j. Предположим, что

$$\lim (\beta_j^2 - 4\alpha_j \gamma_j) = \delta$$

существует. Тогда найдется подпоследовательность $f_{j_s}(x, y)$, сходящаяся к пределу $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$ в том смысле, что

$$\alpha_{j_s} \to \alpha, \quad \beta_{j_s} \to \beta, \quad \gamma_{j_s} \to \gamma.$$

Кроме того,

$$\beta^2 - 4\alpha\gamma = \delta.$$

Доказательство. Из условий леммы следует, что для достаточно больших j

$$|\beta_j| \leqslant K_4, \quad |\gamma_j| \leqslant K_5,$$

где K_4, K_5 не зависят от j. Поэтому точки $P_j(\alpha_j, \beta_j, \gamma_j)$ лежат в ограниченной области 3-мерного эвклидова пространства. Следовательно, должна существовать последовательность точек P_{j_s}, сходящаяся к предельной точке, скажем, $P(\alpha, \beta, \gamma)$. Ясно, что α, β, γ обеспечивают справедливость леммы.

Следствие. *Если α_j, β_j, γ_j — целые, то существует бесконечно много j, для которых $f_j(x, y) = f(x, y)$.*

Доказательство очевидно.

Лемма 3. *Пусть α, β, γ — рациональные числа, такие, что θ, φ — иррациональные (т. е. δ не является точным квадратом). Тогда при некотором η $(0 < \eta < 1)$ и целых a, b, c, d, удовлетворяющих условию $ad - bc = 1$, имеем тождественно*

$$L(ax + by, cx + dy) = \eta L(x, y),$$
$$M(ax + by, cx + dy) = \eta^{-1} M(x, y).$$

Доказательство[1]). Не ограничивая общности, можно считать числа α, β, γ целыми. Только для доказательства данной леммы будем обозначать $\mathbf{x}=(x, y)$; и если $\mathbf{S}=\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ — квадратная матрица, то обозначим $\mathbf{xS}=(ax+by, cx+dy)$. Матрицы $\mathbf{S}$ с целыми a, b, c, d и $ad-bc=1$ образуют группу, т. е. если $\mathbf{S}_1$, $\mathbf{S}_2$ — матрицы указанного вида, то $\mathbf{S}_1\mathbf{S}_2$ и $\mathbf{S}_1^{-1}$ — матрицы такого же вида.

По теореме III приложения В для любого $\varepsilon>0$ существует целый вектор $\mathbf{x}^{(1)}=(x_1, y_1)\neq\mathbf{0}$, такой, что

$$|L(\mathbf{x}^{(1)})|<\varepsilon, \quad |M(\mathbf{x}^{(1)})|\leqslant|\theta-\varphi|\varepsilon^{-1}.$$

Следовательно,

$$|f(\mathbf{x}^{(1)})|=|\alpha L(\mathbf{x}^{(1)})M(\mathbf{x}^{(1)})|<|\alpha(\theta-\varphi)|.$$

Без ограничения общности можно считать x_1, y_1 взаимно простыми. Но $L(\mathbf{x}^{(1)})\neq 0$, так как θ иррационально. Устремляя ε к нулю, получаем бесконечную последовательность векторов $\mathbf{x}^{(r)}=(x_r, y_r)$ со взаимно простыми координатами, для которых

$$|f(\mathbf{x}^{(r)})|<|\alpha(\theta-\varphi)|, \quad L(\mathbf{x}^{(r)})\to 0,$$

Взяв в случае необходимости $-\mathbf{x}^{(r)}$ вместо $\mathbf{x}^{(r)}$, будем иметь

$$L(\mathbf{x}^{(r)})>0, \quad L(\mathbf{x}^{(r)})\to 0. \tag{1}$$

По лемме 1 существует матрица $\mathbf{S}_r=\begin{pmatrix} x_r & y_r \\ z_r & t_r \end{pmatrix}$ с целыми z_r, t_r и $x_rt_r-z_ry_r=1$, такая, что

$$f(\mathbf{xS}_r)=\alpha_r x^2+\beta_r xy+\gamma_r y^2, \qquad \alpha_r=f(\mathbf{x}^{(r)}),$$

где $|\beta_r|\leqslant|\alpha_r|$, $\beta_r^2-4\alpha_r\gamma_r=\beta^2-4\alpha\gamma$ и $1\leqslant|\alpha_r|<|\alpha(\theta-\varphi)|$, так как $f(\mathbf{x}^{(r)})$ — целое, не равное нулю. По следствию из леммы 2 можно считать, взяв вместо последовательности матриц $\mathbf{S}_r$ ее подпоследовательность, что, скажем,

$$f(\mathbf{xS}_r)=\varphi(\mathbf{x}) \tag{2}$$

[1]) Применительно к цепочкам Маркова a, b, c, d можно всегда выписать явно. Мы формулируем общую теорему существования так, чтобы можно было высказать лемму 4 и теорему I в самом общем виде.

не зависит от r. Пусть $\varphi(\mathbf{x}) = \lambda(\mathbf{x})\,\mu(\mathbf{x})$ — какое-нибудь разложение на произведение линейных множителей. С другой стороны,

$$\varphi(\mathbf{x}) = f(\mathbf{x}\mathbf{S}_r) = \alpha L(\mathbf{x}\mathbf{S}_r)\, M(\mathbf{x}\mathbf{S}_r).$$

Следовательно, для каждого r тождественно относительно $\mathbf{x}$ или

$$L(\mathbf{x}\mathbf{S}_r) = \nu_r \lambda(\mathbf{x}), \quad M(\mathbf{x}\mathbf{S}_r) = \pi_r \mu(\mathbf{x}), \tag{3}$$

или

$$L(\mathbf{x}\mathbf{S}_r) = \nu_r \mu(\mathbf{x}), \quad M(\mathbf{x}\mathbf{S}_r) = \pi_r \lambda(\mathbf{x})$$

при некоторых действительных ν_r, π_r. Взяв опять подпоследовательность и, в случае необходимости, поменяв ролями $\lambda(\mathbf{x})$, $\mu(\mathbf{x})$, можно считать, что всегда имеют место равенства (3).

По определению, $(1, 0)\,\mathbf{S}_r = \mathbf{x}^{(r)}$. Следовательно, полагая в (3) $\mathbf{x} = (1, 0)$ и используя (1), получаем

$$0 < \nu_r/\nu_1 = L(\mathbf{x}^{(r)})/L(\mathbf{x}^{(1)}) \to 0 \quad (r \to \infty).$$

Положим $\eta = \nu_r/\nu_1$, $\mathbf{T} = \mathbf{S}_1^{-1}\mathbf{S}_r$, где r настолько велико, что $0 < \eta < 1$. Тогда

$$f(\mathbf{x}\mathbf{T}) = \varphi\left(\mathbf{x}\mathbf{S}_1^{-1}\right) = f(\mathbf{x}), \tag{4}$$

согласно (2), где вместо $\mathbf{x}$ берется $\mathbf{x}\mathbf{S}_1^{-1}$. Аналогично из (3) имеем

$$L(\mathbf{x}\mathbf{T}) = \nu_r \lambda\left(\mathbf{x}\mathbf{S}_1^{-1}\right) = \eta L(\mathbf{x}).$$

Наконец, согласно (4), $M(\mathbf{x}\mathbf{T}) = \eta^{-1} M(\mathbf{x})$, так как $f(\mathbf{x}\mathbf{T}) = \alpha L(\mathbf{x}\mathbf{T})\, M(\mathbf{x}\mathbf{T})$. Этим самым лемма доказана при $\mathbf{T} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$.

Следствие. *Пусть x_0, y_0, n — любые целые числа. Тогда существуют целые x_1, y_1, такие, что $f(x_1, y_1) = f(x_0, y_0)$ и*

$$L(x_1, y_1) = \eta^n L(x_0, y_0), \quad M(x_1, y_1) = \eta^{-n} M(x_0, y_0).$$

Доказательство. Для $n > 0$ и для $\mathbf{T}$, полученного в предыдущем доказательстве, имеем

$$L\left(\mathbf{x}\mathbf{T}^n\right) = \eta L\left(\mathbf{x}\mathbf{T}^{n-1}\right) = \ldots = \eta^n L(\mathbf{x}),$$
$$M\left(\mathbf{x}\mathbf{T}^n\right) = \ldots \qquad\qquad = \eta^{-n} M(\mathbf{x}).$$

Заменяя $\mathbf{x}$ на $\mathbf{xT}^{-1}$ в $L(\mathbf{xT}) = \eta L(\mathbf{x})$, получаем

$$L\left(\mathbf{x}\ \ ^{-1}\right) = \eta^{-1} L(\mathbf{x})$$

и аналогично

$$L\left(\mathbf{xT}^{n}\right) = \eta^{n} L(\mathbf{x}), \quad M\left(\mathbf{xT}^{n}\right) = \eta^{-n} M(\mathbf{x})$$

при $n < 0$. Полагая $(x_1, y_1) = (x_0, y_0)\,\mathbf{T}^n$, получаем доказательство следствия.

Лемма 4. *Предположим, что* θ *иррационально и является корнем уравнения*

$$f(\theta, 1) = 0.$$

Как и ранее, положим $\nu = \nu(\theta) = \liminf q\|q\theta\|$ *и*

$$\mu = \mu(f) = \inf|f(x, y)|$$

(x, y — *целые, не равные нулю одновременно*).

Тогда

A. $$\nu(\theta) \geqslant \delta^{-1/2}\mu(f), \tag{5}$$

каковы бы ни были α, β, γ (*рациональные или иррациональные*).

B. *Если* α, β, γ — *рациональные, то в* (5) *всегда имеет место знак равенстза и* $\mu(f)$ *достигается.*

C. *Если, кроме того,* $f(x, y)$ *принимает оба значения* $\pm\mu$ *для целых значений переменных, то существует бесконечно много целых* q, *таких, что*

$$q\|q\theta\| < \nu.$$

Доказательство. Доказательство опирается на очевидное тождество

$$\begin{aligned} f(p, q) &= \alpha(p - \theta q)(p - \varphi q) = \\ &= \alpha(\theta - \varphi)\,q\,(p - \theta q) + \alpha(p - \theta q)^2. \end{aligned} \tag{6}$$

Предположим сначала, что ν' — любое число $> \nu$. Тогда обязательно существуют решения неравенства $q\,|q\theta - p| < \nu'$ с произвольно большим q. Поэтому из (6) следует

$$|f(p, q)| \leqslant |\alpha|\,|\theta - \varphi|\,\nu' + |\alpha|\,\nu'^2 q^{-2}.$$

Но

$$|f(p, q)| \geqslant \mu \quad \text{и} \quad |\alpha(\theta - \varphi)| = \delta^{1/2}.$$

Значит,

$$\mu \leqslant \nu' \delta^{1/2} + |\alpha| \nu'^2 p^{-2}.$$

Следовательно, $\mu \leqslant \nu\delta^{1/2}$, так как q сколь угодно велико, а ν' — любое число $> \nu$. Это и доказывает утверждение A.

Если α, β, γ — рациональные, то существует целое h, такое, что $hf(x, y)$ — всегда целое при целых x, y. Таким образом, $|hf(x, y)|$ должно достигать своей нижней грани, т. е. $|f(p, q)| = \mu$ при целых p, q. По следствию из леммы 3 существуют целые p, q, для которых $|q\theta - p|$ произвольно мало. Результат $\mu \geqslant \nu\delta^{1/2}$, а значит, и утверждение B получаются путем обращения предыдущих рассуждений.

Наконец, если $f(x, y)$ принимает оба значения $\pm\mu$, то существуют целые $q > 0$, p, такие, что $f(p, q)$ имеет одно из двух значений $\pm\mu$ и $|q\theta - p|$ произвольно мало. Тогда при подходящем выборе знака

$$\mu = |f(p, q)| > |\alpha(\theta - \varphi) q (\theta q - p)|,$$

так как второй член справа в (6) имеет всегда тот же знак, что и α, а по абсолютной величине он меньше, чем $|f(p, q)| = \mu$, если $|q\theta - p|$ достаточно мало. Это и доказывает утверждение C.

Теорема I („теорема изоляции“, Ремак, Роджерс). *Предположим, что $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$, где α, β, γ — рациональные, но корни θ, φ уравнения $f(x, 1) = 0$ — иррациональные. Пусть $\mu > 0$ есть минимум $|f(x, y)|$ при целых x, y, не равных одновременно нулю. Предположим, далее, что оба уравнения*

$$f(x, y) = \pm\mu \tag{7}$$

разрешимы в целых числах. Тогда существуют числа $\mu' < \mu$ и $\varepsilon_0 > 0$, зависящие только от α, β, γ, обладающие следующим свойством.

Пусть

$$f^*(x, y) = \alpha^*(x - \theta^* y)(x - \varphi^* y) \tag{8}$$

— любая квадратичная форма, для которой

$$|\alpha - \alpha^*| < \varepsilon_0, \quad |\theta - \theta^*| < \varepsilon_0, \quad |\varphi - \varphi^*| < \varepsilon_0. \tag{9}$$

Тогда существуют целые x_0, y_0, не равные одновременно нулю, такие, что

$$|f^*(x_0, y_0)| < \mu' \tag{10}$$

при условии, что f^* не имеет вида λf при постоянном λ.

Замечание 1. Фактически теорема утверждает, что все „достаточно близкие“ к f формы, кроме форм, кратных f, имеют несколько меньший минимум. Последнее условие существенно, так как минимум формы λf равен $|\lambda|\mu$, а λ может быть как угодно близко к 1.

Замечание 2. Реальное ограничение состоит в том, что оба уравнения $f(x, y) = \pm\mu$ должны быть разрешимы. Таким образом, теорема не применима к $x^2 - 3y^2$.

Доказательство. Без ограничения общности считаем α, β, γ целыми. Если $\theta^* = \theta$, $\varphi^* = \varphi$, то f^* кратно f. Следовательно, можно предполагать, в силу симметрии, что

$$\theta^* \neq \theta, \quad \alpha > 0. \tag{11}$$

По условию существуют целые x_1, y_1, x_2, y_2, такие, что

$$f(x_1, y_1) = \mu, \quad f(x_2, y_2) = -\mu,$$

и, изменив в случае необходимости знак, можно считать, пользуясь обозначениями, введенными на стр. 32, что

$$L_1 = L(x_1, y_1) > 0, \quad M_1 = M(x_1, y_1) > 0, \quad \alpha L_1 M_1 = \mu; \tag{12}$$

$$L_2 = L(x_2, y_2) > 0, \quad M_2 = M(x_2, y_2) < 0, \quad \alpha L_2 M_2 = -\mu. \tag{13}$$

Обозначим через c_1, c_2, ... положительные постоянные, зависящие только от α, β, γ, L_1, M_1, L_2, M_2, η, где η — число, о котором говорится в лемме 3, т. е. в конечном счете постоянные c_1, c_2, ... зависят только от α, β, γ. Пусть μ' — любое число, такое, что

$$\mu > \mu' > \mu(1 - \eta^2). \tag{14}$$

Достаточно будет показать, что требуемые x_0, y_0 существуют при условии, что ε_0 меньше некоторого числа, зависящего только от α, β, γ и μ'.

Обозначим

$$L^*(x, y) = x - \theta^* y, \quad M^* = x - \varphi^* y, \tag{15}$$

так что

$$L^* = (1 - \rho) L + \rho M, \quad M^* = \sigma L + (1 - \sigma) M, \tag{16}$$

где

$$\rho = \frac{\theta^* - \theta}{\varphi - \theta}, \quad \sigma = \frac{\varphi^* - \varphi}{\theta - \varphi}. \tag{17}$$

В частности,

$$0 < |\rho| < c_1\varepsilon_0, \quad |\sigma| < c_1\varepsilon_0. \tag{18}$$

Первый случай, $\rho \leqslant 0$. Определим целое n из неравенства

$$\eta^{2n} \geqslant \frac{-\rho M_1}{(1-\rho) L_1} > \eta^{2(n+1)}, \tag{19}$$

так что

$$0 < \eta^{2n} < c_2\varepsilon_0. \tag{20}$$

Выберем теперь целые x_0, y_0 согласно следствию леммы 3, так что

$$L_0 = L(x_0, y_0) = \eta^n L_1, \quad M_0 = M(x_0, y_0) = \eta^{-n} M_1. \tag{21}$$

Соответствующие значения $L_0^* = L^*(x_0, y_0)$, $M_0^* = M^*(x_0, y_0)$ получаются из (16). Следовательно, по (19), (20), (21) они удовлетворяют неравенствам

$$\begin{aligned} 0 \leqslant \eta^{-n} L_0^* = (1-\rho) L_1 + \rho\eta^{-2n} M_1 \leqslant (1-\rho)(1-\eta^2) L_1 \leqslant \\ \leqslant (1 + c_1\varepsilon_0)(1-\eta^2) L_1 \end{aligned} \tag{22}$$

и

$$\begin{aligned} |\eta^n M_0^*| \leqslant |\sigma| \eta^{2n} |L_1| + (1+|\sigma|)|M_1| \leqslant \\ \leqslant c_3\varepsilon_0^2 + (1 + c_1\varepsilon_0)|M_1| \leqslant (1 + c_4\varepsilon_0)|M_1|. \end{aligned} \tag{23}$$

Тогда по (9), (11), (22), (23)

$$\begin{aligned} |f^*(x_0, y_0)| &= |\alpha^* L_0^* M_0^*| \leqslant \\ &\leqslant (\alpha + \varepsilon_0)(1 + c_1\varepsilon_0)(1 + c_4\varepsilon_0)(1-\eta^2)|L_1 M_1| \leqslant \\ &\leqslant (1 + c_5\varepsilon_0)(1-\eta^2)\alpha |L_1 M_1| \leqslant \\ &\leqslant (1 + c_5\varepsilon_0)(1-\eta^2)\mu < \mu' \end{aligned}$$

при условии, что ε_0 достаточно мало.

Второй случай, $\rho > 0$. Аналогично, только теперь L_2, M_2 выполняют роль L_1, M_1.

Следствие. *Если $\theta \neq \theta^*$ и ε_0 достаточно мало, то можно считать, что*

$$|x_0 - \theta^* y_0| < 1.$$

Доказательство. Из (20), (21) и (22) имеем

$$|x_0 - \theta^* y_0| = |L_0^*| < \eta^n (1 + c_1\varepsilon_0)(1-\eta^2) L_1 < c_6\eta^n < c_7\varepsilon_0^{1/2} < 1.$$

§ 3. Об одном диофантовом уравнении. Мы рассмотрим сначала решение уравнения

$$m^2+m_1^2+m_2^2=3mm_1m_2 \tag{1}$$

в целых положительных числах. Числа m, удовлетворяющие этому уравнению, называются *числами Маркова*.

Предположим сначала, что какие-нибудь два числа среди чисел m, m_1, m_2 равны, например, $m_1=m_2$. Тогда $m_1^2 \mid m^2$, т. е. $m=dm_1$, а значит, $d^2+2=3m_1d$. Поэтому $d \mid 2$ и $d=1$ или 2. В обоих случаях $m_1=1$, и мы получили решения (1, 1, 1) и (2, 1, 1), которые назовем *сингулярными решениями* (вместе с их перестановками). Теперь рассмотрим случай, когда m, m_1, m_2 различны.

Квадратный трехчлен

$$\Phi(x)=x^2-3xm_1m_2+m_1^2+m_2^2$$

имеет целый положительный корень m. Другой корень m', удовлетворяющий равенствам $m+m'=3m_1m_2$, $mm'=m_1^2+m_2^2$, должен быть также целым положительным. Если, например, $m_1>m_2$, то

$$(m_1-m)(m_1-m')=\Phi(m_1)=2m_1^2+m_2^2-3m_1^2m_2<0.$$

Следовательно, $\max(m_1, m_2)$ лежит строго между m и m', кроме, быть может, сингулярных решений. Таким образом, каждое несингулярное решение порождает три различных решения

$$(m', m_1, m_2),\quad (m, m_1', m_2),\quad (m, m_1, m_2'),$$

где

$$m'=3m_1m_2-m,\quad m_1'=3mm_2-m_1,\quad m_2'=3mm_1-m_2. \tag{2}$$

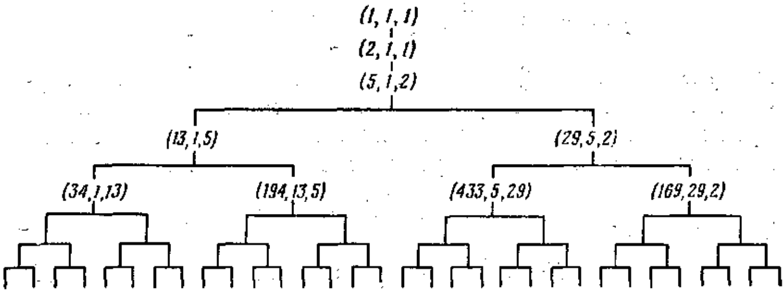
Будем называть эти три решения *соседними решениями* для первоначального решения. Взяв последовательно соседние решения, мы можем надеяться получить бесконечно много решений из одного данного. Если (m, m_1, m_2) — несингулярное решение и

$$m=\max(m, m_1, m_2), \tag{3}$$

то

$$\left.\begin{aligned} &m'<\max(m_1, m_2)<m,\\ &m_1'>\max(m, m_2)=m,\quad m_2'>m. \end{aligned}\right\} \tag{4}$$

Таким образом, одно соседнее решение имеет меньший максимальный элемент, а два других соседних решения имеют бо́льшие максимальные элементы. Если мы возьмем какое-нибудь решение и будем брать последовательно соседние решения с меньшим максимальным элементом, то придем в конечном счете к сингулярному решению. С другой стороны, (1, 1, 1) имеет единственное соседнее решение (2, 1, 1),



Фиг. 1. Цепочка Маркова решений уравнения
$m^2+m_1^2+m_2^2=3mm_1m_2$.

которое, как легко видеть, имеет единственное соседнее решение (5, 2, 1), не считая перестановок. Таким образом, решения уравнения (1) располагаются так, как указано на фиг. 1. Резюмируем сказанное в следующей лемме.

Лемма 5. *Все решения могут быть получены из* (1, 1, 1) *в виде цепочки соседних решений. Кроме того,*

$$\text{н. о. д.}\,(m,\ m_1)=\text{н. о. д.}\,(m,\ m_2)=\text{н. о. д.}\,(m_1,\ m_2)=1.$$

Доказательство. Только последнее утверждение нуждается в доказательстве. Если, например, $d=\text{н. о. д.}\,(m,\ m_1)$, то, согласно (1), $d\mid m_2$. Значит, $d\mid m'$, $d\mid m_1'$, $d\mid m_2'$ по (2) и d делит н. о. д. элементов любого соседнего решения. Идя назад к (1, 1, 1), получаем

$$d\mid \text{н. о. д.}\,(1,\ 1,\ 1).$$

В дальнейшем мы будем всегда предполагать, что для несингулярного решения имеет место (3) [а следовательно, и (4)]. Из уравнения (1) учитывая, что m, m_1, m_2, взаимно просты, можно найти целые k, k_1, k_2, такие, что[1])

$$\left.\begin{aligned} &k \equiv \frac{m_2}{m_1} \equiv \frac{-m_1}{m_2}\,(m), && 0 \leqslant k < m, \\ &k_1 \equiv \frac{m}{m_2} \equiv \frac{-m_2}{m}\,(m_1), && 0 \leqslant k_1 < m_1, \\ &k_2 \equiv \frac{m_1}{m} \equiv \frac{-m}{m_1}\,(m_2), && 0 < k_2 \leqslant m_2, \end{aligned}\right\} \tag{5}$$

где вместо знака $\leqslant$ можно брать знак $<$, кроме тех случаев, когда соответствующий модуль m, m_1, m_2 равен 1. Будем называть такую совокупность чисел *упорядоченным множеством Маркова* и условно обозначим так:

$$(m,\ k : m_1,\ k_1;\ m_2,\ k_2).$$

Заметим, что

$$k^2 \equiv \frac{m_2}{m_1} \cdot \frac{-m_1}{m_2} \equiv -1\,(m) \tag{6}$$

и т. д. Значит, существуют целые l, l_1, l_2, такие, что

$$k^2 + 1 = lm, \quad k_1^2 + 1 = l_1 m_1, \quad k_2^2 + 1 = l_2 m_2 \tag{7}$$

Лемма 6. *Если $m > 1$ и $(m,\ k : m_1,\ k_1;\ m_2 k_2)$ — упорядоченное множество Маркова, то таковыми же являются $(m_1',\ k_1' : m,\ k;\ m_2,\ k_2)$ и $(m_2',\ k_2' : m_1,\ k_1;\ m,\ k)$ при соответствующем выборе k_1', k_2'.*

Доказательство сразу следует из (2) и (5). Например, по (5_1)

$$k \equiv \frac{m_2}{m_1} \equiv \frac{-m_2}{m_1'} \equiv \frac{-m_2'}{m_1}\,(m),$$

что является аналогом (5_3) для $(m_2',\ k_2' : m_1,\ k_1;\ m,\ k)$.

Лемма 7. *Для несингулярного решения $(m,\ m_1,\ m_2)$ имеем*

$$\begin{aligned} mk_2 - m_2 k &= m_1, \\ m_1 k - mk_1 &= m_2, \\ m_1 k_2 - m_2 k_1 &= m' = 3m_1 m_2 - m. \end{aligned}$$

---

[1]) Знак $\leqslant$ поставлен для того, чтобы гарантировать справедливость леммы 7. Здесь $a \equiv b/c\,(m)$ для целых a, b и целого c, взаимно простого с m, означает $m \mid (ac - b)$.

Доказательство. Согласно (5), имеем

$$mk_2 - m_2k \equiv mk_2 \equiv m_1\,(m_2)$$

и

$$mk_2 - m_2k \equiv -m_2k \equiv m_1\,(m).$$

Так как н. о. д. $(m,\ m_2) = 1$, то

$$mk_2 - m_2k \equiv m_1\,(mm_2).$$

Но

$$mk_2 - m_2k - m_1 < mk_2 \leqslant mm_2$$

и

$$mk_2 - m_2k - m_1 \geqslant m - m_2(m-1) - m_1 =$$
$$= (m + m_2 - m_1) - mm_2 > -mm_2.$$

Следовательно, $mk_2 - m_2k = m_1$. Аналогично доказываются и два других равенства (ср. с доказательством леммы 6).

§ 4. Формы Маркова. Пусть m, m_1, m_2 — целые положительные числа, такие, что

$$m^2 + m_1^2 + m_2^2 = 3mm_1m_2, \quad m \geqslant \max(m_1, m_2). \tag{1}$$

Как и в § 3, обозначим через k целое, для которого

$$m_1k \equiv m_2\,(m), \quad 0 \leqslant k < m, \tag{2}$$

и через l — целое, определяемое равенством

$$k^2 + 1 = lm. \tag{2'}$$

Форма F_m, определенная равенством

$$mF_m(x,\ y) = mx^2 + (3m - 2k)\,xy + (l - 3k)\,y^2, \tag{3}$$

называется *формой Маркова*. В этом параграфе мы сохраняем обозначения § 3.

Нетрудно проверить справедливость тождества

$$m^2F_m(x,\ y) = \varphi_m(y,\ z), \tag{4}$$

где

$$z = mx - ky \tag{5}$$

и

$$\varphi_m(y,\ z) = y^2 + 3myz + z^2. \tag{6}$$

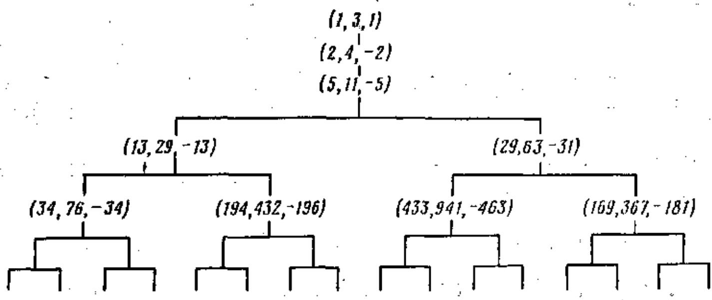
Легко видеть, что

$$\varphi_m(y, z) = \varphi_m(z, y) = \varphi_m(-z, y+3mz) = \\ = \varphi_m(z+3my, -y). \tag{7}$$

Согласно (5), (6), дискриминант формы mF_m равен $9m^2-4$, и, значит,

$$F_m = \left(x + \frac{3m-2k}{2m}y\right)^2 - \left(\frac{9}{4} - \frac{1}{m^2}\right)y^2. \tag{8}$$

Данное определение формы F_m несимметрично относительно m_1, m_2. Предположим, что $m_2k' \equiv m_1\,(m)$, $0 \leqslant k' < m$ и $k'^2 + 1 = l'm$. Пусть F'_m — соответствующая форма. Согласно (3.5), имеем $k + k' \equiv 0\,(m)$, и следовательно, или



Фиг. 2. Цепочка Маркова для форм $mF_m = mx^2 + (3m-2k)\,xy + (l-3k)\,y^2.$

$m=1$, $k=k'=0$, или $m>1$ и $k+k'=m$. В первом случае $F_m = F'_m$, во втором случае $F'_m(x, y) = F_m(x+2y, -y)$, согласно (8). Так как мы имеем дело только с эквивалентностью форм, то нет нужды рассматривать F_m и $F_{m'}$ отдельно. Если упорядочить m_1, m_2 так, что $k \leqslant k'$, то

$$0 \leqslant 2k \leqslant m. \tag{9}$$

При таком упорядочении $x^2+3xy+y^2$ является первой формой, эквивалентной форме x^2+xy-y^2, указанной во введении.

Родословному дереву решений уравнения

$$m^2 + m_1^2 + m_2^2 = 3mm_1m_2$$

соответствует родословное дерево форм Маркова (фиг. 2).

Здесь имеется некоторая неопределенность в обозначении F_m, так как еще не доказано, что не может быть двух различных решений (m, m_1, m_2), (m, m_1^*, m_2^*), которые встретились бы в разных частях родословного дерева. Но не известно ни одного случая таких решений, и это кажется неправдоподобным. Однако на практике никакой неопределенности нет.

Лемма 8. *Для несингулярного решения* (m, m_1, m_2)

$$F_m(k, m) = F_m(k-3m, m) = 1,$$
$$F_m(k_1, m_1) = F_m(k_2 - 3m_2, m_2) = -1.$$

Доказательство. Согласно (4), (5),

$$m^2 F_m(k, m) = \varphi_m(m, 0) = m^2.$$

Аналогично из равенств (4), (5), (7) имеем

$$m^2 F_m(k-3m, m) = \varphi_m(m, -3m^2) = \varphi_m(0, -m) = m^2.$$

По лемме 7, полагая $(x, y) = (k_1, m_1)$, имеем $z = -m_2$. Значит, по (1)

$$m^2 F_m(k_1, m_1) = \varphi_m(m_1, -m_2) = m_1^2 - 3mm_1m_2 + m_2^2 = -m^2.$$

Наконец,

$$m^2 F_m(k_2 - 3m_2, m_2) = \varphi_m(m_2, m_1 - 3mm_2) = \\ = \varphi_m(m_1, -m_2) = -m^2.$$

Следствие. *Пусть* $f(x, y) = x^2 + \beta xy + \gamma y^2$ *при некоторых* β, γ. *Предположим, что*

$$f(k, m) \geqslant 1, \qquad f(k-3m, m) \geqslant 1,$$
$$f(k_1, m_1) \leqslant -1, \quad f(k_2 - 3m_2, m_2) \leqslant -1.$$

Тогда $f(x, y) = F_m(x, y)$.

Доказательство. Пусть $F_m(x, y) = x^2 + \beta_m xy + \gamma_m y^2$. По лемме имеют место следующие неравенства:

$$B_1\beta + C_1\gamma \geqslant B_1\beta_m + C_1\gamma_m, \tag{10}$$
$$-B_2\beta + C_2\gamma \geqslant -B_2\beta_m + C_2\gamma_m, \tag{11}$$
$$-B_3\beta - C_3\gamma \geqslant -B_3\beta_m - C_3\gamma_m, \tag{12}$$
$$B_4\beta - C_4\gamma \geqslant B_4\beta_m - C_4\gamma_m, \tag{13}$$

где каждое B_j, C_j положительно (например, $B_1=km$, $C_1=m^2$ и т. д.). Но из (10), (11) имеем $(B_2C_1+B_1C_2)\gamma \geqslant (B_2C_1+B_1C_2)\gamma_m$, т. е. $\gamma \geqslant \gamma_m$. Аналогично $\gamma \leqslant \gamma_m$, $\beta \geqslant \beta_m$, $\beta \leqslant \beta_m$. Значит, $\beta=\beta_m$, $\gamma=\gamma_m$, что и требовалось доказать.

Лемма 9. *Формы $F_m(x, y)$ и $-F_m(x, y)$ эквивалентны.*

Доказательство. Утверждение справедливо для

$$F_1(x,\ y)=x^2+3xy+y^2 \quad \text{и} \quad F_2(x,\ y)=x^2+2xy-y^2,$$

так как

$$F_1(x+2y, -x-y)=-F_1(x,\ y) \ \text{и} \ F_2(y, -x)=-F_2(x,\ y).$$

Таким образом, мы можем считать, что $(m,\ m_1,\ m_2)$ — несингулярное решение, и покажем, что

$$F_m(k_1x-l_1y,\ m_1x-k_1y)=-F_m(x,\ y). \tag{14}$$

По лемме 8 равенство (14) справедливо, когда $(x,\ y)=(1,\ 0)$, а также когда $(x,\ y)=(k_1,\ m_1)$, так как

$$k_1x-l_1y=k_1^2-l_1m_1=1 \quad \text{и} \quad m_1x-k_1y=0.$$

Равенство (14) имеет место[1]) и при $(x,\ y)=(k,\ m)$, так как, повторно применяя лемму 7, получаем

$$m_1x-k_1y=m_1k-k_1m=m_2$$

и

$$m_1(k_1x-l_1y)=m_1(k_1k-l_1m)=m_1k_1k-m\left(k_1^2+1\right)=$$
$$=k_1m_2-m=m_1k_2-3m_1m_2=m_1(k_2-3m_2).$$

Следовательно, равенство (14), рассматриваемое как квадратное уравнение относительно y/x, имеет три различных корня. Значит, оно должно быть тождеством.

Следствие. *Корни θ, φ уравнения $F_m(x,\ 1)=0$ эквивалентны.*

Доказательство. В силу равенства (14)

$$F_m(-k_1\theta+l_1,\ -m_1\theta+k_1)=-F_m(\theta,\ 1)=0,$$

[1]) Так как дискриминанты обеих форм равны, то мы уже имеем три независимые функции от трех коэффициентов, которые равны для обеих форм. К сожалению, так как одна из этих форм — квадратичная, мы не можем вывести отсюда тождество. Следовательно, необходимо третье множество значений.

т. е.

$$F_m(\theta',\ 1)=0, \quad \theta'=\frac{-k_1\theta+l_1}{-m_1\theta+k_1}.$$

Если бы $\theta'=\theta$, то $m_1\theta^2-2k_1\theta+l_1=0$, что невозможно, так как $k_1^2-m_1l_1=-1<0$. Значит, $\theta'=\varphi$.

Лемма 10. $|F_m(x,\ y)|\geqslant 1$ *при всех целых* $(x,\ y)\neq(0,\ 0)$.

Доказательство. Пусть μ—минимум формы $|F_m(x,\ y)|$ при всех целых $(x,\ y)\neq(0,\ 0)$. Так как mF_m имеет целые коэффициенты, то найдутся целые x_0, y_0, такие, что $|F_m(x_0,\ y_0)|=\mu$. Согласно лемме 9, можно считать, что

$$F_m(x_0,\ y_0)=\mu\geqslant 0. \tag{15}$$

Воспользуемся равенствами (4)—(7). Для того чтобы целые $(y,\ z)$ получались из целого $(x,\ y)$, указанного в (5), необходимо и достаточно, чтобы

$$z\equiv -ky\ (m). \tag{16}$$

Если уравнение (15) имеет несколько решений, то выберем то, для которого

$$|y_0|+|z_0| \text{ есть минимум,} \tag{17}$$

где $z_0=mx_0-ky_0$.

Предположим сначала, если это возможно, что

$$y_0z_0<0, \quad |z_0|>|y_0|. \tag{18}$$

Возьмем $y_1=3my_0+z_0$, $z_1=-y_0$. Ясно, что $(y_1,\ z_1)$ удовлетворяет сравнению (16), так как ему удовлетворяет $(y_0,\ z_0)$ и $k^2=lm-1\equiv -1\ (m)$. Тогда

$$0\leqslant m^2\mu=\varphi_m(y_0,\ z_0)=\varphi_m(y_1,\ z_1)=z_0y_1+y_0^2. \tag{19}$$

Следовательно, $-y_0^2\leqslant z_0y_1\leqslant z_0^2$, где второе неравенство тривиально получается из (18). Таким же образом опять из (18) $|y_1|<|z_0|$. Значит, вопреки (17), мы имели бы $|y_1|+|z_1|<$ $<|y_0|+|z_0|$. Аналогично предположение $y_0z_0<0$, $|y_0|>|z_0|$ приводит к противоречию. Так как

$$\varphi_m(y_0,\ -y_0)=-(3m-2)\,y_0^2<0,$$

то должно быть

$$y_0z_0\geqslant 0. \tag{20}$$

Как и ранее, $y_2 = z_0$, $z_2 = -y_0$ удовлетворяют сравнению (16) и

$$|\varphi_m(y_2, z_2)| = |y_0^2 + z_0^2 - 3my_0z_0| \leqslant$$
$$\leqslant y_0^2 + z_0^2 + 3my_0z_0 = m^2\mu. \quad (21)$$

Согласно определению μ, в (21) должно быть равенство. Значит, или $y_0 = 0$, или $z_0 = 0$. Если $y_0 = 0$, то $m^2\mu = \varphi_m(0, z_0) = z_0^2 \geqslant m^2$, так как $m \mid z_0$ по (16). Аналогично если $z_0 = 0$, то $m^2\mu = y_0^2 \geqslant m^2$.

Лемма 11. *Пусть*

$$f(x, y) = x^2 + \beta xy + \gamma y^2.$$

Предположим, что

$$f(k_1, m_1) \leqslant -1, \quad f(k_2 - 3m_2, m_2) \leqslant -1.$$

Тогда

$$\beta^2 - 4\gamma \geqslant 4\Delta_m = 9 - 4m^{-2}.$$

Доказательство. Запишем $f(x, y)$, $F_m(x, y)$ так:

$$f(x, y) = \left(x + \frac{1}{2}\beta y\right)^2 - \Delta y^2,$$
$$F_m(x, y) = \left(x + \frac{1}{2}\beta_m y\right)^2 - \Delta_m y^2.$$

Нам надо доказать, что

$$\Delta \geqslant \Delta_m. \quad (22)$$

По лемме 8

$$f(x, y) \leqslant F_m(x, y) \quad (23)$$

и при $(x, y) = (k_1, m_1)$ и при $(k_2 - 3m_2, m_2)$. Неравенство (23) можно записать в виде

$$\Delta - \Delta_m \geqslant \left(\frac{x}{y} + \frac{\beta}{2}\right)^2 - \left(\frac{x}{y} + \frac{\beta_m}{2}\right)^2. \quad (24)$$

Если $\beta \geqslant \beta_m$, то (22) следует из (24) при $(x, y) = (k_1, m_1)$, так как $k_1/m_1 \geqslant 0$. Если же $\beta \leqslant \beta_m$, то (22) следует из (24) при $(x, y) = (k_2 - 3m_2, m_2)$, так как

$$\frac{3m_2 - k_2}{m_2} \geqslant 2 > \frac{3m - 2k}{2m} = \frac{\beta_m}{2}.$$

Лемма 12. *Пусть*

$$f(x, y) = x^2 + \beta xy + \gamma y^2.$$

Положим, что

$$f(k, m) \leqslant -1, \quad f(k-3m, m) \leqslant -1.$$

Тогда

$$\beta^2 - 4\gamma \geqslant 9 + 4m^{-2} > 9.$$

Доказательство. Пользуясь обозначениями предыдущего доказательства, имеем по лемме 8

$$f(x, y) \leqslant F_m(x, y) - 2$$

и при $(x, y) = (k, m)$ и при $(x, y) = (k-3m, m)$. Далее рассуждаем так же, как при доказательстве предыдущей леммы.

Лемма 13. *Пусть*

$$f(x, y) = x^2 + \beta xy + \gamma y^2,$$

где

$$2 \leqslant \beta \leqslant 3 \quad \text{и} \quad 0 < \beta^2 - 4\gamma < 9.$$

Предположим, что $|f(x, y)| \geqslant 1$ *при всех целых* $(x, y) \neq (0, 0)$. *Тогда* $f(x, y) \equiv F_m(x, y)$.

Доказательство. При всех целых $(x, y) \neq (0, 0)$ имеет место одна из двух возможностей:

$$\left.\begin{aligned} &P(x, y): \quad x^2 + \beta xy + \gamma y^2 \geqslant 1, \\ &N(x, y): \quad x^2 + \beta xy + \gamma y^2 \leqslant -1. \end{aligned}\right\} \tag{25}$$

Если имеет место $P(1, -1)$, то $\gamma \geqslant \beta$, что противоречит неравенствам $2 \leqslant \beta \leqslant 3$ и $\beta^2 - 4\gamma > 0$. Следовательно, должно иметь место $N(1, -1)$, т. е.

$$-\beta + \gamma \leqslant -2.$$

Если имеет место $P(0, 1)$, т. е. $\gamma \geqslant 1$, то $\beta \geqslant 3$. Следовательно, $\beta = 3$, $\gamma = 1$, так как $2 \leqslant \beta \leqslant 3$. Таким образом, $f(x, y) = x^2 + 3xy + y^2$, т. е. получена первая форма Маркова. В противном случае имеет место $N(0, 1)$, т. е.

$$\gamma \leqslant -1.$$

Рассмотрим $f(-5, 2)$. Если справедливо $P(-5, 2)$, то $25 - 10\beta + 4\gamma \geqslant 1$. Поэтому, используя также $N(0, 1)$, имеем

$$10\beta \leqslant 24 + 4\gamma \leqslant 20.$$

Тогда $\beta=2$, $\gamma=-1$, так как $2\leqslant\beta\leqslant 3$, что дает $x^2+2xy-y^2$, т. е. вторую форму Маркова. В противном случае имеем одновременно

$$N(0,\ 1) \quad \text{и} \quad N(-5,\ 2). \tag{26}$$

Далее доказываем по индукции. Пусть $(m,\ k : m_1,\ k_1;\ m_2,\ k_2)$ — упорядоченное множество Маркова. Положим, что имеет место одновременно

$$N(k_1,\ m_1) \quad \text{и} \quad N(k_2-3m_2,\ m_2). \tag{27}$$

Таким образом, (26) получается из (27) при $(5,\ 2 : 1,\ 0;\ 2,\ 1)$. Теперь рассмотрим разные возможные значения для $f(k,\ m)$ и $f(k-3m,\ m)$. Во-первых, если имеют место одновременно

$$P(k,\ m) \quad \text{и} \quad P(k-3m,\ m),$$

то $f(x,\ y)=F_m(x,\ y)$ по следствию из леммы 8. В противном случае имеем одно из двух: или одновременно

$$N(k,\ m) \quad \text{и} \quad N(k_2-3m_2,\ m_2), \tag{28}$$

или одновременно

$$N(k_1,\ m_1) \quad \text{и} \quad N(k-3m,\ m). \tag{29}$$

Но (28) и (29) есть как раз (27) соответственно для

$$\left(m_1',\ k_1' : m,\ k;\ m_2,\ k_2\right) \quad \text{и} \quad \left(m_2',\ k_2' : m_1,\ k_1;\ m,\ k\right),$$

где $\left(m_1',\ m,\ m_2\right)$, $\left(m_2',\ m_1,\ m\right)$ — два начала продолжения дерева непосредственно под $(m,\ m_1,\ m_2)$ на фиг. 1. Следовательно, если бы $f(x,\ y)$ не являлась формой Маркова, то она должна была бы удовлетворять (27) для бесконечной последовательности множеств Маркова

$$M^{(j)}=\left(m^{(j)},\ k^{(j)} : m_1^{(j)},\ k_1^{(j)};\ m_2^{(j)},\ k_2^{(j)}\right), \tag{30}$$

где $m^{(1)}<m^{(2)}<\ldots$. Но из (27) по лемме 11 следует, что $\beta^2-4\gamma\geqslant 9-4m^{-2}$. Значит,

$$\beta^2-4\gamma\geqslant\lim_{j\to\infty}\left(9-4\left(m^{(j)}\right)^{-2}\right)=9,$$

что противоречит условию. Лемма доказана.

Следствие. *Пусть* $m>2$, $\tilde{m}>2$ *и предположим, что* $(\tilde{m},\ \tilde{m}_1,\ \tilde{m}_2)$ *находится на том единственном пути* (на фиг. 1), *который ведет от* (1, 1, 1) *вниз к* (m, m_1, m_2). *Тогда* F_m *удовлетворяет условиям* (27), *если заменить* $M=(m, k: m_1, k_1; m_2, k_2)$ *на* $\tilde{M}=(\tilde{m}, \tilde{k}: \tilde{m}_1, \tilde{k}_1; \tilde{m}_2; \tilde{k}_2)$.

Доказательство. Согласно (8), (9) и лемме 10, функция $f(x, y)=F_m(x, y)$ удовлетворяет условиям леммы. Следовательно, к ней применимы предыдущие рассуждения. Это может быть только в том случае, когда полученная там последовательность (30) оканчивается на $M^{(J)}=M$. Таким образом, $\tilde{M}=M^{(j)}$ для некоторого $j \leqslant J$.

Лемма 14. *Существует несчетное множество форм*

$$f(x, y)=x^2+\beta xy+\gamma y^2$$

с коэффициентами $2 \leqslant \beta \leqslant 3$ *и* $\beta^2-4\gamma=9$, *таких, что* $|f(x, y)| \geqslant 1$ *при всех целых* $(x, y) \neq (0, 0)$.

Доказательство. Пусть $\mathfrak{M}$ — любая бесконечная последовательность $M^{(j)}$ $(j=1, 2, \ldots)$, такая, как в (30), где $\left(m^{(j)}, m_1^{(j)}, m_2^{(j)}\right)$ есть соответственно (1, 1, 1), (2, 1, 1), (5, 1, 2) для $j=1, 2, 3$ и $\left(m^{(j+1)}, m_1^{(j+1)}, m_2^{(j+1)}\right)$ для $j \geqslant 3$ есть одно из двух решений, следующих непосредственно за $\left(m^{(j)}, m_1^{(j)}, m_2^{(j)}\right)$ на фиг. 1. Ясно, что существует несчетное множество последовательностей $\mathfrak{M}$, и мы покажем, что всем им соответствуют различные пары чисел β, γ с нужными свойствами. Положим

$$F^{(j)}=F_{m^{(j)}}=x^2+\beta^{(j)}xy+\gamma^{(j)}y^2.$$

Тогда

$$(\beta^{(j)})^2-4\alpha^{(j)}\gamma^{(j)}=9-4\left(m^{(j)}\right)^{-2} \rightarrow 9.$$

По „лемме о компактности“ (стр. 33) найдутся β, γ и подпоследовательность $j_1<j_2<\ldots$, такие, что [1])

$$\beta^{(j_t)} \rightarrow \beta, \ \gamma^{(j_t)} \rightarrow \gamma \quad \text{и} \quad \beta^2-4\gamma=9.$$

Положим $f(x, y)=x^2+\beta xy+\gamma y^2$. Тогда по лемме 10

$$|f(x, y)|=\lim_{t \rightarrow \infty}\left|F^{(j_t)}(x, y)\right| \geqslant 1$$

---

[1]) Нетрудно видеть, что в действительности $\beta^{(j)}, \gamma^{(j)}$ имеют пределы.

при всех целых $(x, y) \neq (0, 0)$. По следствию из леммы 13 $F^{(j)}(x, y)$ удовлетворяет (27) для всех множеств $M^{(i)}$ $(3 \leqslant i \leqslant j)$. Следовательно, вспоминая определение $N(x, y)$ в (25), видим, что $f(x, y)$ удовлетворяет (27) для всех $M^{(i)}$ $(3 \leqslant i < \infty)$. Но две различные последовательности $\mathfrak{M}, \overline{\mathfrak{M}}$ должны иметь $M^{(j)}$, $\overline{M}^{(j)}$, совпадающие при всех j вплоть до некоторого J, но отличные при $j = J+1$. Тогда одна из соответствующих форм $f, \overline{f}$, скажем f, должна удовлетворять (28), а другая, $\overline{f}$, должна удовлетворять (29) для $M^{(J)}$. Но (28) и (29) несовместимы по лемме 12, так как $\beta^2 - 4\gamma = 9$. Значит, $f \neq \overline{f}$, т. е. каждой последовательности $\mathfrak{M}$ соответствует своя особая форма f.

§ 5. Цепочка Маркова для форм.

Теорема II. *Предположим, что*

$$f(x, y) = \alpha x^2 + \beta xy + \gamma y^2, \quad \delta = \beta^2 - 4\alpha\gamma > 0$$

и

$\mu = \inf |f(x, y)|$ *(x, y не равны нулю одновременно).*

А. *Если*

$$\mu > \frac{1}{3}\delta^{1/2}, \tag{1}$$

то f эквивалентна кратному формы Маркова.

В. *Обратно, неравенство* (1) *имеет место для всех форм, эквивалентных кратным формам Маркова.*

С. *Существует несчетное множество форм, ни одна из которых не эквивалентна кратному любой другой, таких, что $\mu = \frac{1}{3}\delta^{1/2}$.*

Доказательство. Можно считать, что $\mu = 1$, рассмотрев в противном случае $\mu^{-1}f$ вместо f. Утверждение В — просто иная формулировка леммы 10. Утверждение С следует сразу из леммы 14 и из того факта, что существует только счетное множество форм $f'(x, y) = f(ax+by, cx+dy)$ с целыми a, b, c, d, эквивалентных любой заданной форме f. Значит, можно считать, что

$$0 < \delta < 9, \quad \mu = 1,$$

и остается доказать утверждение А.

По условию для заданного $\varepsilon > 0$ найдутся целые взаимно простые a, c, такие, что $1 = \mu \leqslant |f(a, c)| < 1 + \varepsilon$. Следовательно, по следствию из леммы 1 имеется форма

$$f'(x, y) = \alpha' x^2 + \beta' xy + \gamma' y^2,$$

эквивалентная $\pm f(x, y)$, такая, что

$$1 \leqslant \alpha' < 1 + \varepsilon, \quad 2\alpha' \leqslant \beta' \leqslant 3\alpha'.$$

Если $\alpha' = 1$, то $f'(x, y)$ есть форма Маркова по лемме 13, и теорема доказана, так как $\pm F_m(x, y)$ эквивалентны по лемме 9. В противном случае можно найти бесконечную последовательность форм

$$f_n(x, y) = \alpha_n x^2 + \beta_n xy + \gamma_n y^2,$$

$$\alpha_n \to 1, \quad 2\alpha_n \leqslant \beta_n \leqslant 3\alpha_n, \quad \beta_n^2 - 4\alpha_n \gamma_n = \delta, \tag{2}$$

каждая из которых эквивалентна $\pm f(x, y)$, так что, в частности,

$$|f_n(x, y)| \geqslant 1, \quad (x, y) \text{ — целые } \neq (0, 0).$$

По „лемме о компактности“ (стр. 33) можно считать, выбирая в случае надобности подпоследовательность первоначальной подпоследовательности, что β_n, γ_n имеют пределы, скажем

$$\alpha_n \to 1 = \alpha_0, \quad \beta_n \to \beta_0, \quad \gamma_n \to \gamma_0, \tag{3}$$

где

$$2 \leqslant \beta_0 \leqslant 3, \quad \beta_0^2 - 4\gamma_0 = \delta.$$

Обозначим

$$f_0(x, y) = x^2 + \beta_0 xy + \gamma_0 y^2.$$

Пусть θ_0, φ_0 — корни трехчлена $f_0(x, 1)$, и θ_n, φ_n [1]) — корни трехчлена $f_n(x, 1)$. Тогда

$$\theta_n \to \theta_0, \quad \varphi_n \to \varphi_0 \tag{4}$$

при соответствующем выборе θ_n из θ_n, φ_n. Далее,

$$|f_0(x, y)| = \lim |f_n(x, y)| \geqslant 1 \qquad (n \to \infty)$$

при всех целых $(x, y) \neq (0, 0)$. Значит, по лемме 13 $f_0(x, y)$ есть $F_m(x, y)$. Но, согласно лемме 8, $F_m(x, y)$ принимает

---

[1]) Обозначения θ_n, φ_n не следует смешивать с обозначениями предыдущей главы.

оба значения ± 1, а поэтому применима „теорема изоляции" (стр. 37). Пусть $\mu' < \mu = 1$, $\varepsilon_0 > 0$ — соответствующие постоянные, определяемые теоремой I для $f_0(x, y) = F_m$. Тогда по (3) и (4)

$$|\alpha_n - \alpha_0| < \varepsilon_0, \quad |\theta_n - \theta_0| < \varepsilon_0, \quad |\varphi_n - \varphi_0| < \varepsilon_0$$

для достаточно больших n. Так как $|f_n(x, y)| \geqslant 1 > \mu'$ при всех целых $(x, y) \neq (0, 0)$, то отсюда следует, что $f_n(x, y)$ есть $\lambda F_m(x, y)$ при некоторой постоянной[1] λ. Но $\pm f$ эквивалентна f_n, что и доказывает утверждение A.

§ 6. Цепочка Маркова для приближений.

Теорема III. *Пусть θ иррационально и*

$$\nu = \liminf q \| q\theta \|. \tag{1}$$

A. *Если $\nu > \frac{1}{3}$, то θ эквивалентна корню уравнения $F_m(x, 1) = 0$, где F_m — форма Маркова.*

B. *Обратно, если θ эквивалентна корню уравнения $F_m(x, 1) = 0$, то*

$$\nu = (9 - 4m^{-2})^{-1/2} > \frac{1}{3} \tag{2}$$

и существует бесконечно много решений неравенства $q\|q\theta\| < \nu$. Оба корня уравнения $F_m(x, 1) = 0$ эквивалентны друг другу.

C. *Существует несчетное множество неэквивалентных θ, таких, что $\nu = 1/3$.*

Доказательство A. Рассмотрим

$$f(x, y) = x(\theta x - y). \tag{3}$$

По условию для любого как угодно малого $\varepsilon > 0$ существует $X_0 = X_0(\varepsilon)$, такое, что при целых (x, y)

$$|f(x, y)| > \nu - \varepsilon, \quad \text{как только} \quad |x| > X_0. \tag{4}$$

Так как θ иррационально, то, как легко видеть, сказанное эквивалентно утверждению, что найдется $Y_0 = Y_0(\varepsilon) > 0$, такое, что при целых $(x, y) \neq (0, 0)$

$$|f(x, y)| > \nu - \varepsilon, \quad \text{как только} \quad |\theta x - y| < Y_0(\varepsilon). \tag{5}$$

---

[1]) Легко видеть, что $\lambda = 1$.

Далее, по условию существует такая последовательность пар целых a_n, b_n, которые можно считать взаимно простыми, что

$$|f(a_n, b_n)| \to \nu, \quad a_n \to \infty, \quad |\theta a_n - b_n| \to 0. \tag{6}$$

По следствию из леммы 1 существуют подстановки

$$x_n = a_n x + c_n y, \quad y_n = b_n x + d_n y, \tag{7}$$

где

$$a_n,\ b_n,\ c_n,\ d_n \text{ — целые}, \quad a_n d_n - b_n c_n = \pm 1, \tag{8}$$

такие, что

$$\pm f(x_n, y_n) = f_n(x, y) = \alpha_n x^2 + \beta_n xy + \gamma_n y^2 \tag{9}$$

удовлетворяет условиям

$$\left.\begin{aligned} &\alpha_n = |f(a_n, b_n)| \to \nu, \\ &2\alpha_n \leqslant \beta_n \leqslant 3\alpha_n, \quad \beta_n^2 - 4\alpha_n\gamma_n = 1. \end{aligned}\right\} \tag{10}$$

По „лемме о компактности“ (стр. 33) можно считать, выбирая подпоследовательность, что

$$\left.\begin{aligned} &\alpha_n \to \alpha_0 = \nu, \quad \beta_n \to \beta_0, \quad \gamma_n \to \gamma_0, \\ &2\alpha_0 \leqslant \beta_0 \leqslant 3\alpha_0, \quad \beta_0^2 - 4\alpha_0\gamma_0 = 1 \end{aligned}\right\} \tag{11}$$

при некоторых β_0, γ_0. Обозначим

$$f_0(x, y) = \alpha_0 x^2 + \beta_0 xy + \gamma_0 y^2 = \nu(x - \theta_0 y)(x - \varphi_0 y) \tag{12}$$

и

$$\theta_n = \frac{-\theta c_n + d_n}{\theta a_n - b_n}, \quad \varphi_n = \frac{-c_n}{a_n}. \tag{13}$$

Тогда по (7)

$$x_n = a_n(x - \varphi_n y), \tag{14}$$

$$\theta x_n - y_n = (\theta a_n - b_n)(x - \theta_n y). \tag{15}$$

Следовательно,

$$f_n(x, y) = \alpha_n(x - \theta_n y)(x - \varphi_n y). \tag{16}$$

Можно считать, что

$$\theta_n \to \theta_0, \quad \varphi_n \to \varphi_0. \tag{17}$$

меняя, в случае надобности, ролями θ_0, φ_0 и выбирая подпоследовательность функций f_n. Пусть x, y — фиксированные целые, а x_n, y_n определены равенствами (7). Тогда

$$\lim |\theta x_n - y_n| = \lim |x - \theta_n y| |\theta a_n - b_n| = 0 \quad (n \to \infty) \tag{18}$$

по (6), (15), так как $|x - \theta_n y|$ — величина ограниченная. Следовательно, согласно (5),

$$|f_0(x, y)| = \lim |f_n(x, y)| = \lim |f(x_n, y_n)| \geqslant \nu \qquad (n \to \infty). \tag{19}$$

Таким образом, по (11) форма $\nu^{-1} f_0(x, y)$, имеющая дискриминант $\nu^{-2} < 9$, по предположению, удовлетворяет условиям леммы 13. Значит,

$$f_0(x, y) = \nu F_m(x, y), \tag{20}$$

где F_m — некоторая форма Маркова.

Если $\theta_n = \theta_0$ при всех n, то, очевидно, θ эквивалентна θ_0, и утверждение А доказано. Мы можем считать, что при всех $n \geqslant 1$

$$\theta_n \neq \theta_0, \tag{21}$$

и придем к противоречию. Ясно, что следствие теоремы I применимо к $F_m(x, y)$ и $\nu^{-1} f_n(x, y)$ с $\mu = 1$ по (17), (18), (20), (21). Следовательно, существует $\mu' < 1$, такое, что для всех достаточно больших n найдутся целые $(\bar{x}_n, \bar{y}_n)$, для которых

$$|f_n(\bar{x}_n, \bar{y}_n)| < \mu' \nu, \quad |\bar{x}_n - \theta_n \bar{y}_n| \leqslant 1. \tag{22}$$

Положим

$$\bar{x}^{(n)} = a_n \bar{x}_n + c_n \bar{y}_n, \quad \bar{y}^{(n)} = b_n \bar{x}_n + d_n \bar{y}_n.$$

Тогда по (9)

$$|f(\bar{x}^{(n)}, \bar{y}^{(n)})| = |f_n(\bar{x}_n, \bar{y}_n)| < \mu' \nu < \nu$$

и по (6), (15), (22)

$$|\theta \bar{x}^{(n)} - \bar{y}^{(n)}| = |\theta a_n - b_n| |\bar{x}_n - \theta_n \bar{y}_n| \leqslant |\theta a_n - b_n| \to 0$$
$$(n \to \infty),$$

что противоречит (5).

Доказательство В следует сразу из леммы 4, 9 (и их следствий) и 10, так как тогда $F_m(x, y)$ имеет $\mu = 1$, $\delta = 9 - 4m^{-2}$.

Доказательство С. Согласно леммам 4, 14, существует несчетное множество чисел θ, для которых $\nu \geqslant {}^1/_3$. Согласно утверждению А, существует только счетное множество чисел θ, для которых $\nu > {}^1/_3$, а множество чисел, эквивалентных любому числу, очевидно, счетно.

ЗАМЕЧАНИЯ

§ 1. Первоначальное доказательство Маркова использует теорию непрерывных дробей [Марков (1879) или Диксон (1930)]. Приведенное здесь доказательство восходит к Ремаку (1924) и Фробениусу (1913). Иная точка зрения (но не доказательство) имеется у Кона (1955).

Немногое известно о возможных значениях величины $\delta^{-1/2}(f)\mu(f)$, меньших ${}^1/_3$, или, что практически то же самое, величины $\nu(\theta)$; см. Коксма (1936), гл. III. Простое доказательство того, что эти значения не могут встречаться между $12^{-1/2}$ и $13^{-1/2}$, см. у Дейвиса (1950). М. Холл показал, что они принимают все значения в интервале справа от нуля, но не опубликовал детали доказательства. Результат такого рода непосредственно следует из (2.15) гл. I и из результатов М. Холла (1947), где дано краткое описание такого применения.

§ 2. „Теорема изоляции“ и ее применение в этом контексте принадлежат Роджерсу (не опубликовано). Имеются любопытные предположения у Ремака (1925). Дальнейшее распространение техники „изоляции“ см. у Касселса и Суиннертона-Дайера (1955).

§ 3. Дальнейшее рассмотрение этого уравнения см. у Фробениуса (1913). Техника Фробениуса была недавно применена некоторыми авторами к другим диофантовым уравнениям.

Глава III

НЕОДНОРОДНЫЕ ПРИБЛИЖЕНИЯ

§ 1. Введение. В предыдущих двух главах мы занимались однородными задачами, т. е. стремились сделать малой дробную долю $\|q\theta\|$ однородного выражения $q\theta$, или, более общо, стремились сделать малыми одновременно $\|q\theta_1\|, \ldots$ $\ldots, \|q\theta_n\|$. В этой главе мы будем заниматься неоднородной формой $q\theta - \alpha$ или более общими совместными задачами. Между однородными и неоднородными задачами имеется существенное различие. В однородной задаче значение $q = 0$ дает тривиальный результат, который должен быть исключен, а предположение $q < 0$ не вносит общности, так как $\|(-q)\theta\| = \|q\theta\|$. В неоднородном случае обычно бывает уместно позволять целой переменной принимать все значения — положительные, отрицательные и нуль. Ограничиваясь положительными значениями переменной, мы приходим к другому варианту задачи.

Если θ рационально, скажем $\theta = m/n$, где $n > 0$, m — целые, то, очевидно, что $\|q\theta - \alpha\| \geqslant n^{-1}\|n\alpha\|$, причем равенство имеет место для бесконечно многих q. Другой тривиальный случай имеет место при $\alpha = m\theta + n$ для некоторых целых m, n. Тогда $\|q\theta - \alpha\| = \|(q - m)\theta\|$, и задача о поведении $\|q\theta - \alpha\|$ является, по существу, однородной задачей. В § 2 мы покажем, не считая эти два случая, что всегда существует бесконечно много целых q, таких, что $|q|\,\|q\theta - \alpha\| < {}^1/_4$, и что в этом утверждении ${}^1/_4$ для переменного θ не может быть заменена меньшей постоянной. Эта теорема является аналогом однородной теоремы относительно $q\|q\theta\| < 5^{-1/2}$. В § 3 мы покажем, что не существует хотя бы и слабого неоднородного аналога существования решений неравенств $0 < q < Q$, $\|q\theta\| \leqslant Q^{-1}$ при всех $Q > 1$.

В задаче совместного неоднородного приближения возникают новые соображения. Предположим, что мы хотим найти целое q, такое, что одновременно

$$\|q\theta_i - \alpha_i\| < \varepsilon \qquad (1 \leqslant i \leqslant n), \tag{1}$$

где θ_i, α_i и $\varepsilon > 0$ заданы. Пусть имеются целые $u_1, \ldots, u_n$, не равные одновременно нулю, такие, что $u_1\theta_1 + \ldots + u_n\theta_n$ — целое. Тогда из (1) следует, что

$$\begin{aligned}\|u_1\alpha_1 + \ldots + u_n\alpha_n\| &= \\ &= \|u_1(\alpha_1 - q\theta_1) + \ldots + u_n(\alpha_n - q\theta_n)\| \leqslant \\ &\leqslant |u_1|\,\|\alpha_1 - q\theta_1\| + \ldots + |u_n|\,\|\alpha_n - q\theta_n\| < \\ &\qquad < (|u_1| + \ldots + |u_n|)\,\varepsilon.\end{aligned}$$

Таким образом, если неравенства (1) разрешимы при любом сколь угодно малом $\varepsilon > 0$, то мы должны иметь $\|u_1\alpha_1 + \ldots + u_n\alpha_n\| = 0$, т. е. выражение $u_1\alpha_1 + \ldots + u_n\alpha_n$ должно быть целым числом. Это дает ряд необходимых условий разрешимости (1) при любом малом $\varepsilon > 0$. В § 5 мы покажем в более общем плане, что это необходимое условие является также и достаточным. В гл. V мы выясним, как этот результат может быть сформулирован количественно.

§ 2. Одномерный случай. Мы сначала докажем один довольно общий результат:

Теорема I (Минковский). *Пусть при* $j = 1, 2$ $L_j = L_j(x, y) = \lambda_j x + \mu_j y$ — *пара линейных форм, и пусть* $\Delta = \lambda_1\mu_2 - \lambda_2\mu_1 \neq 0$. *Тогда*:

А. *Для любых чисел* ρ_1, ρ_2 *существуют целые* x, y, *такие, что*

$$|L_1 + \rho_1|\,|L_2 + \rho_2| \leqslant \frac{1}{4}|\Delta|. \tag{1}$$

В. *Если, далее,* μ_1/λ_1 *иррационально, а* $\varepsilon > 0$ *произвольно мало, то существуют решения неравенства* (1), *для которых*

$$|L_1 + \rho_1| < \varepsilon. \tag{2}$$

Теорема I есть простое следствие следующей леммы.

Лемма 1. *Пусть* θ, φ, ψ, ω — *четыре действительных числа, таких, что*

$$|\theta\omega - \varphi\psi| \leqslant \frac{1}{2}|\Delta|, \quad |\psi\omega| \leqslant |\Delta|, \quad \psi > 0. \tag{3}$$

Тогда найдется целое u, такое, что

$$|\theta+\psi u||\varphi+\omega u|\leqslant\frac{1}{4}|\Delta| \tag{4}$$

и

$$|\theta+\psi u|\leqslant\psi. \tag{5}$$

Доказательство. Можно считать, что $-\psi\leqslant\theta<0$ и $\varphi\geqslant 0$, взяв в случае необходимости вместо θ, φ соответственно $\theta+u_0\psi$, $\varphi+u_0\varphi$ при подходящем целом u_0 и $-\varphi$, $-\omega$ вместо φ, ω. Теперь покажем, что $u=0$ или 1 обеспечивает справедливость леммы.

Предположим сначала, что $\varphi+\omega\leqslant 0$. Тогда

$$16|\theta\varphi||(\theta+\psi)(\varphi+\omega)|\leqslant$$
$$\leqslant(|\theta|+|\theta+\psi|)^2(|\varphi|+|\varphi+\omega|)^2=\psi^2\omega^2\leqslant|\Delta|^2. \tag{6}$$

Если же $\varphi+\omega>0$, то

$$2(|\theta\varphi||(\theta+\psi)(\varphi+\omega)|)^{1/2}\leqslant|\varphi||\theta+\psi|+|\theta||\varphi+\omega|=$$
$$=|\varphi(\theta+\psi)-\theta(\varphi+\omega)|=|\varphi\psi-\theta\omega|\leqslant\frac{1}{2}|\Delta|. \tag{7}$$

Следовательно, в обоих случаях

$$\min(|\theta\varphi|,|(\theta+\psi)(\varphi+\omega)|)\leqslant\frac{1}{4}|\Delta|. \tag{8}$$

Так как $\max(|\theta|,\ |\theta+\psi|)\leqslant\psi$, то тем самым лемма доказана.

Доказательство теоремы I. Мы начнем с доказательства B. По теореме Минковского о линейных формах (приложение B, теорема III) найдутся целые x_0, y_0, не равные нулю одновременно, такие, что

$$|\lambda_1x_0+\mu_1y_0|<\varepsilon,\quad |\lambda_2x_0+\mu_2y_0|\leqslant\varepsilon^{-1}|\Delta|. \tag{9}$$

Без ограничения общности можно считать x_0, y_0 взаимно простыми. Так как μ_1/λ_1 иррационально, то мы можем считать, что

$$0<\lambda_1x_0+\mu_1y_0<\varepsilon, \tag{9'}$$

заменяя величины x_0, y_0 в случае необходимости величинами $-x_0$, $-y_0$. Выберем теперь целые x_1, y_1 так, чтобы $x_0y_1-x_1y_0=1$. Положим

$$x=x'x_0+y'x_1,\quad y=x'y_0+y'y_1,$$

так что x, y — целые, если x', y' — целые, и наоборот. Тогда

$$L_j = \lambda_j x + \mu_j y = \lambda'_j x' + \mu'_j y' \qquad (j = 1,\ 2),$$

где $\lambda'_1\mu'_2 - \lambda'_2\mu'_1 = \lambda_1\mu_2 - \lambda_2\mu_1 = \Delta$ и $0 < \lambda'_1 < \varepsilon$, $|\lambda'_2| \leqslant \varepsilon^{-1}|\Delta|$, по (9) и (9′).

Пусть теперь y' — целое, такое, что

$$|\rho_1\lambda'_2 - \rho_2\lambda'_1 - \Delta y'| \leqslant \frac{1}{2}|\Delta|.$$

Мы можем теперь применить лемму 1, выбирая

$$\theta = \mu'_1 y' + \rho_1, \quad \varphi = \mu'_2 y' + \rho_2,$$
$$\psi = \lambda'_1, \qquad \omega = \lambda'_2,$$

так как $|\theta\omega - \psi\varphi| = |\rho_1\lambda'_2 - \rho_2\lambda'_1 - \Delta y'| \leqslant \frac{1}{2}|\Delta|$

и

$$|\psi\omega| = |\lambda'_1\lambda'_2| < |\Delta|.$$

Следовательно, существует целое $x' = u$, такое, что

$$L_j = \lambda'_j x' + \mu'_j y' \qquad (j = 1,\ 2)$$

удовлетворяют неравенствам

$$|L_1 + \rho_1||L_2 + \rho_2| \leqslant \frac{1}{4}|\Delta|,$$
$$|L_1 + \rho_1| \leqslant \lambda'_1 < \varepsilon,$$

что и требовалось доказать.

Для доказательства A заметим, что обязательно найдутся целые x_0, y_0, не равные нулю одновременно, такие, что

$$|\lambda_j x_0 + \mu_j y_0| \leqslant |\Delta|^{1/2} \qquad (j = 1,\ 2).$$

Если $\lambda_1 x_0 + \mu_1 y_0 \neq 0$, то рассуждаем так, как показано выше; если же $\lambda_1 x_0 + \mu_1 y_0 = 0$, то тогда $\lambda_2 x_0 + \mu_2 y_0 \neq 0$ и L_1, L_2 меняются ролями.

Следствие. *Постоянная $^1/_4$ не может быть заменена меньшей.*

Доказательство.

$$\left|x + \frac{1}{2}\right|\left|y + \frac{1}{2}\right| \geqslant \frac{1}{4}$$

при всех целых x, y.

При более внимательном рассмотрении доказательства можно было бы показать, что это, в сущности, является единственным случаем, когда в (1) имеет место равенство. Вместо этого мы докажем следующую теорему.

Теорема II (Минковский). А. *Если θ иррационально и α не может быть представлено в виде $\alpha = m\theta + n$ при целых m, n, то существует бесконечно много целых q, таких что*

$$|q|\,\|q\theta - \alpha\| < \frac{1}{4}.$$

В. *Для любого заданного $\varepsilon > 0$ существуют иррациональное θ и $\alpha \neq m\theta + n$, такие, что $|q|\,\|q\theta - \alpha\| > {}^1/_4 - \varepsilon$ при всех $q \neq 0$ и $\liminf |q|\,\|q\theta - \alpha\| = {}^1/_4$ при $|q| \to \infty$.*

Доказательство А. По теореме I В с

$$L_1 + \rho_1 = \theta x - y - \alpha, \quad L_2 + \rho_2 = x, \quad |\Delta| = 1$$

существуют целые $x = q$, $y = p$, такие, что

$$|q|\,|q\theta - p - \alpha| \leqslant \frac{1}{4}, \quad |q\theta - p - \alpha| < \varepsilon.$$

Так как $\alpha \neq q\theta - p$ при всех целых p, q, то, заставляя $\varepsilon \to 0$, мы получаем бесконечно много пар целых p, q. Наконец, ${}^1/_4$ достигается самое большее один раз, так как из равенств

$$q\theta - p - \alpha = \pm \frac{1}{4} q^{-1}, \quad q'\theta - p' - \alpha = \pm \frac{1}{4} q'^{-1}, \quad q \neq q'$$

при любой комбинации знаков следует, что $(q - q')\theta$ рационально, а значит, и θ рационально вопреки предположению.

Доказательство В. Запишем θ в виде непрерывной дроби, как в гл. I,

$$\theta = [a_1, a_2, \ldots],$$

где требования на a_n будут наложены в ходе доказательства. Имеем

$$\left| \frac{q_{n+1}\theta - p_{n+1}}{q_n\theta - p_n} \right| = \theta_{n+1} = [a_{n+1}, a_{n+2}, \ldots] < a_{n+1}^{-1} \tag{10}$$

и для $n \geqslant 1$

$$\frac{q_n}{q_{n+1}} = \varphi_n = [a_n, a_{n-1}, \ldots, a_1] \leqslant a_n^{-1}. \tag{11}$$

По (2.15), (2.16) гл. I имеем [1])

$$|q_n(q_n\theta-p_n)|=(a_n+\varphi_{n-1}+\theta_{n+1})^{-1}=(a_n+O(1))^{-1} \quad (12)$$

и

$$|q_{n+1}(q_n\theta-p_n)|=(1+\theta_{n+1}\varphi_n)^{-1}=1+O\left(a_n^{-1}a_{n+1}^{-1}\right). \quad (13)$$

Положим теперь $\alpha=\frac{1}{2}(1-\theta)$. Очевидно, достаточно рассмотреть только целые $q\neq 0$, p, такие, что

$$1\geqslant 4|q||q\theta-p-\alpha|=|2q||(2q+1)\theta-(2p+1)|. \quad (14)$$

Если $|2q+1|\leqslant a_1^{1/2}$, то $|(2q+1)\theta|<a_1^{-1/2}$, и правая часть неравенства (14) будет больше, чем

$$2\left(1-a_1^{-1/2}\right)\geqslant 1,$$

если $a_1\geqslant 4$, что мы и будем теперь предполагать. Таким образом, существует целое $n\geqslant 1$, такое, что

$$a_n^{1/2}q_n\leqslant|2q+1|\leqslant a_{n+1}^{1/2}q_{n+1}. \quad (15)$$

Следовательно, по (12), (14) и по тривиальному неравенству $|(2q+1)/2q|<2$

$$\frac{|(2q+1)\theta-(2p+1)|}{|q_n\theta-p_n|}\leqslant$$

$$\leqslant\frac{|2q+1|}{|2q|}\cdot\frac{q_n}{|2q+1|}\cdot\frac{1}{|q_n(q_n\theta-p_n)|}=O\left(a_n^{1/2}\right). \quad (16)$$

Так как $|p_{n+1}q_n-q_{n+1}p_n|=1$, то найдутся целые u, v, такие, что

$$2p+1=up_n+vp_{n+1},\quad 2q+1=uq_n+uq_{n+1}. \quad (17)$$

В действительности, по (15), (16) и (12), (13)

$$|u|=|(2q+1)(q_{n+1}\theta-p_{n+1})-q_{n+1}((2q+1)\theta-$$
$$-(2p+1))|=O\left(a_{n+1}^{1/2}q_{n+1}|q_{n+1}\theta-p_{n+1}|\right)+$$
$$+O\left(a_n^{1/2}q_{n+1}|q_n\theta-p_n|\right)=O\left(a_n^{1/2}\right).$$

Таким образом,

$$\frac{2q+1}{q_{n+1}}=v+u\frac{q_n}{q_{n+1}}=v+O\left(a_n^{-1/2}\right). \quad (18)$$

---

[1]) $f=O(g)$ означает, что $|fg^{-1}|$ меньше некоторой абсолютной постоянной, где f, $g>0$ могут зависеть от нескольких переменных. В частности, $f=h+O(g)$ означает, что $f-h=O(g)$.

Следовательно, используя (15), имеем $v = O\left(a_{n+1}^{1/2}\right)$ и, значит,

$$\frac{(2q+1)\theta-(2p+1)}{q_n\theta-p_n} = u + v\frac{q_{n+1}\theta-p_{n+1}}{q_n\theta-p_n} = u + O\left(a_{n+1}^{-1/2}\right). \quad (19)$$

Предположим теперь, что все a_n — четные. Так как

$$q_{n+1} = a_n q_n + q_{n-1}, \quad p_{n+1} = a_n p_n + p_{n-1}$$

и

$$p_0 = q_1 = 1, \quad p_1 = q_0 = 0,$$

то или p_n, q_{n+1} — нечетные, а q_n, p_{n+1} — четные, или наоборот. В обоих случаях u, v — нечетные по (17), и, значит, $uv \neq 0$. Таким образом, по (18), (19)

$$\frac{|2q+1|\,|(2q+1)\theta-(2p+1)|}{q_{n+1}\,|q_n\theta-p_n|} \geqslant 1 - O\left(a_n^{-1/2}\right) - O\left(a_{n+1}^{-1/2}\right).$$

Но по (15) $|2q/(2q+1)| \geqslant 1 - O\left(q_n^{-1}a_n^{-1/2}\right)$ и по (13)

$$4\,|q(q\theta-p-\alpha)| = |2q|\,|(2q+1)\theta-(2p+1)| >$$
$$> 1 - O\left(a_n^{-1/2}\right) - O\left(a_{n+1}^{-1/2}\right),$$

т. е. $> 1-4\varepsilon$, если $\min a_n$ больше постоянной, зависящей только от ε. Ясно, что $n\to\infty$, когда $|q|\to\infty$, и, значит,

$$\liminf |q(q\theta-p-\alpha)| \geqslant \frac{1}{4},$$

если, кроме того, $a_n\to\infty$. Построенные таким образом θ, α обладают указанными в теореме свойствами.

§ 3. Отрицательный результат.

Теорема III. *Пусть $\varphi(q)$ — любая положительная функция целочисленного аргумента q, такая, что*

$$\varphi(q)\to 0 \quad (q\to\infty). \quad (1)$$

Тогда существуют α и иррациональное θ, такие, что пара неравенств

$$|q| \leqslant Q, \quad \|q\theta-\alpha\| < \varphi(Q) \quad (2)$$

неразрешима для бесконечно многих значений Q.

Замечание. Функция $\varphi(q)$ может стремиться к нулю сколь угодно медленно[1]). В этом случае утверждение теоремы III является противоположным утверждению о том, что пара неравенств $0 < q < Q$, $\|q\theta\| \leqslant Q^{-1}$ всегда разрешима. В нашем примере α — рациональное, но нетрудно видоизменить построение так, чтобы получить α иррациональное.

Доказательство. Положим $\alpha = {}^1/_2$ и определим θ как предел последовательности рациональных чисел u_n/v_n ($n = 1, 2, \ldots$), где u_n, v_n — целые и v_n — нечетное. Следовательно,

$$\left| q\frac{u_n}{v_n} - \frac{1}{2} \right| \geqslant \frac{1}{2v_n} \tag{3}$$

при всех целых q. Определим целые Q_n для $n \geqslant 2$. Положим $u_1/v_1 = {}^1/_3$. Если u_n/v_n, Q_n уже определены для $n \leqslant N$, то определим Q_{N+1} как любое целое, такое, что

$$\left.\begin{aligned} \varphi(Q_{N+1}) &< (4v_N)^{-1} \qquad (N \geqslant 1), \\ Q_{N+1} &> 2Q_N \qquad (N \geqslant 2), \end{aligned}\right\} \tag{4}$$

что всегда возможно, согласно (1). Затем выберем u_{N+1}, v_{N+1} как любые целые, такие, что v_{N+1} — нечетное и

$$\left| \frac{u_{N+1}}{v_{N+1}} - \frac{u_N}{v_N} \right| < \frac{1}{8v_N Q_{N+1}}, \quad v_{N+1} > 2v_N.$$

Тогда предел

$$\theta = \lim u_n/v_n \qquad (n \to \infty)$$

существует, и

$$\left| \theta - \frac{u_n}{v_n} \right| < \frac{1}{8v_n Q_{n+1}} + \frac{1}{8v_{n+1}Q_{n+2}} + \ldots <$$
$$< \frac{1}{8v_n Q_{n+1}}\left(1 + \frac{1}{4} + \frac{1}{16} + \ldots\right) < \frac{1}{4v_n Q_{n+1}}.$$

Следовательно, если $|q| \leqslant Q_{n+1}$, то по (3) и (4)

$$\left\| q\theta - \frac{1}{2} \right\| \geqslant \left| q\frac{u_n}{v_n} - \frac{1}{2} \right| - q\left| \theta - \frac{u_n}{v_n} \right| \geqslant \frac{1}{2v_n} - \frac{1}{4v_n} > \varphi(Q_{n+1}).$$

Это и доказывает теорему для данных θ, α и для бесконечной последовательности целых $Q_2, Q_3, \ldots$.

§ 4. Линейная независимость над полем рациональных чисел. Говорят, что система чисел $\mu_1, \ldots, \mu_l$

[1]) Возьмем, например, $\varphi(q) = q^{-1}$. — *Прим. перев.*

называется *линейной независимой* (*над полем рациональных чисел*), если равенство $v_1\mu_1 + \ldots + v_l\mu_l = 0$, где $v_1, \ldots, v_l$ — рациональные числа, имеет место тогда и только тогда, когда $v_1 = \ldots = v_l = 0$. Число λ называется *линейно зависимым от* $\mu_1, \ldots, \mu_l$ (*над полем рациональных чисел*), если $\lambda = v_1\mu_1 + \ldots + v_l\mu_l$ при рациональных $v_1, \ldots, v_l$. Для доказательства теоремы IV нам понадобится следующая

Лемма 2. *Пусть* $\lambda_1, \ldots, \lambda_n$ — *действительные числа, не равные нулю одновременно. Тогда существует линейно независимая система чисел* $\mu_1, \ldots, \mu_l$ ($l \leqslant n$), *такая, что каждое* λ_j *линейно зависит от* $\mu_1, \ldots, \mu_l$.

Доказательство. Если $\lambda_1, \ldots, \lambda_n$ линейно независимы, то полагаем $l = n$, $\mu_j = \lambda_j$. В противном случае существуют рациональные $v_1, \ldots, v_n$, не равные нулю одновременно, такие, что имеет место равенство

$$v_1\lambda_1 + \ldots + v_n\lambda_n = 0. \tag{1}$$

Без ограничения общности можно считать, что $v_n \neq 0$. Тогда λ_n линейно зависит от $\lambda_1, \ldots, \lambda_{n-1}$. Если $\lambda_1, \ldots, \lambda_{n-1}$ линейно независимы, то полагаем $l = n - 1$, $\mu_j = \lambda_j$ ($j \leqslant n - 1$). В противном случае существует линейное соотношение $v_1\lambda_1 + \ldots$ $\ldots + v_{n-1}\lambda_{n-1} = 0$, в котором, не ограничивая общности, полагаем $v_{n-1} \neq 0$. Повторяя предыдущие рассуждения, видим, что λ_n, λ_{n-1} линейно зависят от $\lambda_1, \ldots, \lambda_{n-2}$. В конечном счете мы получим линейно независимое подмножество чисел $\mu_j = \lambda_j$ ($1 \leqslant j \leqslant l$) с соответствующим упорядочением λ_j, от которых линейно зависят $\lambda_1, \ldots, \lambda_n$.

Следствие. *Если* $\lambda_1 \neq 0$, *то можно выбрать* $\mu_1 = \lambda_1$.

Доказательство. Если в (1) $\lambda_1 \neq 0$, то тогда $v_j \neq 0$ при некотором $j \neq 1$; переставляя только числа $\lambda_2, \ldots, \lambda_n$, мы можем получить $v_n \neq 0$. Аналогично проводятся следующие этапы доказательства.

§ 5. Совместные приближения (теорема Кронекера).

Теорема IV (Кронекер)[1]. *Пусть даны* n *однородных линейных форм*

$$L_j(\mathbf{x}) = L_j(x_1, \ldots, x_m) \quad (1 \leqslant j \leqslant n)$$

[1]) Мы пользуемся векторными обозначениями (см. стр. 7). Другое доказательство теоремы IV дано в конце гл. V, § 8.

относительно любого числа m переменных x_i. Тогда каждое из следующих двух утверждений относительно действительного вектора $\boldsymbol{\alpha}=(\alpha_1, \ldots, \alpha_n)$ влечет за собой другое.

А. *Для любого $\varepsilon>0$ существует целый вектор $\mathbf{a}=(a_1, \ldots, a_n)$, такой, что одновременно выполняются неравенства*

$$\|L_j(\mathbf{a})-\alpha_j\|<\varepsilon \qquad (1 \leqslant j \leqslant n). \tag{1}$$

В. *Если $\mathbf{u}=(u_1, \ldots, u_n)$ — любой целый вектор, такой, что форма*

$$u_1L_1(\mathbf{x})+\ldots+u_nL_n(\mathbf{x})$$

относительно переменных x_i имеет целые коэффициенты, то

$$u_1\alpha_1+\ldots+u_n\alpha_n \tag{2}$$

число целое.

Доказательство. Очевидно, что утверждение А влечет за собой В, так как в § 1 этот факт был доказан для частного случая, а общий случай доказывается аналогично. Остается доказать, что В влечет за собой А.

Обозначим через Λ множество всех $\mathbf{z}=(z_1, \ldots, z_n)$, которые могут быть представлены в виде

$$z_j=L_j(\mathbf{x})-y_j, \tag{3}$$

где $\mathbf{x}=(x_1, \ldots, x_m)$, $\mathbf{y}=(y_1, \ldots, y_n)$ — целые. Ясно, что если $\mathbf{z}^{(1)}, \mathbf{z}^{(2)} \in \Lambda$, то $a\mathbf{z}^{(1)}+b\mathbf{z}^{(2)} \in \Lambda$ для всех целых a, b. Все точки $\mathbf{z}$ с целыми $z_1, \ldots, z_n$ принадлежат Λ. Пусть $\mathbf{u}=(u_1, \ldots, u_n)$ — целый вектор. Тогда, очевидно, для того чтобы форма

$$u_1L_1(\mathbf{x})+\ldots+u_nL_n(\mathbf{x})$$

была формой относительно $\mathbf{x}$ с целыми коэффициентами, необходимо и достаточно, чтобы $\mathbf{uz}$ было целым для всех $\mathbf{z} \in \Lambda$. Если $\mathbf{uz}$ — целое при некотором действительном $\mathbf{u}$ и для всех $\mathbf{z} \in \Lambda$, то $u_1, \ldots, u_n$ — целые, так как каждый вектор $(0, \ldots, 0, 1, 0, \ldots, 0) \in \Lambda$.

Теперь то, что нам надлежит доказать, можно сформулировать так: предположим, что $\mathbf{u}\boldsymbol{\alpha}=u_1\alpha_1+\ldots+u_n\alpha_n$ — целое число для всякого действительного $\mathbf{u}$, для которого

$\mathbf{uz}$ — целое при всех $\mathbf{z} \in \Lambda$. Тогда для любого $\varepsilon > 0$ существует вектор $\mathbf{z}^{(\varepsilon)} \in \Lambda$, такой, что

$$|z_j^{(\varepsilon)} - \alpha_j| < \varepsilon \qquad (1 \leqslant j \leqslant n).$$

Лемма 3. *Существует совокупность $s \leqslant n$ целых векторов $\mathbf{u}^{(t)}$ $(1 \leqslant t \leqslant s)$, таких, что:*

(1) *для того чтобы действительный вектор $\mathbf{u}$ удовлетворял условию $\mathbf{uz}$ — целое при всех $\mathbf{z} \in \Lambda$, необходимо и достаточно, чтобы $\mathbf{u} = v_1\mathbf{u}^{(1)} + \ldots + v_s\mathbf{u}^{(s)}$ при некоторых целых $v_1, \ldots, v_s$;*

(2) *после соответствующей перестановки форм $L_j(\mathbf{x})$, если в этом есть надобность, векторы $\mathbf{u}^{(t)}$ примут вид*

$$\mathbf{u}^{(t)} = (0, \ldots, 0, u_{t,t}, u_{t,t+1}, \ldots, u_{t,n}), \qquad u_{t,t} \neq 0.$$

Замечание. Таким образом, бесконечное число условий $\mathbf{u\alpha}$ — целое заменяется конечным числом условий $\mathbf{u}^{(t)}\boldsymbol{\alpha}$ — целое.

Доказательство. Ясно, что рассматриваемые векторы образуют модуль в смысле приложения А. Поэтому справедливость леммы 3 следует из леммы 1 и ее следствия приложения А, так как вектор $\mathbf{u}$, как было замечено выше, всегда целый.

Следствие 1. *Если $\rho_1, \ldots, \rho_s$ — действительные числа и*

$$\rho_1\mathbf{u}^{(1)} + \ldots + \rho_s\mathbf{u}^{(s)} = 0,$$

то

$$\rho_1 = \ldots = \rho_s = 0.$$

Следствие 2. *$(n-1)$-мерные векторы, полученные из $\mathbf{u}^{(2)}, \ldots, \mathbf{u}^{(s)}$ вычеркиванием первой координаты 0, обладают тем же свойством относительно форм $L_2, \ldots, L_n$, что и $\mathbf{u}^{(1)}, \ldots, \mathbf{u}^{(s)}$ относительно $L_1, \ldots, L_n$.*

Доказательство очевидно.

Лемма 4. *При надлежащем выборе*[1]) *векторов $\mathbf{u}^{(1)}, \ldots, \mathbf{u}^{(s)}$ можно считать, что для любого множе-*

[1]) Нетрудно доказать, что любые векторы $\mathbf{u}^{(1)}, \ldots, \mathbf{u}^{(s)}$, удовлетворяющие лемме 3, удовлетворяют и лемме 4, так что замечание о выборе векторов можно опустить.

ства целых $\omega_1, \ldots, \omega_s$ *найдется вектор* $\mathbf{z} \in \Lambda$, *такой, что*

$$\mathbf{u}^{(t)}\mathbf{z} = \omega_t \qquad (1 \leqslant t \leqslant s).$$

Доказательство. Достаточно, очевидно, найти векторы $\mathbf{z}^{(r)} \in \Lambda$ $(1 \leqslant r \leqslant s)$, такие, что

$$\mathbf{u}^{(t)}\mathbf{z}^{(t)} = 1,$$

$$\mathbf{u}^{(t)}\mathbf{z}^{(r)} = 0, \quad \text{если} \quad r \neq t,$$

так как тогда теорема справедлива при $\mathbf{z} = \omega_1\mathbf{z}^{(1)} + \ldots$ $\ldots + \omega_s\mathbf{z}^{(s)}$.

Предположим сначала, что $s = 1$. Если d', d'' — целые вида $\mathbf{u}^{(1)}\mathbf{z}, \mathbf{z} \in \Lambda$, то тогда и $a'd' + a''d''$ имеют тот же вид при любых целых a', a''. Таким образом, множество значений, принимаемых величиной $\mathbf{u}^{(1)}\mathbf{z}$, есть множество всех кратных некоторого целого числа $d > 0$. Но тогда $\mathbf{uz}$ — целое для всех $\mathbf{z} \in \Lambda$, где $\mathbf{u} = d^{-1}\mathbf{u}^{(1)}$. По лемме 3 $d = 1$. Теперь $\mathbf{u}^{(1)}\mathbf{z}^{(1)} = d = 1$ для некоторого $\mathbf{z}^{(1)} \in \Lambda$ по определению d, что и доказывает лемму в случае $s = 1$.

Предположим теперь, что $s > 1$ и что лемма 4 доказана для меньших значений s. В частности, рассматривая только

$$L_2(\mathbf{x}), \ldots, L_n(\mathbf{x}),$$

можно найти

$$\mathbf{z}^{(r)} \quad (2 \leqslant r \leqslant s),$$

такие, что

$$\mathbf{u}^{(t)}\mathbf{z}^{(t)} = 1 \qquad (2 \leqslant t \leqslant s),$$

$$\mathbf{u}^{(t)}\mathbf{z}^{(r)} = 0 \quad (2 \leqslant r, \quad t \leqslant s; \quad r \neq t).$$

Обозначим целые $\mathbf{u}^{(1)}\mathbf{z}^{(t)}$ через h_t. Рассматривая

$$\mathbf{u}^{(1)} - h_2\mathbf{u}^{(2)} - \ldots - h_s\mathbf{u}^{(s)}$$

вместо $\mathbf{u}^{(1)}$ (что не нарушает справедливости леммы 3), мы можем считать, что

$$\mathbf{u}^{(1)}\mathbf{z}^{(t)} = 0 \qquad (2 \leqslant t \leqslant s). \tag{4}$$

Рассуждая, как и в случае $s = 1$, найдем вектор $\mathbf{z}^{(1)} \in \Lambda$, такой, что

$$\mathbf{u}^{(1)}\mathbf{z}^{(1)} = 1. \tag{5}$$

Обозначим целые $\mathbf{u}^{(t)}\mathbf{z}^{(1)}$ через g_t $(2 \leqslant t \leqslant s)$. Рассматривая $\mathbf{z}^{(1)} - g_2\mathbf{z}^{(2)} - \ldots - g_s\mathbf{z}^{(s)}$ вместо $\mathbf{z}^{(1)}$, можно считать, не нарушая условий (5), что

$$\mathbf{u}^{(t)}\mathbf{z}^{(1)} = 0 \qquad (2 \leqslant t \leqslant s).$$

Этим лемма 4 доказана.

Следствие. *Если теорема* IV *справедлива для всех* $\boldsymbol{\alpha}$, *таких, что*

$$\mathbf{u}^{(t)}\boldsymbol{\alpha} = 0 \qquad (1 \leqslant t \leqslant s), \tag{6}$$

то она справедлива и всегда.

Доказательство. Если $u^{(t)}\alpha = \omega_t$ — целое $(1 \leqslant t \leqslant s)$ и $\mathbf{z}' \in \Lambda$ определяется леммой 4, то

$$\mathbf{u}^{(t)}\boldsymbol{\alpha}' = 0, \qquad \boldsymbol{\alpha}' = \boldsymbol{\alpha} - \mathbf{z}' \qquad (1 \leqslant t \leqslant s).$$

Справедливость теоремы для $\boldsymbol{\alpha}'$ означает, что для любого $\varepsilon > 0$ существует вектор $\mathbf{z}'' \in \Lambda$, такой, что

$$|z_j'' - \alpha_j'| < \varepsilon \qquad (1 \leqslant j \leqslant n).$$

Но тогда $\mathbf{z}^{(\varepsilon)} = \mathbf{z}'' - \mathbf{z}' \in \Lambda$ и

$$|z_j^{(\varepsilon)} - \alpha_j| < \varepsilon \qquad (1 \leqslant j \leqslant n),$$

что и требовалось доказать.

Лемма 5. *Существует* $\varepsilon_0 > 0$, *такое, что все векторы* $\mathbf{z} \in \Lambda$ *с*

$$|z_j| < \varepsilon_0 \qquad (1 \leqslant j \leqslant n)$$

удовлетворяют равенству

$$\mathbf{u}^{(t)}\mathbf{z} = 0 \qquad (1 \leqslant t \leqslant s).$$

Доказательство. Выберем ε_0 так, что

$$\varepsilon_0(|u_{t1}| + \ldots + |u_{tn}|) < 1 \qquad (1 \leqslant t \leqslant s).$$

Если $\max |z_j| < \varepsilon_0$, то $|\mathbf{u}^{(t)}\mathbf{z}| < 1$. Но $\mathbf{u}^{(t)}\mathbf{z}$ — целое, если $\mathbf{z} \in \Lambda$.

Лемма 6. *Предположим, что существует* $\varepsilon_1 > 0$ *и вектор* $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_n)$, *такой, что все векторы* $\mathbf{z} \in \Lambda$, *у которых*

$$|z_j| < \varepsilon_1 \qquad (1 \leqslant j \leqslant n), \tag{7}$$

удовлетворяют также равенству

$$\boldsymbol{\lambda}\mathbf{z}=0. \tag{8}$$

Тогда

$$\boldsymbol{\lambda}=\nu_1\mathbf{u}^{(1)}+\ldots+\nu_s\mathbf{u}^{(s)}, \tag{9}$$

где $\nu_1, \ldots, \nu_s$ — *некоторые действительные числа.*

Доказательство. Пусть ε — любое сколь угодно малое число, в частности

$$0<\varepsilon<\varepsilon_1.$$

Предположим, что $\mathbf{z}\neq\mathbf{0}$ принадлежит Λ и удовлетворяет равенству (7). По теореме VI гл. I существуют целые $\omega\neq 0$, $\mathbf{t}=(t_1, \ldots, t_n)$, такие, что

$$\max_j|\omega z_j-t_j|<\varepsilon<\varepsilon_1. \tag{10}$$

Но $\omega\mathbf{z}-\mathbf{t}\in\Lambda$, так как $\mathbf{z}\in\Lambda$ и все точки с целыми координатами также принадлежат Λ. Таким образом, по условиям леммы имеем

$$\boldsymbol{\lambda}\mathbf{z}=\boldsymbol{\lambda}(\omega\mathbf{z}-\mathbf{t})=0$$

и, значит,

$$\boldsymbol{\lambda}\mathbf{t}=0. \tag{11}$$

По лемме 2 существуют числа $\mu_1, \ldots, \mu_l$ $(l\leqslant n)$, линейно независимые над полем рациональных чисел, от которых линейно зависят $\lambda_1, \ldots, \lambda_n$, например

$$\boldsymbol{\lambda}=\mu_1\mathbf{v}^{(1)}+\ldots+\mu_l\mathbf{v}^{(l)}$$

с рациональными векторами $\mathbf{v}^{(1)}, \ldots, \mathbf{v}^{(l)}$.
Тогда из (11) следует, что

$$\mu_1\mathbf{v}^{(1)}\mathbf{t}+\ldots+\mu_l\mathbf{v}^{(l)}t=0$$

и, значит,

$$\mathbf{v}^{(i)}\mathbf{t}=0 \qquad (1\leqslant i\leqslant l), \tag{12}$$

так как $\mathbf{v}^{(i)}$ и $\mathbf{t}$ — рациональные. Но теперь по (10) и (12)

$$|\mathbf{v}^{(i)}\mathbf{z}|\leqslant|\omega\mathbf{v}^{(i)}\mathbf{z}|=|\mathbf{v}^{(i)}(\omega\mathbf{z}-\mathbf{t})|<R^{(i)}\varepsilon,$$

где $R^{(i)}$ — сумма абсолютных значений координат векторов $\mathbf{v}^{(i)}$. Следовательно,

$$\mathbf{v}^{(i)}\mathbf{z}=0 \qquad (1\leqslant i\leqslant l), \tag{13}$$

так как ε сколь угодно мало. Таким образом, из (7) и (8) мы получили l уравнений (13), которые по форме подобны первоначальному уравнению (8) и в которых, кроме того, все координаты векторов $\mathbf{v}^{(l)}$ рациональны. Если все $\mathbf{v}^{(l)}$ имеют вид (9), то такой же вид имеет и $\boldsymbol{\lambda}$. Следовательно, достаточно доказать лемму для случая, когда все $\lambda_1, \ldots, \lambda_n$ рациональны.

Положим теперь, что $\lambda_1, \ldots, \lambda_n$ рациональны и $\mathbf{z}$ — любой вектор из Λ. Как и ранее, существуют целые $\omega \neq 0$, $\mathbf{t} = (t_1, \ldots, t_n)$, такие, что

$$|\omega z_j - t_j| < \varepsilon_1 \qquad (1 \leqslant j \leqslant n).$$

Так как $\omega\mathbf{z} - \mathbf{t} \in \Lambda$, то $\boldsymbol{\lambda}(\omega\mathbf{z} - \mathbf{t}) = 0$. Значит, $\boldsymbol{\lambda}\mathbf{z}$ рационально, так как $\boldsymbol{\lambda}, \mathbf{t}$ рациональны и $\omega \neq 0$. В частности, все коэффициенты при $\mathbf{x}$, $\mathbf{y}$ в

$$\sum_j \lambda_j (L_j(\mathbf{x}) - y_j)$$

рациональны. Таким образом, существует целое q, такое, что все коэффициенты в

$$\sum (q\lambda_j)(L_j(\mathbf{x}) - y_j)$$

являются целыми. По лемме 3 $q\boldsymbol{\lambda} = p_1\mathbf{u}^{(1)} + \ldots + p_s\mathbf{u}^{(s)}$ при некоторых целых $p_1, \ldots, p_s$. Отсюда получается (9) при $\nu_i = p_i/q$.

Лемма 7. *Существует $n - s$ линейно независимых*[1]) *векторов*

$$\mathbf{z}^{(1)}, \ldots, \mathbf{z}^{(n-s)} \in \Lambda,$$

у которых $\max|z_j| < \varepsilon$ *для любого* $\varepsilon > 0$.

Доказательство. Будем строить векторы $\mathbf{z}^{(1)}, \ldots, \mathbf{z}^{(n-s)}$ последовательно. Предположим, что мы уже имеем q векторов $\mathbf{z}^{(1)}, \ldots, \mathbf{z}^{(q)}$, где $0 \leqslant q < n - s$. Очевидно, что существует вектор $\boldsymbol{\lambda}$, не представимый в виде $\boldsymbol{\lambda} = \nu_1\mathbf{u}^{(1)} + \ldots + \nu_s\mathbf{u}^{(s)}$, такой, что

$$\boldsymbol{\lambda}\mathbf{z}^{(p)} = 0 \qquad (1 \leqslant p \leqslant q). \tag{14}$$

---

[1]) То есть из $\rho_1\mathbf{z}^{(1)} + \ldots + \rho_{n-s}\mathbf{z}^{(n-s)} = 0$ при действительных $\rho_1, \ldots, \rho_{n-s}$ следует, что $\rho_1 = \ldots = \rho_{n-s} = 0$.

По лемме 6 существует вектор $\mathbf{z}^{(q+1)} \in \Lambda$ с $\max|z_j| < \varepsilon$, такой, что $\lambda\mathbf{z}^{(q+1)} \neq 0$. Тогда $\mathbf{z}^{(1)}, \ldots, \mathbf{z}^{(q+1)}$ — линейно независимые векторы.

Доказательство теоремы IV. По следствию из леммы 4 достаточно рассмотреть $\boldsymbol{\alpha}$ в пространстве $\mathscr{S}$, определенном равенствами

$$\mathbf{u}^{(t)}\boldsymbol{\alpha} = 0 \qquad (1 \leqslant t \leqslant s).$$

Пусть $\varepsilon > 0$ — как угодно мало, а $\mathbf{z}^{(1)}, \ldots, \mathbf{z}^{(n-s)}$ — векторы, о которых говорится в лемме 7. По лемме 5 все они лежат в пространстве $\mathscr{S}$, если $\varepsilon < \varepsilon_0$, что можно предполагать. Так как размерность пространства $\mathscr{S}$ равна $n - s$, то по следствию 1 леммы 3 имеем

$$\boldsymbol{\alpha} = \beta_1\mathbf{z}^{(1)} + \ldots + \beta_s\mathbf{z}^{(s)},$$

где $\beta_1, \ldots, \beta_s$ — некоторые действительные числа. Существуют целые $b_1, \ldots, b_s$, для которых

$$|\beta_r - b_r| \leqslant \frac{1}{2}.$$

Тогда

$$\mathbf{z}^{(\varepsilon)} = b_1\mathbf{z}^{(1)} + \ldots + b_s\mathbf{z}^{(s)} \in \Lambda.$$

Далее, абсолютная величина j-й координаты вектора

$$\boldsymbol{\alpha} - \mathbf{z}^{(\varepsilon)} = (\beta_1 - b_1)\,\mathbf{z}^{(1)} + \ldots$$

не более чем

$$|\beta_1 - b_1||z_{1j}| + \ldots < \frac{1}{2}s\varepsilon \leqslant \frac{1}{2}n\varepsilon.$$

Так как ε сколь угодно мало, этим теорема доказана.

Позднее нам понадобится следующее

Следствие из теоремы IV[1]). *Для любого* $\varepsilon > 0$ *существует число* $X = X(\varepsilon)$, *такое, что для каждого действительного вектора* $\boldsymbol{\alpha}$, *удовлетворяющего* B, *найдется целый вектор* $\mathbf{a}$, *для которого*

$$\|L_j(\mathbf{a}) - \alpha_j\| < \varepsilon \qquad (1 \leqslant j \leqslant n)$$

---

[1]) Это следует также из леммы Гейне — Бореля, если ее применить к гиперкубу $0 \leqslant \alpha_j \leqslant 1$.

и

$$\max(|a_1|, \ldots, |a_m|) \leqslant X(\varepsilon).$$

Доказательство. Можно считать, не ограничивая общности, что $0 \leqslant \alpha_j < 1$. Тогда если α принадлежит $\mathscr{S}$, то числа $\beta_1, \ldots, \beta_{n-s}$, введенные выше, ограничены и, значит, имеется только конечное число возможных значений для $b_1, \ldots, b_{n-s}$, т. е. для $\mathbf{a}$. Доказательство следствия леммы 4 показывает, что вообще вектор $\mathbf{a}$ может быть взят из конечного множества, так как при $0 \leqslant \alpha_j < 1$ существует конечное число возможных значений для $\omega_1, \ldots, \omega_s$. Таким образом, в качестве $X(\varepsilon)$ можно взять наибольшую координату в конечном множестве векторов $\mathbf{x}$.

ЗАМЕЧАНИЯ

§ 2. Полагая $\varepsilon \to 0$ в теореме I В, мы видим, что существует бесконечно много целых решений x, y неравенств (2.1) и (2.2) при условии, что нет решения уравнения $L_1 + \rho_1 = 0$. Но если такое решение существует, то очень возможно, что оно является единственным решением неравенств (2.1) и (2.2), например, для $\rho_1 = \rho_2 = 0$, $L_1 L_2 = x^2 + xy - y^2$ [ср. Морделл (1951) и Касселс (1954b)].

Минковский высказал предположение, что если $L_j(\mathbf{x})$ суть n линейных форм от n переменных $\mathbf{x}$ с определителем $\Delta \neq 0$, а $\alpha_1, \ldots, \alpha_n$ — любые числа, то существуют целые $\mathbf{x}$, для которых

$$\prod |L_j(\mathbf{x}) - \alpha_j| \leqslant 2^{-n} |\Delta|.$$

Теорема I есть подтверждение этого предположения для $n = 2$. Современное состояние этого вопроса, а также соображения относительно того, когда существует бесконечно много таких целых $\mathbf{x}$, см. у Касселса (1952a) и у Роджерса (1954).

„Асимметрические" аналоги теоремы II см. у Блэни (1950), Сойера (1950), Барнса и Суиннертона-Дайера (1955). Случай $x > 0$ рассмотрен у Касселса (1954a).

Много работ посвящено улучшению постоянной $^1/_4 |\Delta|$ в теореме I в случае, когда произведение $L_1 L_2$ есть данная неопределенная квадратичная форма с целыми коэффициентами [см. Барнс и Суиннертон-Дайер (1952)].

Использование непрерывных дробей в доказательстве теоремы II В служит примером общности техники в случае однородной и неоднородной задач. Другое доказательство более слабого результата см. у Канагасабапатхи (1952), а более сильный результат см. у Барнса (1956).

§ 3. Хинчин (1926).

§ 5. Другие (родственные) „теоремы Кронекера" имеются у Перрона (1913). Интересная точка зрения имеется у Турана (1953).

Глава IV

РАВНОМЕРНОЕ РАСПРЕДЕЛЕНИЕ

§ 1. Введение. Положим, что θ иррационально. Согласно результатам гл. III, существуют целые q, для которых $\|q\theta-\alpha\|$ сколь угодно мало при любом заданном α. В частности, существуют целые q, такие, что $\{q\theta\}$ произвольно мало отличаются от любого заданного β из единичного интервала $0\leqslant\beta<1$, или, другими словами, множество чисел $\{q\theta\}$ всюду плотно в единичном интервале. В действительности же имеет место нечто большее. Обозначим через $F_Q(\alpha, \beta)$ при $0\leqslant\alpha<\beta\leqslant 1$ число целых q, таких[1]), что

$$\alpha\leqslant\{q\theta\}<\beta, \quad 1\leqslant q\leqslant Q.$$

Тогда $Q^{-1}F_Q(\alpha, \beta)\rightarrow\beta-\alpha$ при $Q\rightarrow\infty$ равномерно относительно α и β. Это значит, что асимптотически каждый интервал $\alpha\leqslant x<\beta$ содержит „правильное число“ чисел $\{q\theta\}$.

Аналогичные результаты имеют место и для совместного приближения. Если $\theta_1, \ldots, \theta_n$ таковы, что соотношение $u_1\theta_1+\ldots+u_n\theta_n=v$ не имеет места ни при каких целых $u_1, \ldots, u_n, v$, одновременно не равных нулю, то множество дробных долей

$$(\{q\theta_1\}, \ldots, \{q\theta_n\})$$

равномерно распределено в единичном гиперкубе $0\leqslant x_j<1$.

В § 2 мы дадим формальное определение равномерного распределения, а в § 3 докажем (в более общем виде) упомянутые выше теоремы. Наконец, в § 4, 5 мы рассмотрим один общий критерий равномерного распределения, использующий тригонометрические суммы. С помощью этого критерия получаются очень прозрачные доказательства резуль-

---

[1]) Причина одновременного появления знаков $<$ и $\leqslant$ чисто техническая.

татов § 2 и некоторых общих свойств равномерного распределения.

Введем следующие определения. Будем говорить, что два числа $z^{(1)}$, $z^{(2)}$ или, более общо, два вектора $\mathbf{z}^{(1)}$, $\mathbf{z}^{(2)}$ *сравнимы по модулю* 1 или просто сравнимы, если разность $\mathbf{z}^{(1)}-\mathbf{z}^{(2)}$ имеет только целые координаты. Условно этот факт будем записывать так:

$$\mathbf{z}^{(1)}\equiv\mathbf{z}^{(2)}.$$

Это определение симметрично относительно $\mathbf{z}^{(1)}$ и $\mathbf{z}^{(2)}$. Далее, если $\mathbf{z}^{(1)}\equiv\mathbf{z}^{(2)}$, а $\mathbf{z}^{(2)}\equiv\mathbf{z}^{(3)}$, то и $\mathbf{z}^{(1)}\equiv\mathbf{z}^{(3)}$. Таким образом, векторы распадаются на классы сравнимых векторов. Так как мы интересуемся только дробными долями, то данные векторы можно заменять векторами, сравнимыми с данными. Можно дать интерпретацию действительных чисел, в которой сравнимые числа представляются одной и той же точкой, полученной наматыванием действительной оси на окружность длиной 1. В этой интерпретации число z представляется точкой окружности, для которой центральный угол равен $2\pi z$. При рассмотрении равномерности распределения дробных долей множества чисел полезно иметь в виду эту интерпретацию. Аналогично предыдущему можно, естественно, интерпретировать классы сравнимых m-мерных векторов на „m-мерном торе“. Однако такой интерпретацией пользоваться мы не будем.

§ 2. Определение отклонения. Предположим, что дано конечное число векторов $\mathbf{z}^{(q)}=(z_{q1}, \ldots, z_{qn})$ $(1\leqslant q\leqslant Q)$ в единичном гиперкубе

$$0\leqslant z_j<1 \qquad (1\leqslant j\leqslant n). \tag{1}$$

Обозначим через $F(\boldsymbol{\alpha}, \boldsymbol{\beta})$, где $0\leqslant\alpha_j<\beta_j\leqslant 1$ $(1\leqslant j\leqslant n)$, число векторов $\mathbf{z}^{(q)}$, лежащих в гиперпараллелепипеде

$$\alpha_j\leqslant z_j<\beta_j \tag{2}$$

объема $\prod(\beta_j-\alpha_j)$. Тогда

$$D=\sup_{\boldsymbol{\alpha},\,\boldsymbol{\beta}}\left|Q^{-1}F(\boldsymbol{\alpha}, \boldsymbol{\beta})-\prod(\beta_j-\alpha_j)\right| \tag{3}$$

называется *отклонением* векторов $\mathbf{z}^{(q)}$. Ясно, что

$$0 < D \leqslant 1.$$

Если имеется бесконечная последовательность векторов $\mathbf{z}^{(q)}$ $(1 \leqslant q < \infty)$ с условием (1), то через D_Q обозначим отклонение первых Q из них. Если при $Q \to \infty$

$$D_Q \to 0, \tag{4}$$

то будем говорить, что последовательность *равномерно распределена* в единичном гиперкубе. Более общо, пусть имеется множество векторов $\mathbf{z}^{(\mathbf{q})}$ с (1), связанных с множеством m целых положительных векторов $\mathbf{q} = (q_1, \ldots, q_m)$. Обозначим через $D_{Q_1 \ldots Q_m}$ отклонение $Q_1 Q_2 \ldots Q_m$ векторов $\mathbf{z}^{(\mathbf{q})}$ с $1 \leqslant q_i \leqslant Q_i$ $(1 \leqslant i \leqslant m)$. Будем говорить, что множество векторов $\mathbf{z}^{(\mathbf{q})}$ *равномерно распределено*, если $D_{Q_1 \ldots Q_m} \to 0$ при Q_i, стремящихся к ∞ независимо друг от друга[1]).

Пусть $\mathbf{z}$ — любой вектор. Тогда через $\{\mathbf{z}\}$ обозначим вектор $(\{z_1\}, \ldots, \{z_n\})$, координаты которого равны дробным долям вектора $\mathbf{z}$. Будем говорить, что множество векторов $\mathbf{z}^{(q)}$ или $\mathbf{z}^{(\mathbf{q})}$ *равномерно распределено по модулю* 1, если равномерно распределено соответствующее множество их дробных долей.

На первый взгляд кажется, что было бы естественно оценивать равномерность распределения по модулю 1 множества векторов $\mathbf{z}^{(q)}$ $(1 \leqslant q \leqslant Q)$ с помощью отклонения D их дробных долей, но по техническим соображениям удобнее поступать по-другому (ср. с замечаниями в конце § 1). Пусть $\Lambda^{(Q)}$ — множество всех векторов $\mathbf{x} = \mathbf{z}^{(q)} + \mathbf{t}$, $\mathbf{t}$ — целый вектор. Пусть для любых $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ с $\beta_j \geqslant \alpha_j$ $(1 \leqslant j \leqslant n)$ $F^*(\boldsymbol{\alpha}, \boldsymbol{\beta})$ обозначает число точек $\mathbf{x} \in \Lambda^{(Q)}$ при $\alpha_j \leqslant x_j < \beta_j$. Ясно, что при целом $\mathbf{t}$

$$F^*(\boldsymbol{\alpha} + \mathbf{t}, \boldsymbol{\beta} + \mathbf{t}) = F^*(\boldsymbol{\alpha}, \boldsymbol{\beta}), \tag{5}$$

и для $0 \leqslant \alpha_j < \beta_j \leqslant 1$

$$F^*(\boldsymbol{\alpha}, \boldsymbol{\beta}) = F(\boldsymbol{\alpha}, \boldsymbol{\beta}), \tag{6}$$

где F определяется через дробные доли, как указано выше.

---

[1]) То есть $D_{Q_1 \ldots Q_m} < \varepsilon$, как только все Q_i больше некоторой постоянной, зависящей от ε.

Назовем *отклонением по модулю* 1

$$D^* = \sup_{0 \leqslant \beta_j - \alpha_j \leqslant 1} \left| Q^{-1} F^*(\alpha, \beta) - \prod (\beta_j - \alpha_j) \right|, \tag{7}$$

где вектор α пробегает все значения, но, согласно (5), может быть ограничен и единичным кубом. Покажем, что

$$D \leqslant D^* \leqslant 2^n D, \tag{8}$$

причем левая часть этого неравенства тривиальна по (3), (6), (7). Любая область $\alpha_j \leqslant x_j < \beta_j$, где $0 \leqslant \alpha_j < 1$, $\beta_j - \alpha_j \leqslant 1$, разлагается[1]) самое большее на 2^n областей вида $\alpha'_j \leqslant x_j < \beta'_j$, где для каждого j независимо

$$\text{или } 0 \leqslant \alpha'_j < \beta'_j \leqslant 1, \text{ или } 1 \leqslant \alpha'_j < \beta'_j \leqslant 2. \tag{9}$$

Тогда $F^*(\alpha, \beta) = \sum F^*(\alpha', \beta')$ по определению и

$$\prod (\beta_j - \alpha_j) = \sum \prod (\beta'_j - \alpha'_j),$$

так как $\prod (\beta_j - \alpha_j)$ есть объем всей области, а $\prod (\beta'_j - \alpha'_j)$ есть объем одной из частей. Следовательно,

$$\left| Q^{-1} F^*(\alpha, \beta) - \prod (\beta_j - \alpha_j) \right| \leqslant \\ \leqslant \sum \left| Q^{-1} F^*(\alpha', \beta') - \prod (\beta'_j - \alpha'_j) \right|. \tag{10}$$

Но в (10) каждое слагаемое не более D по (2), (3), (5), (6), (9), а всех слагаемых самое большее 2^n. Согласно (7), это и доказывает неравенства (8).

Согласно (8), равномерность распределения по модулю 1 может быть определена как с помощью $D_Q \to 0$, так и с помощью $D^*_Q \to 0$ (в очевидных обозначениях).

Относительно среднего по α функции $F^*(\alpha, \alpha + \gamma)$ при любом фиксированном γ ($\gamma_j > 0$) справедлива следующая

Лемма 1. *Для любого* γ *с* $\gamma_j > 0$ $(1 \leqslant j \leqslant n)$ (γ_j *не обязательно* $\leqslant 1$) *имеем*

$$\int_{0 \leqslant \alpha_j < 1} \cdots \int F^*(\alpha, \alpha + \gamma)\, d\alpha = Q \prod \gamma_j; \quad d\alpha = d\alpha_1 \ldots d\alpha_n.$$

---

[1]) Читателю рекомендуется начертить схему для $n = 2$, $\alpha = (^1/_2, {}^3/_4)$, $\beta = (^4/_3, {}^3/_2)$.

Доказательство.

$$F^*(\alpha, \alpha+\gamma) = \sum_{1 \leqslant q \leqslant Q} f_q(\alpha, \gamma), \tag{11}$$

где $f_q(\alpha, \gamma)$ — число векторов $\mathbf{x} = \mathbf{z}^{(q)} + \mathbf{t}$ ($\mathbf{t}$ — целый вектор) с $\alpha_j \leqslant x_j < \alpha_j + \gamma_j$ $(1 \leqslant j \leqslant n)$. Но

$$f_q(\alpha, \gamma) = \sum_{\mathbf{t}} \varphi_q(\alpha - \mathbf{t}, \gamma),$$

где суммирование проводится по всем целым векторам $\mathbf{t}$, а $\varphi_q(\beta, \gamma) = 1$, если β находится в области

$$z_{qj} \geqslant \beta_j > z_{qj} - \gamma_j \qquad (1 \leqslant j \leqslant n)$$

объема $\prod \gamma_j$, в противном случае $\varphi_q(\beta, \gamma) = 0$. Следовательно,

$$\int_{0 \leqslant \alpha_j < 1} \cdots \int f_q(\alpha, \gamma)\, d\alpha = \sum_{\mathbf{t}} \int_{0 \leqslant \alpha_j < 1} \cdots \int \varphi_q(\alpha - \mathbf{t}, \gamma)\, d\alpha =$$
$$= \int_{-\infty < \alpha_j < \infty} \cdots \int \varphi_q(\alpha, \gamma)\, d\alpha = \prod \gamma_j.$$

Это и доказывает лемму, согласно (11).

§ 3. Равномерное распределение линейных форм.

Теорема 1. *Пусть* $L_j(\mathbf{x})$ $(1 \leqslant j \leqslant n)$ — *однородные формы относительно* m *переменных* $\mathbf{x} = (x_1, \ldots, x_m)$. *Предположим, что единственное множество целых* $u_1, \ldots, u_n$, *таких, что*

$$u_1 L_1(\mathbf{x}) + \ldots + u_n L_n(\mathbf{x})$$

имеет целые коэффициенты при $x_1, \ldots, x_m$, *есть* $u_1 = \ldots = u_n = 0$. *Тогда множество векторов* $\mathbf{z}^{(\mathbf{x})} = (L_1(\mathbf{x}), \ldots, L_n(\mathbf{x}))$ *при целых* $\mathbf{x}$ *равномерно распределено по модулю* 1.

Замечание. Читатель без труда сформулирует соответствующий результат для случая, когда $\sum u_l L_l(\mathbf{x})$ имеет целые коэффициенты при некотором $\mathbf{u} \neq \mathbf{0}$, и видоизменит надлежащим образом доказательство.

Доказательство. Основная идея доказательства уже ясна при $m = n = 1$. Для простоты мы ограничимся этим

случаем. Тогда $L_1(\mathbf{x}) = \theta x_1$ при некотором иррациональном θ. Записывая x вместо x_1, мы покажем, что функция θx ($x = 1, 2, \ldots$) равномерно распределена по модулю 1. По следствию из теоремы IV гл. III, стр. 73, для любого $\varepsilon > 0$ существует такое $X(\varepsilon)$, что при любом действительном α найдутся целые x, y, такие, что

$$|\theta x - y - \alpha| < \varepsilon, \qquad |x| \leqslant X(\varepsilon). \tag{1}$$

Пусть теперь $Q > X(\varepsilon)$. Рассмотрим множество $\Lambda^{(Q)}$, введенное в предыдущем параграфе, т. е. множество чисел $q\theta - p$, где p, q — целые и $1 \leqslant q \leqslant Q$. Пусть $F^*(\alpha, \beta)$ определяется относительно множества $\Lambda^{(Q)}$ так же, как и в § 2. Покажем, что

$$F^*(\alpha, \beta) \leqslant F^*(\gamma, \delta) + X, \; X = X(\varepsilon), \tag{2}$$

где α, β, γ, δ — любые четыре числа, удовлетворяющие неравенству

$$0 < \beta - \alpha = \delta - \gamma - 2\varepsilon \leqslant 1. \tag{3}$$

Здесь $F^*(\alpha, \beta)$ — число пар целых p, q с условием

$$1 \leqslant q \leqslant Q \tag{4}$$

и

$$\alpha \leqslant q\theta - p < \beta. \tag{5}$$

Пусть x_0, y_0 — решение неравенств

$$|x_0\theta - y_0 - (\gamma + \varepsilon - \alpha)| < \varepsilon, \quad |x_0| \leqslant X(\varepsilon). \tag{6}$$

Тогда, согласно (3), (5) и (6), целые $q' = q + x_0$, $p' = p + y_0$ удовлетворяют неравенству

$$\gamma \leqslant q'\theta - p' < \delta. \tag{7}$$

Но $F^*(\gamma, \delta)$ есть число решений неравенства (7) с

$$1 \leqslant q' \leqslant Q. \tag{8}$$

Так как $1 \leqslant q \leqslant Q$, то неравенство (8) имеет место, кроме тех случаев, когда $1 \leqslant q \leqslant |x_0|$ при $x_0 < 0$ и когда $Q - x_0 + 1 \leqslant q \leqslant Q$ при $x_0 > 0$. В любом случае существует самое большее $|x_0| \leqslant X$ значений q, таких, что (4) [но не (8)] имеет место; для каждого q неравенству (5) удовлетворяет самое большее одно p, так как $\beta \leqslant \alpha + 1$. Следовательно, число решений неравенств (4) и (5) отличается от числа решений неравенств (7), (8) самое большее на X. Это и доказывает (2).

Таким образом, при фиксированных α, β, $0<\beta-\alpha\leqslant 1$, имеем, согласно (2), (3) и лемме 1,

$$F^*(\alpha,\ \beta)\leqslant X+\int_0^1 F^*(\gamma,\ \gamma+\beta-\alpha+2\varepsilon)d\gamma=$$
$$=X+(\beta-\alpha+2\varepsilon)Q. \qquad (9)$$

Аналогично, взаимно заменяя пары чисел α, β и γ, δ, имеем при $2\varepsilon<\beta-\alpha\leqslant 1$

$$F^*(\alpha,\ \beta)\geqslant -X+\int_0^1 F^*(\gamma,\ \gamma+\beta-\alpha-2\varepsilon)\,d\gamma=$$
$$=-X+(\beta-\alpha-2\varepsilon)Q. \qquad (10)$$

Очевидно, всегда

$$F^*(\alpha,\ \beta)\geqslant 0. \qquad (11)$$

Поэтому, в силу (9), (10), (11), имеем

$$\left|Q^{-1}F^*(\alpha,\ \beta)-(\beta-\alpha)\right|\leqslant 2\varepsilon+Q^{-1}X<3\varepsilon,$$

если, например, $Q>\varepsilon^{-1}X(\varepsilon)=Q_0(\varepsilon)$. Следовательно, по определению $D_Q^*<3\varepsilon$ при $Q>Q_0(\varepsilon)$. Этим теорема доказана, так как ε произвольно мало.

§ 4. Критерии Вейля. Для простоты обозначений будем рассматривать только последовательность векторов $\mathbf{z}^{(q)}$, $(q=1,\ 2,\ \ldots)$. Обобщение на $\mathbf{z}^{(\mathbf{q})}$, $\mathbf{q}=(q_1,\ \ldots,\ q_m)$ получается немедленно. Докажем две теоремы, принадлежащие Вейлю.

Теорема II. *Пусть* $\mathbf{z}^{(q)}$ $(q=1,\ 2,\ \ldots)$ — *последовательность векторов, лежащих в n-мерном единичном гиперкубе* $0\leqslant z_j<1$. *Для того чтобы эта последовательность векторов была равномерно распределена в единичном гиперкубе, необходимо и достаточно, чтобы*

$$\lim_{Q\to\infty} Q^{-1}\sum_{q<Q} f(\mathbf{z}^{(q)})=\int\limits_{0\leqslant z_j<1}\ldots\int f(\mathbf{z})\,d\mathbf{z} \qquad (1)$$

для всех действительных или комплексных интегрируемых по Риману функций $f(\mathbf{z})$, определенных в единичном гиперкубе.

Теорема III. *Пусть $\mathbf{z}^{(q)}$, $(q=1, 2, \ldots)$ — любая последовательность n-мерных векторов, которые могут и не принадлежать единичному гиперкубу. Для того чтобы эта последовательность векторов была равномерно распределена по модулю* 1, *необходимо и достаточно, чтобы для всех целых векторов* $\mathbf{t} \neq \mathbf{0}$

$$\lim_{Q \to \infty} Q^{-1} \sum_{q \leqslant Q} e(\mathbf{tz}^{(q)}) = 0, \tag{2}$$

где

$$e(x) = e^{2\pi i x}, \qquad i^2 = -1.$$

Замечание 1. В теореме ничего не говорится о равномерной сходимости в (2). Здесь только утверждается, что (2) имеет место для каждого целого $\mathbf{t} \neq \mathbf{0}$.

Замечание 2. Предположим, в частности, что $\mathbf{z}^{(q)} = q\boldsymbol{\theta}$, где

$$\boldsymbol{\theta} = (\theta_1, \ldots, \theta_n)$$

и $\mathbf{t}\boldsymbol{\theta}$ не целое при целом $\mathbf{t} \neq \mathbf{0}$. Тогда $e(\mathbf{t}\boldsymbol{\theta}) \neq 1$ для каждого $\mathbf{t}$ и

$$\left| Q^{-1} \sum_{q \leqslant Q} e(\mathbf{tz}^{(q)}) \right| = \left| Q^{-1} \sum_{q \leqslant Q} e(q\mathbf{t}\boldsymbol{\theta}) \right| =$$
$$= \left| \frac{e(\mathbf{t}\boldsymbol{\theta})(1 - e(Q\mathbf{t}\boldsymbol{\theta}))}{Q(1 - e(\mathbf{t}\boldsymbol{\theta}))} \right| \leqslant \frac{2}{Q\,|1 - e(\mathbf{t}\boldsymbol{\theta})|} \to 0.$$

Следовательно, по теореме III $\mathbf{z}^{(q)}$ равномерно распределены по модулю 1. Это есть частный случай $(m = 1)$ теоремы I. Общий случай теоремы I получается из соответствующего обобщения теоремы III.

Замечание 3. Так как теорема III остается в силе, если заменить векторы $\mathbf{z}^{(q)}$ векторами, сравнимыми с $\mathbf{z}^{(q)}$ по модулю 1, то можно считать, что все векторы $\mathbf{z}^{(q)}$ лежат в единичном гиперкубе $0 \leqslant z_j < 1$. В этом случае равномерность распределения по модулю 1 становится просто равномерностью распределения.

Доказательство теорем II, III. Для простоты рассуждений будем считать, что $n = 1$, так как никаких больших дополнительных трудностей в случае $n > 1$ нет. Значит, наши векторы $\mathbf{z}^{(q)}$ являются фактически числами, которые мы будем обозначать через $z^{(q)}$. Доказательство теорем II и III (и даже несколько более сильного утверждения) будет получено, если мы докажем цикл импликаций

$$\mathrm{A} \to \mathrm{B} \to \mathrm{C} \to \mathrm{D} \to \mathrm{A}$$

относительно $z^{(q)}$, где

$$0 \leqslant z^{(q)} < 1 \quad (q = 1, 2, \ldots), \tag{3}$$

а A, B, C, D — следующие утверждения.

Утверждение A. $z^{(q)}$ равномерно распределены в $0 \leqslant z < 1$.

Утверждение B.

$$Q^{-1} F_Q(\alpha, \beta) \to \beta - \alpha \quad (Q \to \infty) \tag{4}$$

для любой пары чисел α, β, $0 \leqslant \alpha < \beta \leqslant 1$, где, как и ранее, $F_Q(\alpha, \beta)$ есть число решений неравенств

$$\alpha \leqslant z^{(q)} < \beta, \quad 1 \leqslant q \leqslant Q. \tag{5}$$

Равномерность предельного перехода относительно α и β не предполагается.

Утверждение C.

$$Q^{-1} \sum_{q \leqslant Q} f(z^{(q)}) \to \int_0^1 f(z)\,dz \tag{6}$$

для всех функций $f(z)$, интегрируемых по Риману в $0 \leqslant z \leqslant 1$.

Утверждение D.

$$Q^{-1} \sum_{q \leqslant Q} e(tz^{(q)}) \to 0 \tag{7}$$

для всех целых $t \neq 0$. Здесь опять не предполагается равномерности относительно t.

Доказательство того, что из A следует B, очевидно, так как B более слабая[1]) форма A.

---

[1]) Для читателя было бы небезынтересно найти простое непосредственное доказательство обратной импликации.

Доказательство того, что из С следует D, очевидно, так как $e(tz)$ — функция, интегрируемая по Риману (а в действительности непрерывная), и

$$\int_0^1 e(tz)dz = 0 \quad (t \neq 0 \text{ — целое}).$$

Доказательство того, что из В следует[1]) С. Рассматривая действительную и мнимую части $f(z)$ отдельно, можно считать, не ограничивая общности, что $f(z)$ — функция действительная и, прибавляя к $f(z)$ подходящую постоянную, что

$$f(z) \geqslant 0. \tag{8}$$

Пусть $\varepsilon > 0$ задано, а V — достаточно большое целое положительное число. Пусть для всех целых v, $1 \leqslant v \leqslant V$, m_v, M_v — соответственно минимум и максимум функции $f(z)$ в интервале

$$v - 1 \leqslant Vz < v, \tag{9}$$

так что

$$0 \leqslant m_v \leqslant M_v. \tag{10}$$

Тогда, в силу интегрируемости по Риману функции $f(z)$, имеем при достаточно большом V

$$\int_0^1 f(z)\,dz - \varepsilon \leqslant V^{-1} \sum m_v \leqslant V^{-1} \sum M_v \leqslant \int_0^1 f(z)dz + \varepsilon. \tag{11}$$

Пусть теперь V — некоторое фиксированное целое, такое, что (11) имеет место. Согласно предположению, что В справедливо, число $F_Q(v - 1/V, v/V) = \varphi_v$ точек $z^{(q)}$, $1 \leqslant q \leqslant Q$, попавших в (9), удовлетворяет неравенству

$$(1 - \varepsilon) V^{-1} \leqslant Q^{-1} \varphi_v \leqslant (1 + \varepsilon) V^{-1}$$

---

[1]) Обратная импликация $C \to B$ доказывается тривиально, если рассмотреть функцию $f(z)$, равную 1 при $\alpha \leqslant z < \beta$ и равную нулю во всех других случаях.

при всех достаточно больших Q. Для таких Q имеем, используя (10) и (11),

$$Q^{-1}\sum_{q\leqslant Q} f(z^{(q)}) = \sum_{v} Q^{-1} \sum_{\substack{q\leqslant Q \\ v-1\leqslant Vz^{(q)}<v}} f(z^{(q)}) \leqslant$$

$$\leqslant \sum_{v} Q^{-1}\varphi_v M_v \leqslant (1+\varepsilon) V^{-1} \sum M_v \leqslant (1+\varepsilon)\left(\int_0^1 f(z)\,dz+\varepsilon\right).$$

Аналогично

$$Q^{-1}\sum_{q\leqslant Q} f(z^{(q)}) \geqslant (1-\varepsilon)\left(\int_0^1 f(z)\,dz-\varepsilon\right).$$

Так как ε как угодно мало, то (6) доказано.

Доказательство того, что А следует из D.

Лемма 2. *Для любого* $\varepsilon > 0$ *найдется число* $E = E(\varepsilon)$, *обладающее следующим свойством:*

для каждых α, β $(0 \leqslant \alpha < \beta \leqslant 1)$ *существуют функции* $f_-(z)$, $f_+(z)$ *с периодом* 1, *имеющие непрерывные вторые производные, такие, что*

(i) $0 \leqslant f_-(z) \leqslant 1$, $0 \leqslant f_+(z) \leqslant 1$.

(ii) $f_+(z) = 1$, *если* $\alpha \leqslant z < \beta$,

$f_-(z) = 0$, *если* $0 \leqslant z < \alpha$ *или* $\beta \leqslant z < 1$.

(iii) $\displaystyle\int_0^1 f_+(z)\,dz \leqslant \beta-\alpha+\varepsilon$,

$$\int_0^1 f_-(z)\,dz \geqslant \beta-\alpha-\varepsilon.$$

(iv) $|f''_+(z)| \leqslant E$, $|f''_-(z)| \leqslant E$ *для всех* z.

Замечание. Из условий (i) и (ii), очевидно, следует, что

$$\sum_{q\leqslant Q} f_-(z^{(q)}) \leqslant F_Q(\alpha, \beta) \leqslant \sum_{q\leqslant Q} f_+(z^{(q)}). \tag{12}$$

Как мы увидим, (iii), (iv) обеспечивают удобные разложения в ряд Фурье функций $f_\pm(z)$.

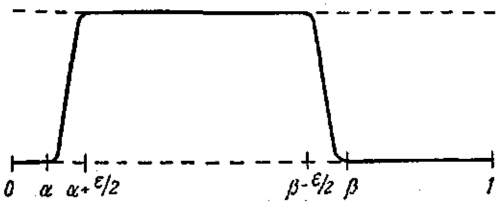
Доказательство. Сначала построим функцию $f_{-}(z)$. Если $\beta-\alpha\leqslant\varepsilon$, то $f_{-}(z)\equiv 0$ обладает всеми нужными свойствами. Значит, можно считать, что $\beta>\alpha+\varepsilon$. Всегда существует дважды дифференцируемая функция $\varphi(x)$, определенная на интервале $0\leqslant x\leqslant 1$, со следующими свойствами:

$$\varphi(0)=\varphi'(0)=\varphi''(0)=0;$$
$$\varphi(1)=1,\ \varphi'(1)=\varphi''(1)=0;$$
$$0\leqslant\varphi(x)\leqslant 1 \quad \text{для} \quad 0\leqslant x\leqslant 1.$$

Например,

$$\varphi(x)=\begin{cases} 8x^3-8x^4, & \text{если } 0\leqslant x\leqslant \frac{1}{2},\\ 1-8(1-x)^3+8(1-x)^4, & \text{если } \frac{1}{2}\leqslant x\leqslant 1,\end{cases}$$

так как $\varphi'(^1/_2)$, $\varphi''(^1/_2)$ существуют и, очевидно, $\varphi(x)$ обладает



Фиг. 3. График функции $f_{-}(z)$.

всеми остальными необходимыми свойствами. Определим, как показано на фиг. 3,

$$f_{-}(z)=\begin{cases} 0, & \text{если } 0\leqslant z<\alpha,\\ \varphi(2\varepsilon^{-1}(z-\alpha)), & \text{если } \alpha\leqslant z<\alpha+\frac{1}{2}\varepsilon,\\ 1, & \text{если } \alpha+\frac{1}{2}\varepsilon\leqslant z<\beta-\frac{1}{2}\varepsilon,\\ \varphi(2\varepsilon^{-1}(\beta-z)), & \text{если } \beta-\frac{1}{2}\varepsilon\leqslant z<\beta,\\ 0, & \text{если } \beta\leqslant z<1.\end{cases}$$

Ясно, что $f_{-}(z)$ дважды дифференцируема и

$$|f''_{-}(z)\leqslant 4\varepsilon^{-2}\max|\varphi''(x)|=E(\varepsilon),$$

где E не зависит от α и β. Таким образом, $f_-(z)$ удовлетворяет (i), (ii) и (iv). Она также удовлетворяет и (iii), так как

$$\int_0^1 f_-(z)\,dz \geqslant \int_{\alpha+\varepsilon/2}^{\beta-\varepsilon/2} dz = \beta-\alpha-\varepsilon.$$

Функция $f_+(z)$ строится аналогично.

Следствие.

$$f_+(z) = \sum_{-\infty<t<\infty} c_t^+ e(tz), \tag{13}$$

$$f_-(z) = \sum_{-\infty<t<\infty} c_t^- e(tz), \tag{14}$$

где

$$c_0^- \geqslant \beta-\alpha-\varepsilon,\ c_0^+ \leqslant \beta-\alpha+\varepsilon, \tag{15}$$

$$|c_t^\pm| \leqslant t^{-2}M \quad (t\neq 0) \tag{16}$$

при M, зависящем от ε, но не зависящем от α или β.

Доказательство. Согласно общей теории рядов Фурье, существуют разложения (13), (14), где

$$c_0^\pm = \int_0^1 f_\pm(z)\,dz,$$

и для $t\neq 0$, если проинтегрировать дважды по частям,

$$c_t^\pm = \int_0^1 f_\pm(z)\,e(-tz)\,dz = -\frac{1}{4\pi^2t^2}\int_0^1 f''_\pm(z)\,e(-tz)\,dz.$$

Применяя теперь (iii), (iv), получаем доказательство следствия.

Доказательство того, что A следует из D, получается немедленно. Пусть $\varepsilon>0$ как угодно мало и $f_\pm(z)$ построены для любых α, β, $0\leqslant\alpha<\beta\leqslant 1$, согласно лемме 2. Тогда по неравенству (12) и следствию из леммы 2 имеем

$$F_Q(\alpha,\beta) \leqslant \sum_{q\leqslant Q} f_+(z^{(q)}) = \sum_{-\infty<t<\infty} c_t^+ \sum_{q\leqslant Q} e(tz^{(q)}) \leqslant$$
$$\leqslant Q(\beta-\alpha+\varepsilon) + \sum_{t\neq 0} t^{-2}M\Bigl|\sum_{q\leqslant Q} e(tz^{(q)})\Bigr|.$$

Используя $f_-(z)$, получаем подобную оценку снизу. Значит,

$$D_Q \leqslant \varepsilon + MQ^{-1}\sum_{t\neq 0} t^{-2}\Bigl|\sum_{q\leqslant Q} e(tz^{(q)})\Bigr|. \tag{17}$$

Так как ряд $\sum t^{-2}$ сходится, то можно выбрать T, такое, что $M \sum_{t \geqslant T} t^{-2} < \varepsilon$. Следовательно, сумма членов с $|t| \geqslant T$ в (17) не более 2ε, так как очевидно, что $\left|\sum e(tz^{(q)})\right| \leqslant Q$. Зафиксируем теперь ε, T. Если D справедливо, то

$$\left| Q^{-1} \sum_{q \leqslant Q} e(tz^{(q)}) \right| < (TM)^{-1}\varepsilon \tag{18}$$

для всех t из $0 < |t| \leqslant T$ и при всех $Q \geqslant$ некоторого $Q_0(\varepsilon)$, так как рассматривается только конечное число значений t. Следовательно, $D_Q < 5\varepsilon$ для всех $Q \geqslant Q_0(\varepsilon)$ по (17), (18). Так как ε как угодно мало, утверждение A доказано.

§ 5. Следствие из критериев Вейля.

Теорема IV. *Для того чтобы 2-мерные векторы* $\mathbf{z}^{(q)} = (x^{(q)}, y^{(q)})$ *были равномерно распределены по модулю 1, необходимо и достаточно, чтобы 1-мерные последовательности* $ux^{(q)} + vy^{(q)}$ *были равномерно распределены по модулю 1 для всех пар целых* u, v, *не равных нулю одновременно.*

Теорема V. *Для того чтобы 1-мерная последовательность* $z^{(q)}$ *была равномерно распределена по модулю 1, достаточно*[1]), *чтобы была равномерно распределена последовательность* $z^{(q+h)} - z^{(q)}$ *при любом целом* $h > 0$.

Теорема VI. *Пусть многочлен*

$$f(x) = \alpha_r x^r + \ldots + \alpha_0 \tag{1}$$

имеет хотя бы один иррациональный коэффициент α_j $(j > 0)$. *Тогда последовательность*

$$z^{(q)} = f(q) \tag{2}$$

равномерно распределена по модулю 1.

Теорема IV есть прямое следствие теоремы III, и поэтому доказательство ее мы опускаем. Теорема VI получается из

---

[1]) Но не необходимо, как показывает пример последовательности $z^{(q)} = q\theta$ с иррациональным θ.

теоремы V, которая в свою очередь является почти прямым следствием теоремы III и следующей леммы.

Лемма 3. *Пусть $u_1, \ldots, u_Q$ — любые действительные или комплексные числа, сопряженные к которым обозначим через $\overline{u}_q$; пусть $1 \leqslant H \leqslant Q$. Тогда*

$$H^2\Big|\sum_{1\leqslant q\leqslant Q} u_q\Big|^2 \leqslant H(H+Q-1)\sum_{1\leqslant q\leqslant Q}|u_q|^2 + \\ +2(H+Q-1)\sum_{0<h<H}(H-h)\Big|\sum_{1\leqslant q\leqslant Q-h}\overline{u}_q u_{q+h}\Big|. \qquad (3)$$

Доказательство. Введем временно следующее соглашение: $u_q=0$, если $q\leqslant 0$ или $q>Q$. Тогда

$$H\sum_{1\leqslant q\leqslant Q} u_q = \sum_{0<p<H+Q}\Big(\sum_{0\leqslant r<H} u_{p-r}\Big).$$

Следовательно, по неравенству Шварца[1]) левая часть (3) не превосходит произведения $H+Q-1$ на

$$\sum_{0<p<H+Q}\Big|\sum_{0\leqslant r<H} u_{p-r}\Big|^2 = \sum_{\substack{0<p<H+Q\\ 0\leqslant r,\ s<H}} u_{p-r}\overline{u}_{p-s}. \qquad (4)$$

Но любой член $|u_q|^2$ встречается в (4) точно H раз, а именно: при $q=p-r=p-s$ и $0\leqslant r<H$. Любой член $u_q\overline{u}_{q+h}$ или $\overline{u}_q u_{q+h}$ $(h>0)$ может встречаться только при $h<H$, а значит, он встречается точно $H-h$ раз. Следовательно, (4) принимает вид

$$H\sum_{1\leqslant q\leqslant Q}|u_q|^2 + \sum_{0<h<H}(H-h)\sum_{1\leqslant q\leqslant Q-h}(u_q\overline{u}_{q+h}+\overline{u}_q u_{q+h}),$$

и лемма доказана.

Следствие. *Предположим, что*

$$Q^{-1}\sum_{1\leqslant q\leqslant Q} e\big(z^{(q+h)}-z^{(q)}\big)\to 0 \quad (Q\to\infty)$$

---

[1]) А именно: $\left|\sum \eta_l\zeta_l\right|^2 \leqslant \sum|\eta_l|^2\sum|\zeta_l|^2$ для всех комплексных чисел η_l, ζ_l $(1\leqslant l\leqslant L)$. Относительно доказательства см. примечание на стр. 149.

для каждого $h > 0$ (не обязательно равномерно относительно h). Тогда

$$Q^{-1} \sum_{1 \leqslant q \leqslant Q} e\left(z^{(q)}\right) \to 0 \quad (Q \to \infty).$$

Доказательство. Положим $u_q = e\left(z^{(q)}\right)$. Для всех $Q > H > 0$ имеем

$$Q^{-2} \left| \sum_{1 \leqslant q \leqslant Q} e\left(z^{(q)}\right) \right|^2 \leqslant \frac{H+Q-1}{HQ} +$$
$$+ 2 \sum_{0 < h < H} \frac{(H+Q-1)(H-h)}{H^2 Q^2} \left| \sum_{1 \leqslant q \leqslant Q-h} e\left(z^{(q+h)} - z^{(q)}\right) \right|. \quad (5)$$

Если теперь H фиксировано, а $Q \to \infty$, то правая часть неравенства (5) стремится к H^{-1}, которое может быть сделано как угодно малым за счет подходящего выбора с самого начала числа H. Следовательно, левая часть неравенства (5) должна стремиться к нулю при $Q \to \infty$.

Доказательство теоремы V. Так как по предположению последовательность $z^{(q+h)} - z^{(q)}$ равномерно распределена, то по теореме III

$$Q^{-1} \sum_{1 \leqslant q \leqslant Q} e\left(t\left(z^{(q+h)} - z^{(q)}\right)\right) \to 0$$

при всех целых $h > 0$, $t \neq 0$. Применяя следствие из леммы 3 к $tz^{(q)}$, получаем

$$Q^{-1} \sum_{1 \leqslant q \leqslant Q} e\left(tz^{(q)}\right) \to 0 \quad (t \neq 0).$$

Значит, опять по теореме III последовательность $z^{(q)}$ равномерно распределена по модулю 1.

Доказательство теоремы VI. Предположим сначала, что первый коэффициент α_r иррационален. Если $r = 1$, то теорема VI есть частный случай теоремы I. Поэтому можно считать, что $r > 1$ и что теорема уже доказана для $r - 1$. Для любого фиксированного целого $h > 0$

$$z^{(q+h)} - z^{(q)} = f(q+h) - f(q)$$

является многочленом относительно q степени $r - 1$ с первым коэффициентом $h\alpha_r$. Следовательно, справедливость теоремы для r следует из справедливости теоремы для $r-1$ и из теоремы V.

Если же α_r рационально, то существует некоторое s, $0<s<r$, такое, что α_s иррационально, а $\alpha_{s+1}, \ldots, \alpha_r$ рациональны. Пусть $M>0$ — целое, такое, что числа $M\alpha_{s+1}, \ldots$ $\ldots, M\alpha_r$ — тоже целые. Очевидно, что достаточно доказать равномерность распределения по модулю 1 последовательности

$$z^{(Mq+m)}=\zeta^{(q)} \quad (q=1, 2, \ldots)$$

для каждого $m=0, 1, \ldots, M-1$. Но

$$\begin{aligned}\zeta^{(q)}&=\alpha_0+\alpha_1(Mq+m)+\ldots+\alpha_r(Mq+m)^r\equiv\\&\equiv\alpha_0+\alpha_1(Mq+m)+\ldots+\alpha_s(Mq+m)^s+\\&+\alpha_{s+1}m^{s+1}+\ldots+\alpha_r m^r \pmod 1,\\ \zeta^{(q)}&=\beta_0+\beta_1 q+\ldots+\beta_s q^s,\end{aligned}$$

где $\beta_1, \ldots, \beta_s$ не зависят от q. В частности, $\beta_s=M^s\alpha_s$ иррационально. Таким образом, мы имеем опять первый случай, и теорема доказана.

ЗАМЕЧАНИЯ

§ 2. Замечательная теорема Ардена — Эренфеста утверждает, что $QD_Q\to\infty$ для любой последовательности действительных чисел из $0\leqslant z<1$ [см. Рот (1954)].

§ 3. Как и в § 3 гл. III можно показать, что теорема I не может быть заменена любой как угодно слабой количественной формулировкой. О работах относительно специального θ, когда $m=n=1$, см. Коксма (1936), гл. IX, § 2. Например, $QD_Q=O(\log Q)$, если θ — квадратичная иррациональность.

§ 4. Простую количественную форму теоремы III, которая является в настоящее время самой сильной, см. у Эрдеша и Турана (1948).

Функции $e(\mathbf{t}\mathbf{z})$ при целых $\mathbf{t}$ являются характерами аддитивной группы векторов по модулю 1. Доказательство довольно слабого результата, использующее теорию топологических групп, см. у Понтрягина (1938), § 33.

§ 5. Интересные рассмотрения см. у Ван дер Корпута (1931). Количественную форму теоремы V см. у Касселса (1953). Много работ, содержащих количественные результаты, было посвящено распределению дробных долей многочленов и связанной с этим задаче об оценке $\sum e(f(q))$, где $f(q)$ — многочлен [см. Виноградов (1947)].

Глава V

ТЕОРЕМЫ ПЕРЕНОСА

§ 1. Введение. В этой главе мы покажем, как сведения об одной задаче относительно системы линейных форм позволяют иногда получить сведения о другой задаче, касающейся системы линейных форм, определенным образом связанной с первой.

Пусть даны n линейных форм от m переменных:

$$L_j(\mathbf{x}) = \sum_i \theta_{ji} x_i \quad (1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n),$$

и пусть

$$M_i(\mathbf{u}) = \sum_j \theta_{ji} u_j$$

— *транспонированная* система m линейных форм от n переменных. По теореме VI гл. I всегда найдется целый вектор $\mathbf{x} \neq \mathbf{0}$, такой, что при любом $X > 1$ и $C = X^{-m/n}$

$$\|L_j(\mathbf{x})\| \leqslant C \ (1 \leqslant j \leqslant n),\ |x_i| \leqslant X \ (1 \leqslant i \leqslant m). \tag{1}$$

В § 2 мы покажем, что если неравенства (1) разрешимы при $\mathbf{x} \neq \mathbf{0}$ для некоторого X и некоторого C, много меньшего $X^{-m/n}$, то транспонированная система неравенств

$$\|M_i(\mathbf{u})\| \leqslant D, \quad |u_j| \leqslant U \tag{2}$$

разрешима при $\mathbf{u} \neq \mathbf{0}$ для некоторого U, зависящего от X и C, и некоторого D, много меньшего естественного $U^{-n/m}$. В частности, случай $m = 1$ устанавливает связь между задачей совместного приближения n иррациональных чисел

$$\|\theta_j x\| \leqslant C, \quad |x| \leqslant X, \tag{3}$$

где $\theta_j = \theta_{j1}$ и $x = x_1$, и приближением одной линейной формы

$$\|\theta_1 u_1 + \ldots + \theta_n u_n\| \leqslant D, \quad |u_j| \leqslant U. \tag{4}$$

Этот случай будет рассмотрен более подробно в § 3.

В § 4, 5 мы покажем, что существует связь между „однородной" задачей (1) и соответствующей „неоднородной" задачей решения неравенств

$$\|L_j(\mathbf{x})-\alpha_j\|\leqslant C_1, \quad |x_i|\leqslant X_1 \tag{5}$$

в целых $\mathbf{x}$ при заданном $\boldsymbol{\alpha}$. Грубо говоря, мы покажем, что если $L_1, \ldots, L_n$ хорошо совместно приближают 0 [т. е. если неравенства (1) разрешимы при некотором X с очень малым C], то существует $\boldsymbol{\alpha}$, которое плохо приближается формами $L_1, \ldots, L_n$ [т. е. существует X_1, зависящее от X и C, такое, что неравенства (5) разрешимы только при очень большом значении C_1], и наоборот. В § 6, 7 мы используем эту теорию для выяснения некоторых положений, опущенных в гл. III.

Сопоставляя результаты § 2, 4, мы видим, что однородные задачи для $L_j(\mathbf{x})$, $M_i(\mathbf{u})$ и соответствующие неоднородные задачи дают сведения одна относительно другой. В частности, необходимое и достаточное условие того, чтобы неравенства (5) были разрешимы для всех $\boldsymbol{\alpha}$ при некоторых заданных C_1, X_1, состоит в том, чтобы неравенства (2) были неразрешимы при некоторых D и U, зависящих только от C_1, X_1. Конечно, D и U не обязательно совпадают и для необходимого и для достаточного условия. Специальный случай теоремы Кронекера (теорема IV, гл. III), в которой $u_1L_1(\mathbf{x})+\ldots+u_nL_n(\mathbf{x})$ не является формой с целыми коэффициентами при $\mathbf{x}$ для любых целых $\mathbf{u}\neq\mathbf{0}$, можно рассматривать как „предельный случай" $C_1=\varepsilon>0$, $X_1=U=\infty$, $D=0$ этого последнего результата: неравенство $\|L_j(\mathbf{x})-\alpha_j\|<\varepsilon$ $(1\leqslant j\leqslant n)$ разрешимо для всех $\boldsymbol{\alpha}$ в целых $\mathbf{x}$ при условии, что не существует целого $\mathbf{u}\neq\mathbf{0}$, для которого $\|M_i(\mathbf{u})\|=0$ $(1\leqslant i\leqslant m)$. В § 8 мы докажем количественное обобщение общей теоремы Кронекера, а в § 9 кратко наметим другой подход к теоремам переноса.

§ 2. Теоремы переноса для двух однородных задач. Теоремы, упомянутые во введении, легко получаются из следующей теоремы.

Теорема I. *Пусть даны l линейно независимых однородных линейных форм $f_k(\mathbf{z})$ $(1\leqslant k\leqslant l)$ от l переменных $\mathbf{z}=(z_1, \ldots, z_l)$ и l линейно независимых однородных* *линейных форм* $g_k(\mathbf{w})$ *от* l *переменных* $\mathbf{w}=(w_1, \ldots, w_l)$ *с определителем* d. *Предположим, что в*

$$\Phi(\mathbf{z}, \mathbf{w})=\sum_k f_k(\mathbf{z}) g_k(\mathbf{w}) \tag{1}$$

коэффициенты при всех произведениях $z_i w_j$ $(1 \leqslant i, j \leqslant l)$ *целые. Если неравенства*

$$|f_k(\mathbf{z})| \leqslant \lambda \quad (1 \leqslant k \leqslant l) \tag{2}$$

разрешимы в целых $\mathbf{z} \neq \mathbf{0}$, *то и неравенства*

$$|g_k(\mathbf{w})| \leqslant (l-1)\,|\lambda d|^{1/(l-1)} \tag{3}$$

разрешимы в целых $\mathbf{w} \neq \mathbf{0}$.

Доказательство. В силу ленейной независимости функций $f_k(\mathbf{z})$ уравнения $f_k(\mathbf{z})=0$ $(1 \leqslant k \leqslant l)$ имеют единственное решение $\mathbf{z}=\mathbf{0}$. Следовательно, по условию существует целый $\mathbf{z} \neq \mathbf{0}$, такой, что

$$0<\max |f_k(\mathbf{z})| \leqslant \lambda. \tag{4}$$

Так как правая часть (3) уменьшается вместе с уменьшением λ, то можно считать, изменяя в случае необходимости порядок $f_1, \ldots, f_l$, что

$$\max |f_k(\mathbf{z})|=f_l(\mathbf{z})=\lambda>0. \tag{5}$$

В дальнейшем под $\mathbf{z}$ понимаем фиксированный целый вектор, для которого (5) имеет место.

Рассмотрим теперь l линейных форм

$$\begin{gathered}\Phi(\mathbf{z}, \mathbf{w}), \\ g_k(\mathbf{w}) \quad (k \neq l)\end{gathered}$$

от l переменных $\mathbf{w}$. Как легко видеть, их определитель равен

$$f_l(\mathbf{z})\, d=\lambda d.$$

По теореме Минковского о линейных формах (теорема III приложения В) существует целый вектор $\mathbf{w} \neq \mathbf{0}$, такой, что

$$\left.\begin{array}{l}|\Phi(\mathbf{z}, \mathbf{w})|<1, \\ |g_k(\mathbf{w})| \leqslant|\lambda d|^{1/(l-1)} \quad (k \neq l).\end{array}\right\} \tag{6}$$

Но по условию $\Phi(\mathbf{z}, \mathbf{w})$ — целое число, а значит,

$$\Phi(\mathbf{z}, \mathbf{w}) = 0.$$

Следовательно, используя (5),

$$\lambda g_l(\mathbf{w}) = f_l(\mathbf{z})\, g_l(\mathbf{w}) = -\sum_{k \neq l} f_k(\mathbf{z})\, g_k(\mathbf{w}),$$

а отсюда в силу (5), (6)

$$|g_l(\mathbf{w})| \leqslant (l-1)\,|\lambda d|^{1/(l-1)}. \tag{7}$$

Неравенство (3) сразу следует из (6) и (7), и теорема доказана.

Из доказанной теоремы почти немедленно следует

Теорема II. *Пусть*

$$L_j(\mathbf{x}) = \sum_i \theta_{ji} x_i, \quad M_i(\mathbf{u}) = \sum_j \theta_{ji} u_j,$$

где $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$. *Предположим, что существуют целые* $\mathbf{x} \neq \mathbf{0}$, *такие, что*

$$\|L_j(\mathbf{x})\| \leqslant C, \quad |x_i| \leqslant X$$

при некоторых постоянных C *и* X, *где* $0 < C < 1 \leqslant X$. *Тогда найдутся целые* $\mathbf{u} \neq \mathbf{0}$, *такие, что*

$$\|M_i(\mathbf{u})\| \leqslant D, \quad |u_j| \leqslant U, \tag{8}$$

где

$$D = (l-1)\, X^{(1-n)/(l-1)} C^{n/(l-1)}, \quad U = (l-1)\, X^{m/(l-1)} C^{(1-m)/(l-1)} \tag{9}$$

и

$$l = m + n.$$

Доказательство. Введем новые переменные

$$\mathbf{y} = (y_1, \ldots, y_n), \quad \mathbf{v} = (v_1, \ldots, v_m).$$

Положим

$$f_k(\mathbf{x}, \mathbf{y}) = \begin{cases} C^{-1}(L_k(\mathbf{x}) + y_k) & (1 \leqslant k \leqslant n), \\ X^{-1} x_{k-n} & (n < k \leqslant l) \end{cases}$$

и

$$g_k(\mathbf{u}, \mathbf{v}) = \begin{cases} C u_k & (1 \leqslant k \leqslant n) \\ X(-M_{k-n}(\mathbf{u}) + v_{k-n}) & (n < k \leqslant l). \end{cases}$$

Тогда f_k — линейно независимые формы от l переменных $\mathbf{z}=(\mathbf{x}, \mathbf{y})$, а g_k — линейно независимые формы от l переменных $\mathbf{w}=(\mathbf{u}, \mathbf{v})$ с определителем

$$d = C^n X^m.$$

Далее,

$$\sum_{k \leqslant l} f_k g_k = \sum_{j \leqslant n} u_j y_j + \sum_{i \leqslant m} v_i x_i,$$

так как все члены с $x_i u_j$ уничтожаются. По условию существуют целые $\mathbf{x}$, $\mathbf{y}$, такие, что

$$|f_k(\mathbf{x}, \mathbf{y})| \leqslant 1.$$

Значит, можно применить теорему I с $\lambda = 1$. Следовательно, найдутся целые $(\mathbf{u}, \mathbf{v}) \neq (\mathbf{0}, \mathbf{0})$, для которых

$$\left.\begin{array}{c} C|u_j| \\ X|-M_i(\mathbf{u})+v_i| \end{array}\right\} \leqslant (l-1)(C^n X^m)^{1/(l-1)} = \left\{\begin{array}{l} CU \\ XD. \end{array}\right.$$

Если $D < 1$, $\mathbf{u}=\mathbf{0}$, то мы имели бы $v_j = 0$, и, значит, $(\mathbf{u}, \mathbf{v}) = \mathbf{0}$, что невозможно. Следовательно, $\mathbf{u} \neq \mathbf{0}$, как и утверждалось, или $D \geqslant 1$. Но $U \geqslant 1$, так как $X \geqslant 1 > C$, и неравенства (8), очевидно, разрешимы, когда $D \geqslant 1$.

Следствие. *Для существования постоянной* $\gamma > 0$, *такой, что*

$$(\max \|L_j(\mathbf{x})\|)^n (\max |x_i|)^m \geqslant \gamma \tag{10}$$

для всех целых $\mathbf{x} \neq \mathbf{0}$, *необходимо и достаточно существования* $\delta > 0$, *такого, что*

$$(\max \|M_i(\mathbf{u})\|)^m (\max |u_j|)^n \geqslant \delta \tag{11}$$

для всех целых $\mathbf{u} \neq \mathbf{0}$.

Доказательство. Пусть $\mathbf{x} \neq \mathbf{0}$ — целый, и пусть

$$X = \max |x_i|, \quad C \geqslant \max \|L_j(\mathbf{x})\| \quad (1 > C > 0). \tag{12}$$

Если $\delta > 0$ существует, то $D^m U^n \geqslant \delta$ для D, U из (8), (9). Но из (9), (12)

$$X^m C^n \geqslant (l-1)^{-l(l-1)} \delta^{l-1} = \gamma.$$

Аналогично ввиду симметрии связи между $L_j(\mathbf{x})$ и $M_i(\mathbf{u})$, если существует γ, то существует и δ.

§ 3. Применение к совместным приближениям[1]). Мы докажем дополнение к теореме VII гл. I (ср. с теоремой VIII гл. I).

Теорема III. *Пусть $\theta_1, \ldots, \theta_n$ — любые n чисел в действительном алгебраическом поле степени $n+1$, такие, что $1, \theta_1, \ldots, \theta_n$ линейно независимы над полем рациональных чисел. Тогда существует постоянная $\gamma > 0$, зависящая только от $\theta_1, \ldots, \theta_n$, такая, что для всех целых $x > 0$*

$$\max \| \theta_j x \| \geqslant \gamma x^{-1/n}. \tag{1}$$

Доказательство. Согласно следствию из теоремы II, достаточно доказать существование $\delta > 0$, такого, что

$$\| u_1\theta_1 + \ldots + u_n\theta_n \| \geqslant \delta (\max | u_j |)^{-n} \tag{2}$$

для всех целых $\mathbf{u} \neq \mathbf{0}$. Левая часть (2) есть

$$| v + u_1\theta_1 + \ldots + u_n\theta_n | \leqslant \frac{1}{2} \tag{3}$$

при некотором целом v. Существует некоторое целое рациональное $q \neq 0$, такое, что $q\theta_1, \ldots, q\theta_n$ являются целыми алгебраическими, и, значит,

$$\alpha = qv + qu_1\theta_1 + \ldots + qu_n\theta_n$$

есть целое алгебраическое число, отличное от нуля по условию. Согласно (3), для любого из n его других алгебраических сопряженных

$$\alpha' = qv + qu_1\theta_1' + \ldots + qu_n\theta_n'$$

справедлива оценка

$$|\alpha'| \leqslant |\alpha| + |\alpha' - \alpha| \leqslant$$
$$\leqslant \frac{1}{2} |q| + | qu_1(\theta_1' - \theta_1) + \ldots + qu_n(\theta_n' - \theta_n) | \leqslant E \max | u_j |,$$

где E не зависит от $\mathbf{u}$. С другой стороны, если мы умножим α на произведение всех n его других сопряженных, то

[1]) Этот параграф требует некоторого знакомства с теорией алгебраических чисел. При первом чтении его можно опустить.

получим целое рациональное число, отличное от нуля, и, значит, $\geqslant 1$ по абсолютной величине. Следовательно,

$$|\alpha|(E\max|u_j|)^n \geqslant 1.$$

Отсюда получается (2), если взять $\delta = q^{-1}E^{-n}$.

В качестве другого приложения теоремы II читатель сам без особого труда докажет следующую теорему.

Теорема IV. (принцип переноса Хинчина). *Пусть* $\theta_1, \ldots, \theta_n$ — *любые иррациональные числа, и пусть* $\omega_1 \geqslant 0$, $\omega_2 \geqslant 0$ *являются соответственно верхними гранями чисел* ω, ω', *таких, что неравенства*

$$\|u_1\theta_1 + \ldots + u_n\theta_n\| \leqslant (\max|u_j|)^{-n-\omega},$$
$$\max\|x\theta_j\| \leqslant x^{-(1+\omega')/n}$$

имеют бесконечно много целых решений. Тогда

$$\omega_1 \geqslant \omega_2 \geqslant \frac{\omega_1}{n^2 + (n-1)\omega_1}$$

с очевидной интерпретацией в случае, когда ω_1 *или* ω_2 *равняется бесконечности.*

§ 4. Теоремы переноса для однородной и неоднородной задач. Основным результатом этого параграфа является

Теорема V. *Пусть дано* l *однородных линейных форм* $f_k(\mathbf{z})$ $(1 \leqslant k \leqslant l)$ *от* l *переменных* $\mathbf{z} = (z_1, \ldots, z_l)$ *с определителем* $\Delta \neq 0$. *Предположим, что единственное целое решение неравенства*

$$\max|f_k(\mathbf{z})| < 1 \tag{1}$$

есть $\mathbf{z} = \mathbf{0}$. *Тогда для любых действительных чисел* $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_l)$ *существуют целые решения неравенства*

$$\max|f_k(\mathbf{z}) - \beta_k| < \frac{1}{2}(h+1), \tag{2}$$

где

$$h = [|\Delta|]. \tag{3}$$

Замечание 1. $|\Delta| \geqslant 1$ по теореме Минковского о линейных формах (теорема III приложения B).

Замечание 2. Теорема не имеет места, если в правой части (2) просто написать $\frac{1}{2}|\Delta|$, как это показывает тривиальный пример

$$f_1(\mathbf{z}) = \Delta z_1, \quad f_k(\mathbf{z}) = z_k \qquad (k \neq 1),$$
$$\beta = \left(\frac{1}{2}\Delta,\ 0,\ \ldots,\ 0\right) \qquad (\Delta > 1).$$

Доказательство. Так как $\Delta \neq 0$, то всегда существует, вообще говоря, нецелый вектор $\boldsymbol{\zeta} = (\zeta_1, \ldots, \zeta_l)$, такой, что

$$f_k(\boldsymbol{\zeta}) = \beta_k \qquad (1 \leqslant k \leqslant l).$$

Введем функцию

$$F(\mathbf{z}) = \max |f_k(\mathbf{z})|. \tag{4}$$

Ясно, что

$$F(\lambda \mathbf{z}) = |\lambda| F(\mathbf{z}) \tag{5}$$

для любых чисел λ и

$$F(\mathbf{z}^{(1)} + \mathbf{z}^{(2)}) \leqslant F(\mathbf{z}^{(1)}) + F(\mathbf{z}^{(2)}) \tag{6}$$

для любых векторов[1]) $\mathbf{z}^{(1)}$ и $\mathbf{z}^{(2)}$. Следовательно, неравенство (2) можно записать так:

$$F(\mathbf{z} - \boldsymbol{\zeta}) < \frac{1}{2}(h+1).$$

Для фиксированного $\boldsymbol{\zeta}$ существует, очевидно[2]), только конечное число целых $\mathbf{z}$, таких, что $F(\mathbf{z} - \boldsymbol{\zeta}) \leqslant F(\boldsymbol{\zeta})$. В частности, $F(\mathbf{z} - \boldsymbol{\zeta})$ достигает своей нижней грани, скажем, при $\mathbf{z}^{(0)}$. Взяв $\mathbf{z} - \mathbf{z}^{(0)}$, $\boldsymbol{\zeta} - \mathbf{z}^{(0)}$ вместо $\mathbf{z}$, $\boldsymbol{\zeta}$ соответственно, мы можем считать, не ограничивая общности, что

$$F(\mathbf{z} - \boldsymbol{\zeta}) \geqslant F(\boldsymbol{\zeta}) \tag{7}$$

для всех целых $\mathbf{z}$. Нам надо доказать, что $F(\boldsymbol{\zeta}) < \frac{1}{2}(h+1)$.

Введем теперь новый параметр u и рассмотрим систему неравенств

$$F\left(\mathbf{z} - \frac{2u}{h+1}\boldsymbol{\zeta}\right) < 1, \tag{8}$$

$$|u| \leqslant |\Delta| \tag{9}$$

---

[1]) $F(\mathbf{z})$ есть выпуклая функция расстояния в смысле приложения В.

[2]) Ср. с леммой 4 приложения В.

от $l+1$ переменных $z_1, \ldots, z_l, u$. Если заменить F, согласно определению [см. (4)], то в левых частях неравенств появятся $l+1$ однородных линейных форм с определителем Δ. Следовательно, существуют целые $z_1, \ldots, z_l, u$, не равные нулю одновременно, которые удовлетворяют неравенствам (8) и (9), согласно теореме III приложения В. Если $u=0$, то неравенство (1) имело бы, вопреки предположению, целое решение $\mathbf{z} \neq \mathbf{0}$. Следовательно, заменяя $\mathbf{z}$, u в случае необходимости на $-\mathbf{z}$, $-u$, мы можем считать, что

$$0 < u \leqslant h = [\,|\Delta|\,]. \tag{10}$$

Но тогда при таком целом $\mathbf{z}$ мы имеем

$$F(\mathbf{z}-\boldsymbol{\zeta}) \leqslant F\left(\mathbf{z}-\frac{2u}{h+1}\boldsymbol{\zeta}\right)+F\left(\frac{2u-h-1}{h+1}\boldsymbol{\zeta}\right) <$$
$$< 1+\left|\frac{2u-h-1}{h+1}\right| F(\boldsymbol{\zeta}) \leqslant 1+\frac{h-1}{h+1}F(\boldsymbol{\zeta})$$

по (6), (5), (10) соответственно. Следовательно, согласно (7),

$$F(\boldsymbol{\zeta}) < 1+\frac{h-1}{h+1}F(\boldsymbol{\zeta}),$$

т. е.

$$F(\boldsymbol{\zeta}) < \frac{1}{2}(h+1),$$

что и доказывает теорему.

Дадим непосредственное применение доказанной теоремы.

Теорема VI. *Пусть* $L_j(\mathbf{x})$, $\mathbf{x}=(x_1, \ldots, x_m)$ *суть* n *однородных форм от* m *переменных. Предположим, что не существует ни одного целого* $\mathbf{x} \neq \mathbf{0}$, *такого, что одновременно*

$$\|L_j(\mathbf{x})\| < C, \qquad |x_i| < X.$$

Тогда для любых $\alpha_1, \ldots, \alpha_n$ *неравенства*

$$\|L_j(\mathbf{x})-\alpha_j\| \leqslant C_1, \qquad |x_i| \leqslant X_1,$$

где

$$C_1 = \frac{1}{2}(h+1)C, \qquad X_1 = \frac{1}{2}(h+1)X$$

и

$$h = [X^{-m}C^{-n}],$$

разрешимы в целых $\mathbf{x}$.

Доказательство. Применить непосредственно теорему V к системе из $l = m + n$ форм

$$f_k = \begin{cases} C^{-1}(L_k(\mathbf{x}) - y_k) & (1 \leqslant k \leqslant n), \\ X^{-1} x_{k-n} & (n < k \leqslant l) \end{cases}$$

от l переменных $(x_1, \ldots, x_m, y_1, \ldots, y_n)$ с определителем $X^{-m}C^{-n}$.

Следствие. *Предположим, что*

$$C = \gamma X^{-m/n}$$

для некоторого $\gamma > 0$. *Тогда*

$$X_1 = \frac{1}{2}([\gamma^{-n}] + 1) X, \quad C_1 = \frac{1}{2}([\gamma^{-n}] + 1) C,$$

так что

$$C_1 = \delta X_1^{-m/n},$$

где δ *зависит только от* γ.

Доказательство очевидно.

Следующая простая теорема является косвенным обращением теоремы VI, так как она связывает неоднородную задачу для L_j с однородной задачей для M_l, которая в свою очередь связана с однородной задачей для L_j, согласно теореме II.

Теорема VII. *Предположим, что для любых* $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ *существует целое решение* $\mathbf{x} = (x_1, \ldots, x_m)$ *неравенств*

$$\|L_j(\mathbf{x}) - \alpha_j\| < C_1, \quad |x_l| \leqslant X_1.$$

Тогда не существует ни одного целого решения $\mathbf{u} \neq 0$ *неравенств*

$$\|M_l(\mathbf{u})\| \leqslant D, \quad |u_j| \leqslant U,$$

где

$$D = (4mX_1)^{-1}, \quad U = (4nC_1)^{-1},$$

а L_j, M_j — *транспонированные системы форм, определение которых дано в* § 1.

Доказательство. Воспользуемся тождеством

$$\sum_l x_l M_l(\mathbf{u}) = \sum_{l,j} \theta_{lj} x_l u_j = \sum_j u_j L_j(\mathbf{x}).$$

Предположим, что такое $\mathbf{u}$ существует. Возьмем любой вектор $\boldsymbol{\alpha}$, такой, что $\sum u_j\alpha_j = \frac{1}{2}$. Тогда

$$\frac{1}{2} = \left\| \sum u_j\alpha_j \right\| \leqslant \left\| \sum u_j (\alpha_j - L_j(x)) \right\| + \left\| \sum u_j L_j(\mathbf{x}) \right\| <$$
$$< nUC_1 + \left\| \sum x_i M_i(\mathbf{u}) \right\| \leqslant nUC_1 + mX_1 D = \frac{1}{4} + \frac{1}{4},$$

что невозможно.

Следствие. *Если* $C_1 = \gamma X_1^{-m/n}$, *то* $D = \delta U^{-n/m}$, *где* δ *зависит только от* γ, m, n.

Доказательство очевидно.

Из следствий теорем II, VI, VII сразу получается следующая

Теорема VIII. *Каждое из следующих четырех утверждений влечет за собой все остальные.*

(i) *Существует постоянная* $\gamma_1 > 0$, *такая, что неравенства*

$$\|L_j(\mathbf{x})\| \leqslant \gamma_1 X^{-m/n}, \quad |x_i| \leqslant X$$

неразрешимы в целых $\mathbf{x} \neq \mathbf{0}$ *для всех* $X \geqslant 1$.

(ii) *Существует постоянная* $\gamma_2 > 0$, *такая, что неравенства*

$$\|M_i(\mathbf{u})\| \leqslant \gamma_2 U^{-n/m}, \quad |u_j| \leqslant U$$

неразрешимы в целых $\mathbf{u} \neq \mathbf{0}$ *для всех* $U \geqslant 1$.

(iii) *Существует постоянная* $\gamma_3 > 0$, *такая, что неравенства*

$$\|L_j(\mathbf{x}) - \alpha_j\| \leqslant \gamma_3 X^{-m/n}, \quad |x_i| \leqslant X$$

разрешимы в целых $\mathbf{x}$ *для всех* $X \geqslant 1$ *и всех* $\boldsymbol{\alpha}$.

(iv) *Существует постоянная* $\gamma_4 > 0$, *такая, что неравенства*

$$\|M_i(\mathbf{u}) - \beta_i\| \leqslant \gamma_4 U^{-n/m}, \quad |u_j| \leqslant U$$

разрешимы в целых $\mathbf{u}$ *для всех* $U \geqslant 1$ *и всех* $\boldsymbol{\beta}$.

§ 5. Непосредственное обращение теоремы V[1]**.** Нам понадобится следующая

---

[1]) Этот параграф при первом чтении можно опустить.

Лемма 1. *Пусть $\mathfrak{R}$ — замкнутая выпуклая l-мерная область, симметричная относительно* $\mathbf{0}$ *и содержащая* $(0, \ldots, 0, \pm\mu)$ *при некотором* $\mu > 0$. *Пусть* $\mathfrak{R}_0$ — *множество точек* $\mathbf{x} = (x_1, \ldots, x_{l-1})$ *в* $(l-1)$-*мерном пространстве, такое, что* $(\mathbf{x}, y) \in \mathfrak{R}$ *по меньшей мере для одного* y. *Тогда*

$$lV \geqslant 2V_0\mu,$$

где V, V_0 — *соответственно* l-, $(l-1)$-*мерные объемы областей* $\mathfrak{R}$, $\mathfrak{R}_0$.

Доказательство. Для заданного $\mathbf{x} \in \mathfrak{R}_0$ множество y, таких, что $(\mathbf{x}, y) \in \mathfrak{R}$, образует интервал, скажем, $\eta_1(\mathbf{x}) \leqslant y \leqslant \eta_2(\mathbf{x})$. Область $\mathscr{S}$, состоящая из точек $(\mathbf{x}, y)$, где

$$\mathbf{x} \in \mathfrak{R}_0, \quad |y| \leqslant \frac{1}{2}(\eta_2(\mathbf{x}) - \eta_1(\mathbf{x})) = Y(\mathbf{x}),$$

имеет, очевидно, объем V. Если $\mathbf{x}^{(1)}, \mathbf{x}^{(2)} \in \mathfrak{R}_0$, то, в силу выпуклости, $\mathfrak{R}$ содержит целиком плоский четырехугольник с вершинами

$$(\mathbf{x}^{(i)}, \eta_j(\mathbf{x}^{(i)})) \quad (i, j = 1, 2)$$

и, значит, $\mathscr{S}$ содержит целиком четырехугольник с вершинами

$$(\mathbf{x}^{(i)}, \pm Y(\mathbf{x}^{(i)})) \quad (i = 1, 2).$$

В частности, отрезок, соединяющий любые две точки $(\mathbf{x}^{(i)}, y^{(i)})$ из $\mathscr{S}$, лежит в $\mathscr{S}$, т. е. $\mathscr{S}$ — выпуклая область.

По предположению $(0, \ldots, 0, \pm\mu) \in \mathscr{S}$ и по построению $(\mathbf{x}, 0) \in \mathscr{S}$, как только $\mathbf{x} \in \mathfrak{R}_0$. Следовательно, в силу выпуклости, $\mathscr{S}$ содержит „сдвоенный конус“

$$(\lambda\mathbf{x}, \pm(1-\lambda)\mu), \quad 0 \leqslant \lambda \leqslant 1, \quad \mathbf{x} \in \mathfrak{R}_0.$$

Легко видеть, что этот сдвоенный конус имеет объем $2l^{-1}\mu V_0$; так как он содержится в области $\mathscr{S}$ объема V, лемма доказана.

Теорема IX (Берч). *Пусть* $f_k(\mathbf{z})$ $(1 \leqslant k \leqslant l)$ — *линейные формы от*

$$\mathbf{z} = (z_1, \ldots, z_l)$$

с определителем $\Delta \neq 0$. *Предположим, что для каждого* $\boldsymbol{\zeta}$ *существует целый* $\mathbf{z}$, *для которого*

$$|f_k(\boldsymbol{\zeta} - \mathbf{z})| \leqslant 1 \quad (1 \leqslant k \leqslant l).$$

Тогда

$$\max |f_k(\mathbf{z})| \geqslant l^{-1} 2^{-l+1} |\Delta|$$

для всех целых $\mathbf{z} \neq \mathbf{0}$.

Доказательство. Пусть $\mathbf{z}^{(0)} \neq \mathbf{0}$ — целый вектор, и пусть $\max |f_k(\mathbf{z}^{(0)})| = \lambda_0$. По лемме 7 приложения В, можно считать без ограничения общности, что $\mathbf{z}^{(0)} = (0, 0, \ldots, 0, z_{0l})$. Так как $|z_{0l}| \geqslant 1$, то точки $(0, 0, \ldots, 0 \pm \lambda_0^{-1})$ удовлетворяют неравенству $\max |f_k(\mathbf{z})| \leqslant 1$.

Пусть $\mathfrak{R}$ определяется неравенствами $|f_k(\mathbf{z})| \leqslant 1$ $(1 \leqslant k \leqslant l)$, и пусть $\mathfrak{R}_0$, V, V_0 те же, что и в доказательстве леммы 1. Для любого $\boldsymbol{\zeta} = (\zeta_1, \ldots, \zeta_l)$ по предположению существует в $\mathfrak{R}_0$ $\mathbf{x} \equiv (\zeta_1, \ldots, \zeta_{l-1}) \bmod 1$. Значит, $V_0 \geqslant 1$. Теперь теорема IX следует из леммы 1, если положить

$$V = 2^l |\Delta|^{-1}, \quad \mu = \lambda_0^{-1}, \quad V_0 \geqslant 1.$$

§ 6. Применение к неоднородному приближению. В § 6, 7 мы используем методы, развитые в § 1—4, для того чтобы исследовать, в какой мере результаты гл. III являются наилучшими. Наша ближайшая цель — доказать следующие теоремы.

Теорема X. *Для любых пар целых* $m > 0$, $n > 0$ *найдется постоянная* $\Gamma_{m,n} > 0$, *обладающая следующим свойством. Пусть* $L_j(\mathbf{x})$ — *любые* n *однородных форм от* m *переменных. Тогда существует вектор* $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$, *такой, что*

$$(\max \| L_j(\mathbf{x}) - \alpha_j \|)^m (\max |x_i|)^n \geqslant \Gamma_{m,n}$$

для всех целых $\mathbf{x} \neq \mathbf{0}$.

Теорема XI. *В частности, в качестве* $\Gamma_{1,1}$ *можно взять* $(51)^{-1}$.

Вопрос о наилучшем значении $\Gamma_{m,n}$ остается открытым даже в случае $m = n = 1$. Теорема XI утверждает, в частности, что для каждого θ существует α, такое, что $|x| \| \theta x - \alpha \| \geqslant (51)^{-1}$ для всех целых $x \neq 0$. Этот результат является дополнением к теореме II гл. III.

Для доказательства теоремы X нам понадобятся три леммы, касающиеся транспонированной системы форм $M_i(\mathbf{u})$.

Лемма 2. *Пусть* $\mathbf{u}^{(r)} = (u_{r1}, u_{r2}, \ldots, u_{rn}) \neq \mathbf{0}$, $r = 1, 2, \ldots,$ — *конечная или бесконечная последовательность целых векторов. Определим* $\rho_r > 0$ *равенством*

$$\rho_r^2 = u_{r1}^2 + \ldots + u_{rn}^2. \tag{1}$$

Предположим, что

$$\rho_{r+1} \geqslant k\rho_r \quad (r = 1, 2, \ldots) \tag{2}$$

для некоторого числа $k > 2$. *Тогда существует множество действительных чисел*

$$\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n),$$

такое, что

$$\|\mathbf{u}^{(r)}\boldsymbol{\alpha}\| = \|u_{r1}\alpha_1 + \ldots + u_{rn}\alpha_n\| \geqslant \frac{1}{2}\left(1 - \frac{1}{k-1}\right) \tag{3}$$

для всех r.

Доказательство. Плоскости

$$\mathbf{u}^{(r)}\mathbf{z} = \text{целое число}$$

в пространстве точек $\mathbf{z} = (z_1, \ldots, z_n)$ отстоят друг от друга на расстоянии ρ_r^{-1} (в обычной эвклидовой метрике). Расстояние по перпендикуляру от произвольной точки $\mathbf{z}$ до ближайшей из этих плоскостей равно $\rho_r^{-1}\|\mathbf{u}^{(r)}\mathbf{z}\|$. Построим последовательность сфер $\mathscr{C}_r$, таких, что каждая сфера содержится в предыдущей, радиус сферы $\mathscr{C}_r$ равен

$$^1/_2(k-1)\rho_r, \tag{4}$$

а центр находится на плоскости

$$\mathbf{u}^{(r)}\mathbf{z} = \text{целое число} + \frac{1}{2}. \tag{5}$$

Тогда (3) имеет место для всех точек $\mathscr{C}_r$, в силу геометрической интерпретации $\mathbf{u}^{(r)}\mathbf{z}$. Так как каждая сфера содержит последующие сферы, то найдется точка $\boldsymbol{\alpha}$, принадлежащая всем сферам. Эта точка, очевидно, обеспечивает справедливость теоремы.

Остается построить сферы $\mathscr{C}_r$. Возьмем в качестве $\mathscr{C}_1$ любую сферу с надлежащим радиусом и с центром на

$\mathbf{u}^{(1)}\mathbf{z} = {}^1/_2$. Если $\mathscr{C}_{r-1}$ уже построена и имеет центр, например, в $\boldsymbol{\beta}_{r-1}$, то на одной из плоскостей (5) найдется точка $\boldsymbol{\beta}_r$, отстоящая от $\boldsymbol{\beta}_{r-1}$ самое большее на расстоянии ${}^1/_2\rho_r^{-1}$ [например, основание перпендикуляра, опущенного из $\boldsymbol{\beta}_{r-1}$ на ближайшую плоскость (5)]. Возьмем в качестве $\mathscr{C}_r$ сферу с центром в $\boldsymbol{\beta}_r$ и с радиусом (4). Тогда $\mathscr{C}_r$ содержится в $\mathscr{C}_{r-1}$, так как

$$\frac{1}{2\rho_r} + \frac{1}{2(k-1)\rho_r} \leqslant \frac{1}{2(k-1)\rho_{r-1}}$$

по (2). Следовательно, мы можем построить последовательность сфер $\mathscr{C}_1$, $\mathscr{C}_2$, ..., что и доказывает лемму.

Для любого $\rho \geqslant 1$ определим $\eta(\rho)$ как минимум из

$$\max_i \| M_i(\mathbf{u}) \|,$$

где $\mathbf{u} \neq \mathbf{0}$ пробегают все целые точки, удовлетворяющие неравенству

$$u_1^2 + \ldots + u_n^2 \leqslant \rho^2.$$

Лемма 3. (i) $\eta(\rho)$ *не возрастает с ростом* ρ.

(ii) *Существует постоянная* $\gamma_{m,n}$, *зависящая только от* m, n, *такая, что*

$$(\eta(\rho))^m \rho^n \leqslant \gamma_{m,n}. \tag{6}$$

(iii) *Можно взять* $\gamma_{1,1} = 1$.

Доказательство (i) очевидно.

(ii), (iii). По теореме VI гл. I существует целый вектор $\mathbf{u} \neq \mathbf{0}$, удовлетворяющий неравенствам

$$|u_j| \leqslant n^{-1/2}\rho, \quad \| M_i(\mathbf{u}) \| < (n^{-1/2}\rho)^{-n/m},$$

если $\rho > n^{1/2}$. Утверждение теоремы получается сразу. Если $\rho \leqslant n^{1/2}$, то утверждение тривиально, так как $\eta(\rho) \leqslant {}^1/_2$.

[В другом доказательстве, дающем лучшую оценку для $\gamma_{m,n}$ (кроме $\gamma_{1,1}$), используются теорема IV приложения B и тот факт, что область, определяемая неравенствами

$$|M_i(\mathbf{u}) + v_i| \leqslant D, \ \sum u_j^2 \leqslant \rho^2$$

в пространстве точек

$$(u_1, \ldots, u_n, v_1, \ldots, v_m),$$

выпукла для любых $D > 0$, $\rho > 0$.]

Лемма 4. *Для любого $k > 1$ можно найти последовательность целых векторов $\mathbf{u}^{(r)} = (u_{r1}, \ldots, u_{rn}) \neq \mathbf{0}$, $r = 1, 2, \ldots$, таких, что*

$$\rho_1 \leqslant k, \tag{7}$$

$$\rho_{r+1} \geqslant k\rho_r \qquad (r = 1, 2, \ldots), \tag{8}$$

$$\max_i \| M_i (\mathbf{u}^{(r)}) \| = \eta (k^{-1}\rho_{r+1}), \tag{9}$$

где ρ_r определяются согласно (1). *Эта последовательность бесконечна, если не существует целого $\mathbf{u} \neq \mathbf{0}$ с $\| M_i (\mathbf{u}) \| = 0$ $(1 \leqslant i \leqslant m)$. Если же такое $\mathbf{u}$ существует, то последовательность кончается на таком $\mathbf{u}^{(R)}$, что $\max \| M_i (\mathbf{u}^{(R)}) \| = 0$, но $\max \| M_i (\mathbf{u}^{(r)}) \| \neq 0$ для $r < R$.*

Доказательство. Предположим сначала, что существует целый вектор $\mathbf{u} \neq \mathbf{0}$ с $\| M_i (\mathbf{u}) \| = 0$ $(1 \leqslant i \leqslant m)$. Построим последовательность целых векторов $\mathbf{v}^{(r)} \neq \mathbf{0}$ и чисел $\sigma_r > 0$, удовлетворяющих условию

$$\sigma_r^2 = v_{r1}^2 + \ldots + v_{rn}^2,$$

согласно следующему рецепту:

(i) $\mathbf{v}^{(1)} \neq \mathbf{0}$ — целый вектор с

$$\| M_i (\mathbf{v}^{(1)}) \| = 0 \qquad (1 \leqslant i \leqslant m),$$

для которого σ_1 по возможности мало.

(ii) Если векторы $\mathbf{v}^{(1)}, \ldots, \mathbf{v}^{(R)}$ уже построены для некоторого R и $\sigma_R \leqslant k$, то последовательность обрывается на $\mathbf{v}^{(R)}$.

(iii) Если векторы $\mathbf{v}^{(1)}, \ldots, \mathbf{v}^{(r)}$ уже построены и $\sigma_r > k$, то $\mathbf{v}^{(r+1)} \neq \mathbf{0}$ — целый вектор с

$$\sigma_{r+1} \leqslant k^{-1}\sigma_r, \quad \max \| M_i (\mathbf{v}^{(r+1)}) \| = \eta (k^{-1}\sigma_r),$$

который существует по определению $\eta(\rho)$.

Так как $\sigma_{r+1} \leqslant k^{-1}\sigma_r$, то последовательность кончается на $\mathbf{v}^{(R)}$. Тогда, очевидно, $\mathbf{u}^{(r)} = \mathbf{v}^{(R+1-r)}$ — искомые векторы.

Если не существует целый вектор $\mathbf{u} \neq \mathbf{0}$, для которого $\| M_i (\mathbf{u}) \| = 0$ $(1 \leqslant i \leqslant m)$, то доказательство проводится косвенным путем. Пусть $\varepsilon > 0$ — произвольно малое число и пусть

$$\mathbf{v}^{(1, \varepsilon)}, \ldots, \mathbf{v}^{(R, \varepsilon)},$$

где $R = R(\varepsilon)$ зависит от ε, — любая последовательность векторов, построенная по (ii), (iii), и

(i′) $\mathbf{v}^{(1,\varepsilon)} \neq \mathbf{0}$ — любой целый вектор с

$$\max \| M_l(\mathbf{v}^{(1,\varepsilon)} \| < \varepsilon.$$

Векторы $\mathbf{u}^{(r,\varepsilon)} = \mathbf{v}^{(R+1-r,\varepsilon)}$ удовлетворяют (7), а также (8), (9) для $r < R$.

В силу неравенства (7), имеется только конечное число возможных векторов $\mathbf{u}^{(1,\varepsilon)}$. Значит, один из них, например $\mathbf{u}^{(1)}$, должен встречаться для произвольно малого ε [1]). Так как по предположению $\max \| M_l(\mathbf{u}^{(1)}) \| \neq 0$, то мы должны иметь $R(\varepsilon) \geqslant 2$ для малых ε, согласно (i′). Так как по лемме 3 $\eta(\rho) \to 0$ при $\rho \to \infty$, то существует самое большее конечное число векторов $\mathbf{u}^{(2,\varepsilon)}$, которые удовлетворяют (9) при $r = 1$ и выбранном $\mathbf{u}^{(1)} = \mathbf{u}^{(1,\varepsilon)}$. Выберем $\mathbf{u}^{(2)}$ таким, что $\mathbf{u}^{(1,\varepsilon)} = \mathbf{u}^{(1)}$, $\mathbf{u}^{(2,\varepsilon)} = \mathbf{u}^{(2)}$ встречаются вместе для произвольно малого ε. Предположим, что

$$\mathbf{u}^{(1,\varepsilon)} = \mathbf{u}^{(1)}, \ \ldots, \ \mathbf{u}^{(r,\varepsilon)} = \mathbf{u}^{(r)} \tag{10}$$

встречаются одновременно для произвольно малого ε. Так как по предположению

$$\max \| M_l(\mathbf{u}^{(r)}) \| \neq 0,$$

то, согласно (i′), мы должны иметь $R(\varepsilon) \geqslant r + 1$, если ε достаточно мало и (10) имеет место. Как и ранее, (9) показывает, что существует только конечное число возможных векторов $\mathbf{u}^{(r+1,\varepsilon)}$, совместимых с (10). Значит, один из них, например $\mathbf{u}^{(r+1)}$, должен встречаться для произвольно малого ε. Векторы $\mathbf{u}^{(1)}, \mathbf{u}^{(2)}, \ldots$, построенные таким путем, очевидно, обладают всеми необходимыми свойствами.

Доказательство теоремы X. Пусть $\mathbf{u}^{(r)}$ — векторы, построенные в лемме 4 при $k = 3$, и пусть вектор $\boldsymbol{\alpha}$ построен так, как указано в лемме 2, так что

$$\| \mathbf{u}^{(r)} \boldsymbol{\alpha} \| \geqslant \frac{1}{4}, \tag{11}$$

[1]) То есть для любого ε_0 существует ε, такое, что $0 < \varepsilon < \varepsilon_0$ и $\mathbf{u}^{(1,\varepsilon)} = \mathbf{u}^{(1)}$.

где $1 \leqslant r \leqslant R$ или $1 \leqslant r < \infty$, смотря по тому, какой случай возможен. Пусть $\mathbf{x} \neq \mathbf{0}$ — целый вектор, и положим

$$\max_j \| L_j(\mathbf{x}) - \alpha_j \| = C, \quad \max_i | x_i | = X.$$

Как и в доказательстве теоремы VII, имеем

$$\| \mathbf{u}^{(r)} \boldsymbol{\alpha} \| \leqslant n\rho_r C + mXD_r, \tag{12}$$

где, согласно (9),

$$D_r = \max \| M_i(\mathbf{u}^{(r)}) \| = \begin{cases} \eta\left(\frac{1}{3}\rho_{r+1}\right) & (r \neq R), \\ 0 & (r = R), \end{cases} \tag{13}$$

так как $\max \| u_{rj} \| \leqslant \rho_r$.

Предположим сначала, что можно выбрать целое r, так что

$$mD_{r-1}X \geqslant \frac{1}{8} \geqslant mD_r X. \tag{14}$$

Тогда по неравенствам (11), (12)

$$n\rho_r C \geqslant \frac{1}{8}$$

и, значит,

$$X^m C^m \geqslant \frac{1}{(8m)^m\ (8n)^n\ D_{r-1}^m \rho_r^n} \geqslant \Gamma'_{m,n} \tag{15}$$

при некотором $\Gamma'_{m,n} > 0$ по лемме 3 и (13).

Такое r существует, если только

$$mD_1 X \geqslant \frac{1}{8},$$

и тогда

$$n\rho_1 C > \frac{1}{8}$$

по (11), (12). Так как, в силу (7), $\rho_1 \leqslant k = 3$ и, очевидно,

$$X = \max | x_i | \geqslant 1,$$

то мы имеем

$$X^m C^n \geqslant C^n \geqslant (8n\rho_1)^{-n} \geqslant \Gamma''_{m,n}$$

при некотором $\Gamma''_{m,n} > 0$. Этим и завершается доказательство теоремы X, если положить $\Gamma_{m,n} = \min(\Gamma'_{m,n}\, \Gamma''_{m,n})$.

Следствие. *Предположим, что* $\rho^n(\eta(\rho))^m \to 0$ *при* $\rho \to \infty$. *Тогда неравенство*

$$(\max \|L_j(\mathbf{x}) - \alpha_j\|)^n (\max |x_i|)^m \leqslant M,$$

где $\boldsymbol{\alpha}$ *— построенный выше вектор, имеет только конечное число решений при любом сколь угодно большом* M.

Доказательство. Предположим сначала, что существует $\mathbf{u}^{(R)}$, причем $D_R = 0$. Тогда из (11), (12) следует, что

$$C \geqslant (4n\rho_R)^{-1}.$$

А так как векторов $\mathbf{x}$, для которых $\max |x_i|$ меньше произвольного заданного числа, существует только конечное число, то в этом случае следствие справедливо.

В противном случае r принимает все положительные значения, и среднее выражение в (15) стремится к ∞ при $r \to \infty$, так как $D_{r-1} = \eta(^1/_3\rho_r)$. Но для каждого r существует только конечное число решений $\mathbf{x}$ неравенств (14), и следствие опять справедливо.

Чтобы получить оценку $(51)^{-1}$ для $\Gamma_{1,1}$, нам надо усовершенствовать предыдущее доказательство.

Лемма 5. *Пусть* λ, μ, ν *— неотрицательные числа и* $\varkappa > 1$. *Если*

$$\lambda\mu \leqslant \nu^2, \quad \lambda \leqslant \varkappa\nu, \quad \mu \leqslant \varkappa\nu,$$

то

$$\lambda + \mu \leqslant (\varkappa + \varkappa^{-1})\,\nu.$$

Доказательство. Если $\lambda \leqslant \nu$, $\mu \leqslant \nu$, то доказательство очевидно, так как $\varkappa + \varkappa^{-1} > 2$. Если, например, $\nu < \lambda = \xi\nu$, то $1 < \xi \leqslant \varkappa$ и $\mu \leqslant \lambda^{-1}\nu^2 \leqslant \xi^{-1}\nu$. Следовательно,

$$\lambda + \mu \leqslant (\xi + \xi^{-1})\,\nu \leqslant (\varkappa + \varkappa^{-1})\,\nu.$$

Доказательство теоремы XI. В случае $m = n = 1$ можно упростить обозначения, если писать x, u, $u^{(r)}$, α вместо x_1, u_1, u_{r1}, α_1 соответственно. Так что $\rho_r = |u^{(r)}|$ и $L_1(\mathbf{x}) = \theta x$, $M_1(\mathbf{u}) = \theta u$ для некоторого числа θ.

Пусть $k > 2$ — число, которое мы выберем позднее. Пусть $u^{(r)}$, α определены так, как указано в леммах 4 и 2, так что

$$\|u^{(r)}\alpha\| \geqslant \frac{1}{2}\left(1 - \frac{1}{k-1}\right). \tag{16}$$

Для любого целого $x \neq 0$ имеем, как и ранее,

$$\| u^{(r)}\alpha \| = \| u^{(r)} (\alpha - \theta x) + x u^{(r)} \theta \| \leqslant$$
$$\leqslant | u^{(r)} | \, \| \theta x - \alpha \| + | x | \, \| u^{(r)} \theta \|. \tag{17}$$

Предположим сначала, что существует некоторое целое r, такое, что

$$| x | \, \| u^{(r)} \theta \| \geqslant (k | x | \, \| \theta x - \alpha \|)^{1/2} \geqslant | x | \, \| u^{(r+1)} \theta \|. \tag{18}$$

Но по лемме 3 (iii) и (9)

$$| u^{(r+1)} | \, \| u^{(r)} \theta \| \leqslant k. \tag{19}$$

Значит, используя левую часть неравенства (18), получаем

$$| u^{(r+1)} | \, \| \theta x - \alpha \| \leqslant (k | x | \, \| \theta x - \alpha \|)^{1/2}. \tag{20}$$

Но $| u^{(r+1)} | \, \| u^{(r+1)} \theta \| \leqslant 1$ по (8) и (19). Согласно (20) и правой части (18), применима лемма 5 с

$$\lambda = | x | \, \| u^{(r+1)} \theta \|, \quad \mu = | u^{(r+1)} | \, \| \theta x - \alpha \|,$$
$$\nu^2 = | x | \, \| \theta x - \alpha \|, \quad \varkappa = k^{1/2}.$$

Следовательно, правая часть неравенств (17)

$$\leqslant \left(k^{1/2} + k^{-1/2} \right) (| x | \, \| \theta x - \alpha \|)^{1/2}. \tag{21}$$

Из (16), (17), (21) имеем

$$| x | \, \| \theta x - \alpha \| \geqslant (k - 2)^2 k / 4 (k^2 - 1)^2.$$

Выражение справа достигает максимума примерно при $k = {}^{11}/_2$. Если взять $k = {}^{11}/_2$, то правая часть будет иметь значение, равное $\frac{539}{27{,}378} > \frac{1}{51}$.

Целое r, удовлетворяющее (18), существует всегда, за исключением случая, когда

$$(k | x | \, \| \theta x - \alpha \|)^{1/2} > | x | \, \| u^{(1)} \theta \|.$$

Если также и

$$(k | x | \, \| \theta x - \alpha \|)^{1/2} \geqslant | u^{(1)} | \, \| \theta x - \alpha \|,$$

то предыдущие рассуждения остаются в силе при $r+1=1$. В противном случае, так как $|u^{(1)}|\leqslant k$ и $|x|\geqslant 1$, имеем

$$(k|x|\,\|\theta x-\alpha\|)^{1/2}\leqslant |u^{(1)}|\,\|\theta x-\alpha|,$$
$$\leqslant k|x|\,\|\theta x-\alpha\|$$

и

$$|x|\,\|\theta x-\alpha\|\geqslant k^{-1}=\frac{2}{11}>\frac{1}{51}.$$

§ 7. Регулярные и сингулярные системы. Будем говорить, что система из n форм $L_j(\mathbf{x})$ от m переменных *сингулярна*, если для любого $\varepsilon>0$ система неравенств

$$\|L_j(\mathbf{x})\|<\varepsilon X^{-m/n},\quad |x_i|\leqslant X \tag{1}$$

имеет целое решение $\mathbf{x}\neq\mathbf{0}$ для всех X, бо́льших некоторого $X_0(\varepsilon)$. В противном случае система называется *регулярной*.

[Такая терминология оправдывается тем, что коэффициенты θ_{ji} систем сингулярных форм образуют в mn-мерном пространстве множество меры 0. Докажем этот факт. Так как при целом $\mathbf{x}$ значение $\|L_j(\mathbf{x})\|$ одно и то же для всех θ_{ji}, сравнимых по модулю 1, то можно ограничиться рассмотрением

$$0\leqslant\theta_{ji}<1.$$

Для фиксированного целого вектора $\mathbf{x}\neq\mathbf{0}$, у которого, например, $x_1\neq 0$, и для фиксированных $\theta_{j2},\ldots,\theta_{jm}$ неравенство $\|L_j(\mathbf{x})\|\leqslant\varepsilon X^{-m/n}$ показывает, что мера множества чисел θ_{j1} не превосходит $2\varepsilon X^{-m/n}$. Значит, для фиксированного вектора $\mathbf{x}\neq\mathbf{0}$ множество чисел θ_{ji} с

$$\|L_j(\mathbf{x})\|\leqslant\varepsilon X^{-m/n}\qquad(1\leqslant j\leqslant n)$$

имеет меру $(2\varepsilon)^n X^{-m}$. Но так как всех целых векторов $\mathbf{x}\neq\mathbf{0}$ с $\max|x_i|\leqslant X$ имеется $(2X+1)^m-1<(3X)^m$, то неравенства (1) разрешимы с фиксированным X для множества чисел θ_{ji}, мера которого не более $\varepsilon_1=3^m2^n\varepsilon^n$. Следовательно, по лемме Бореля — Кантелли [1]) и множество чисел θ_{jl}, таких, что неравенства (1) разрешимы для всех X, бо́льших некоторого X_0, зависящего от θ_{jl}, имеет меру самое большее ε_1. Тем более множество сингулярных чисел θ_{jl} имеет меру самое большее ε_1. Так как ε произвольно мало, то это множество имеет меру 0.]

Теорема XII. *Для того чтобы система $L_j(\mathbf{x})$ была сингулярна, необходимо и достаточно, чтобы была сингулярна транспонированная система $M_l(\mathbf{u})$.*

Мы опускаем доказательство, так как оно получается из теоремы II с помощью рассуждений, аналогичных тем, которые используются в доказательстве ее следствия. Следующий результат можно рассматривать как некоторое обобщение теоремы II гл. III.

Теорема XIII. *Для того чтобы система $L_j(\mathbf{x})$ была регулярна, необходимо и достаточно, чтобы существовало число $\delta > 0$, такое, что неравенство*

$$\left(\max_j \| L_j(\mathbf{x}) - \alpha_j \|\right)^n \left(\max_l | x_l |\right)^m < \delta \tag{2}$$

имело бы бесконечно много целых решений $\mathbf{x}$ *для каждого действительного* $\boldsymbol{\alpha}$.

Доказательство. Предположим сначала, что система $L_j(\mathbf{x})$ регулярна, т. е. найдется некоторое $\gamma > 0$, такое, что неравенства

$$\| L_j(\mathbf{x}) \| \leqslant \gamma X^{-m/n}, \quad | x_l | \leqslant X \tag{3}$$

неразрешимы для некоторого как угодно большого значения X. По следствию из теоремы VI существует решение $\mathbf{x}$ неравенств

$$\| L_j(\mathbf{x}) - \alpha_j \| \leqslant \delta_1 X_1^{-m/n}, \quad | x_l | \leqslant X_1 = \lambda X \tag{4}$$

---

[1]) А именно: так как $\left|\bigcap_{r \geqslant R} \mathcal{E}_r\right| \leqslant |\mathcal{E}_R|$, $\left|\bigcup_R \mathcal{F}_R\right| = \lim |\mathcal{F}_R|$ для любой последовательности $\mathcal{F}_R$, такой, что $\mathcal{F}_R$ содержит $\mathcal{F}_S$ при $R \leqslant S$, то $\left|\bigcup_R \bigcap_{r \geqslant R} \mathcal{E}_r\right| \leqslant \liminf |\mathcal{E}_r|$ для любой последовательности множеств $\mathcal{E}_r$ $(r \geqslant 1)$, где $\bigcup$, $\bigcap$ обозначают соответственно объединение и пересечение, а $|G|$ — мера G.

для каждого $\boldsymbol{\alpha}$, где δ_1, λ зависят только от γ. Значит, неравенства (2) имеют место при $\delta = \delta_1^n$. Если $X \to \infty$ по всем значениям, при которых неравенства (3) неразрешимы, то таким образом мы получаем бесконечно много решений неравенства (2). Исключение может представлять лишь случай, когда имеется целый вектор $\mathbf{x}^{(0)}$, такой, что

$$\| L_j(\mathbf{x}^{(0)}) - \alpha_j \| = 0 \qquad (1 \leqslant j \leqslant n).$$

Но по теореме VI гл. I существует целое решение $\mathbf{x} \neq \mathbf{0}$ неравенств

$$\| L_j(\mathbf{x}) \| \leqslant X^{-m/n}, \qquad |x_i| \leqslant X \tag{5}$$

для всех X. Так как $L_j(\mathbf{x})$ регулярна, то мы получим бесконечно много $\mathbf{x}$ при $X \to \infty$, согласно определению регулярности. Подставляя в (5) $\mathbf{x} - \mathbf{x}^{(0)}$ вместо $\mathbf{x}$, мы имеем $\mathbf{x} \neq \mathbf{x}^{(0)}$ в качестве решения неравенств

$$\| L_j(\mathbf{x}) - \alpha_j \| \leqslant X^{-m/n}, \quad |x_i| \leqslant X + X_0,$$

где $X_0 = \max(|x_{01}|, \ldots, |x_{0m}|)$. Так как X_0 фиксировано, то отсюда неравенство (2) имеет бесконечно много решений при любом $\delta > 1$ для $X \to \infty$.

Если же система сингулярна, то функция $\eta(\rho)$, определенная на стр. 108 в § 6, удовлетворяет условию

$$\rho^n (\eta(\rho))^m \to 0 \qquad (\rho \to \infty),$$

согласно теореме XII, и неравенству

$$\max |u_j|^2 \leqslant \rho^2 = u_1^2 + \ldots + u_n^2 \leqslant n \max |u_j|^2.$$

Справедливость нашей теоремы следует теперь сразу из следствия теоремы X.

Когда $m = n = 1$, так что

$$L_1(\mathbf{x}) = \theta x, \quad \theta = \theta_{11}, \quad x = x_1,$$

нетрудно видеть, что сингулярными системами будут как раз те, в которых θ рационально [1]). Ибо если $\theta = p/q$, где p, q — целые, то $x = q$ есть решение (1) при любом $\varepsilon > 0$, коль скоро $X > q$. С другой стороны, если θ иррационально

[1]) Справедливость этого утверждения можно получить также путем сравнения теоремы II гл. III и теоремы XIII.

и p_n/q_n — последовательные наилучшие приближения (в смысле гл. I), то не существует решения неравенств

$$\|x\theta\| < \|q_n\theta\|, \qquad 0 < x < q_{n+1}$$

для любого n, и по (16) гл. I $q_{n+1}\|q_n\theta\| > 1/2$. Однако, за исключением $m = n = 1$, существуют нетривиальные сингулярные системы. По теореме XII, доказывая этот факт, мы можем считать, без ограничения общности, что $m \geqslant n$, так что $m \geqslant 2$. Мы ограничимся простейшим, но типичным случаем, когда $n = 1$, $m = 2$. Для последующего применения мы докажем нечто более сильное, чем простое существование.

Теорема XIV. *Пусть $\omega(t) > 0$ при $t = 1, 2, \ldots$. Тогда существуют числа θ, φ, такие, что*

(A) *пара неравенств*

$$\|r\theta + s\varphi\| < \omega(t), \qquad 0 < \max(|r|, |s|) \leqslant t$$

разрешима в целых r, s для всех $t = 1, 2, \ldots$.

(B) $\|r\theta + s\varphi\| \neq 0$ *для всех целых* $(r, s) \neq (0, 0)$.

Замечание. Для нас интересен случай, когда $\omega(t) \to 0$ достаточно быстро при $t \to \infty$. Если $t^2\omega(t) \to 0$, то система сингулярна по определению.

Доказательство. Можно считать, без ограничения общности, что $\omega(t)$ стремится к нулю монотонно, взяв в случае необходимости $\min\left(t^{-1}, \omega(1), \omega(2), \ldots, \omega(t)\right)$ вместо $\omega(t)$.

Для нас удобно пользоваться геометрической интерпретацией, рассматривая θ, φ как прямоугольные координаты. Мы построим последовательность целых

$$1 = t_1 < t_2 < t_3 < \ldots$$

и последовательность прямоугольников

$$\mathscr{L}_j\colon \quad |\theta - \theta_j| \leqslant \delta_j, \quad |\varphi - \varphi_j| \leqslant \delta_j.$$

Эти прямоугольники $\mathscr{L}_j$ будут удовлетворять следующим четырем условиям:

(i)$_j$ Если $t \leqslant t_j$, то существуют целые r, s, такие, что

$$\|r\theta + s\varphi\| < \omega(t), \qquad 0 < \max(|r|, |s|) \leqslant t$$

для всех $(\theta, \varphi) \in \mathscr{L}_j$.

(ii)$_j$ Если $0 < \max(|r|, |s|) < t_j$, то $\|r\theta + s\varphi\| \neq 0$ для всех $(\theta, \varphi) \in \mathscr{L}_j$.

$(\mathrm{iii})_j$ Центр (θ_j, φ_j) прямоугольника $\mathscr{L}_j$ лежит на некоторой линии

$$r_j\theta_j + s_j\varphi_j = l_j, \qquad t_j = \max(|r_j|, |s_j|),$$

где r_j, s_j, l_j — целые.

$(\mathrm{iv})_j$ $\mathscr{L}_j$ содержится в $\mathscr{L}_{j-1}$ $(j > 1)$.

Прежде всего заметим, что если прямоугольники $\mathscr{L}_j$ построены, то лемма доказана. Согласно $(\mathrm{iv})_j$, должна существовать точка $(\theta_\infty, \varphi_\infty)$, принадлежащая всем $\mathscr{L}_j$. Тогда по $(\mathrm{i})_j$ и $(\mathrm{ii})_j$ точка $(\theta_\infty, \varphi_\infty)$ обладает всеми нужными нам свойствами.

Возьмем в качестве $\mathscr{L}_1$ прямоугольник

$$|\theta - \theta_1| \leqslant \frac{1}{3}\omega(1), \qquad |\varphi| \leqslant \frac{1}{3}\omega(1)$$

при любом θ_1. Тогда $(\mathrm{i})_1$, $(\mathrm{iii})_1$ выполняются при $s_1 = t_1 = 1$, $r_1 = l_1 = 0$, а $(\mathrm{ii})_1$, $(\mathrm{iv})_1$ лишены смысла. Предположим теперь, что $t_1, \ldots, t_j$, $\mathscr{L}_1, \ldots, \mathscr{L}_j$ уже построены, и построим t_{j+1}, $\mathscr{L}_{j+1}$. Очевидно, существует бесконечно много различных прямых $r\theta + s\varphi = l$ (r, s, l — целые), которые пересекают прямую $r_j\theta + s_j\varphi = l_j$ во внутренней точке[1]) прямоугольника $\mathscr{L}_j$. Мы выберем одну такую прямую, например $r_{j+1}\theta + s_{j+1}\varphi = l_{j+1}$, с

$$\text{н. о. д. } (r_{j+1}, s_{j+1}, l_{j+1}) = 1 \text{ и } t_{j+1} = \max(|r_{j+1}|, |s_{j+1}|) > t_j.$$

Ясно, что все точки $(\theta_{j+1}, \varphi_{j+1})$ прямой $r_{j+1}\theta + s_{j+1}\varphi = l_{j+1}$, находящиеся достаточно близко к точке пересечения ее с прямой $r_j\theta + s_j\varphi = l_j$, удовлетворяют одновременно неравенствам

$$|\theta_{j+1} - \theta_j| < \delta_j, \qquad |\varphi_{j+1} - \varphi_j| < \delta_j, \tag{6}$$

$$|r_j\theta_{j+1} + s_j\varphi_{j+1} - l_j| < \omega(t_{j+1}). \tag{7}$$

Мы можем считать, кроме того, что θ_{j+1}, φ_{j+1} — иррациональные. Если r, s, l — любые целые числа, такие, что $0 < \max(|r|, |s|) < t_{j+1}$, то линия $r\theta + s\varphi = l$ не может

[1]) Например, если $\theta = a/c$, $\varphi = b/c$, где a, b, c — целые, есть рациональная точка прямой $r_j\theta + s_j\varphi = l_j$, которая является также и внутренней точкой прямоугольника $\mathscr{L}_j$, то любое решение уравнения $ra + sb = lc$ обеспечивает справедливость этого утверждения.

совпадать с $r_{j+1}\theta + s_{j+1}\varphi = l_{j+1}$ и, значит, обе линии пересекаются в точке с рациональными координатами. Значит,

$$\|r\theta_{j+1} + s\varphi_{j+1}\| \neq 0, \qquad 0 < \max(|r|, |s|) < t_{j+1}. \quad (8)$$

В силу непрерывности, (6), (7), (8) будут иметь место и в том случае, когда θ_{j+1}, φ_{j+1} заменены числами θ, φ при условии, что

$$|\theta - \theta_{j+1}| \leqslant \delta_{j+1}, \qquad |\varphi - \varphi_{j+1}| \leqslant \delta_{j+1},$$

а $\delta_{j+1} > 0$ выбрано достаточно малым. Следовательно, для построенных t_{j+1}, θ_{j+1}, φ_{j+1}, δ_{j+1} утверждения $(\mathrm{ii})_{j+1}$, $(\mathrm{iii})_{j+1}$, $(\mathrm{iv})_{j+1}$ справедливы. Утверждение $(\mathrm{i})_{j+1}$ имеет место для $t \leqslant t_j$ по $(\mathrm{i})_j$ и $(\mathrm{iv})_{j+1}$. Если же $t_j < t \leqslant t_{j+1}$, то, согласно (7), беря (θ, φ) вместо $(\theta_{j+1}, \varphi_{j+1})$, имеем, в силу монотонности $\omega(t)$,

$$\|r_j\theta + s_j\varphi\| < \omega(t_{j+1}) \leqslant \omega(t),$$
$$0 < \max(|r_j|, |s_j|) = t_j < t,$$

что и требуется доказать.

Построенная в теореме XIV форма дает возможность показать, что теорема Кронекера (теорема IV гл. III) не допускает никакой сколь угодно слабой количественной формулировки, не зависящей от специальных форм, ввиду того что $^1/_4$ в теореме Минковского (теорема II гл. III) не зависит от θ при условии, что θ — иррационально.

Теорема XV. *Пусть* $\varepsilon(x) > 0$ $(x = 1, 2, \ldots)$, *и пусть* $\varepsilon(x) \to 0$ *при* $x \to \infty$ *как угодно медленно. Тогда существуют числа* (θ, φ), *для которых* $u\theta + v\varphi$ — *не целое при целых* $(u, v) \neq (0, 0)$, *и числа* (α, β), *такие, что неравенства*

$$\|\theta x - \alpha\| < \varepsilon(|x|), \qquad \|\varphi x - \beta\| < \varepsilon(|x|) \qquad (9)$$

имеют только конечное число целых решений x.

Доказательство. Как показано в доказательстве теоремы III [1]), существуют числа α, β, такие, что при всех

---

[1]) Для читателя, желающего избежать обращение к теории алгебраических чисел, не составит труда изменить доказательство теоремы XIV так, что s_j будет всегда нечетным, положив $\alpha = 0$, $\beta = {}^1/_2$. Доказательство теоремы XV можно легко видоизменить, используя $\|r_j\alpha + s_j\beta\| = {}^1/_2$ вместо (10). Но наше доказательство показывает, что α, β могут быть иррациональными.

целых $(u, v) \neq (0, 0)$

$$\|u\alpha + v\beta\| \geqslant \delta (\max(|u|, |v|))^{-2}, \tag{10}$$

где $\delta > 0$. Для целого t найдется некоторое целое $X(t)$, такое, что для всех $x \geqslant X(t)$

$$\varepsilon(x) < \frac{1}{4}\delta t^{-3}. \tag{11}$$

Возьмем

$$\omega(t) = \delta/2t^2 X(t+1) \tag{12}$$

и пусть θ, φ — соответствующие числа, построенные в теореме XIV.

Так как $\varepsilon(x) \to 0$, то существует самое большее конечное число решений неравенств (9) с $\varepsilon(|x|) \geqslant {}^1/_4\delta$. Покажем, что не существует ни одного решения с $\varepsilon(|x|) < {}^1/_4\delta$. Предположим, что имеется одно такое решение, и определим целое $t \geqslant 1$ неравенством

$$t^3 \leqslant \frac{\delta}{4\varepsilon(|x|)} < (t+1)^3. \tag{13}$$

Тогда по (11) и (12)

$$|x| < X(t+1) = \frac{\delta}{2t^2\omega(t)}. \tag{14}$$

По условию мы можем найти целые (u, v), такие, что

$$\|u\theta + v\varphi\| < \omega(t), \qquad 0 < \max(|u|, |v|) \leqslant t.$$

Согласно (9) и (10), имеем

$$\begin{aligned}\delta t^{-2} \leqslant \|u\alpha + v\beta\| &= \|u(\alpha - \theta x) + v(\beta - \varphi x) + x(u\theta + v\varphi)\| \leqslant \\ &\leqslant |u|\,\|\alpha - \theta x\| + |v|\,\|\beta - \varphi x\| + |x|\,\|u\theta + v\varphi\| < \\ &< 2t\varepsilon(|x|) + |x|\,\omega(t).\end{aligned} \tag{15}$$

Но по (13) и (14) каждое из двух последних слагаемых в (15) $\leqslant {}^1/_2\delta t^{-2}$. Это противоречие и доказывает теорему.

§ 8. Количественная теорема Кронекера. Докажем сначала следующую общую теорему:

Теорема XVI. *Пусть $f_k(\mathbf{z})$, $g_k(\mathbf{w})$, $1 \leqslant k \leqslant l$ — линейные формы от переменных $\mathbf{z} = (z_1, \ldots, z_l)$, $\mathbf{w} = (w_1, \ldots, w_l)$ соответственно. Предположим, что*

$$\sum_k f_k(\mathbf{z})\, g_k(\mathbf{w}) = \sum_k z_k w_k \tag{1}$$

тождественно. Пусть $\beta=(\beta_1, \ldots, \beta_l)$ *состоит из произвольных действительных чисел.*

А. *Для того чтобы для некоторого* $\mathbf{b}$ *имели место неравенства*

$$|\beta_k - f_k(\mathbf{b})| \leqslant 1 \qquad (1 \leqslant k \leqslant l), \tag{2}$$

необходимо выполнение неравенств

$$\left\|\sum g_k(\mathbf{w})\beta_k\right\| \leqslant l \max |g_k(\mathbf{w})| \tag{3}$$

для всех целых $\mathbf{w}$.

В. *Для того чтобы* (2) *имели место для некоторого целого* $\mathbf{b}$, *достаточно выполнения неравенств*

$$\left\|\sum g_k(\mathbf{w})\beta_k\right\| \leqslant 2^{l-1}(l!)^{-2} \max |g_k(\mathbf{w})| \tag{4}$$

для всех целых $\mathbf{w}$.

Доказательство А. $\sum f_k(\mathbf{b})\, g_k(\mathbf{w}) = \sum \omega_k b_k$ — целое число, если $\mathbf{w}$, $\mathbf{b}$ — целые числа. Значит, из (2) следует

$$\left\|\sum g_k(\mathbf{w})\beta_k\right\| = \left\|\sum g_k(\mathbf{w})\left(\beta_k - f_k(\mathbf{b})\right)\right\| \leqslant$$
$$\leqslant \sum |g_k(\mathbf{w})| \leqslant l \max |g_k(\mathbf{w})|.$$

Доказательство В. Будем рассматривать $\mathbf{w}$ как матрицу-строку, а $\mathbf{z}$, β — как матрицы-столбцы. Пусть $\mathbf{G}$ — квадратная матрица, k-й столбец которой состоит из коэффициентов формы g_k, а $\mathbf{F}$ — квадратная матрица, k-я строка которой состоит из коэффициентов формы f_k. Тогда (1) можно записать как

$$\mathbf{G} = \mathbf{F}^{-1}. \tag{5}$$

По теореме VI и по лемме 4 приложения B (если их применить к области, определенной неравенствами $\max |g_j(\mathbf{w})| \leqslant 1$) существует целая матрица $\mathbf{W}$ порядка $l \times l$ с $\det \mathbf{W} = 1$, k-я строка $\mathbf{w}^{(k)}$ которой удовлетворяет условиям

$$\max_j |g_j(\mathbf{w}^{(k)})| = \mu_k, \qquad \prod_k \mu_k \leqslant 2^{1-l} \cdot l! \; |\det \mathbf{G}|. \tag{6}$$

Но $\mathbf{WG}\beta$ — матрица-столбец с k-ым элементом, равным $\sum\limits_j \beta_j g_j(\mathbf{w}^{(k)})$. Следовательно, по (4), (6)

$$\mathbf{WG}\beta = \mathbf{a} + \boldsymbol{\delta},$$

где $\mathbf{a}$ — целая матрица-столбец, а

$$\max|\delta_k| \leqslant 2^{l-1}(l!)^{-2}\mu_k. \tag{7}$$

Следовательно, по (5)

$$\boldsymbol{\beta} = \mathbf{F}\mathbf{b} + \boldsymbol{\gamma}, \tag{8}$$

где

$$\mathbf{b} = \mathbf{W}^{-1}\mathbf{a}, \qquad \boldsymbol{\delta} = \mathbf{W}\mathbf{G}\boldsymbol{\gamma}. \tag{9}$$

Здесь $\mathbf{b}$ — целая матрица, так как $\det \mathbf{W} = 1$. Согласно правилу Крамера, γ_j есть определитель матрицы, полученной из матрицы $\mathbf{WG}$ заменой j-го столбца столбцом $\boldsymbol{\delta}$, умноженный на $\pm(\det \mathbf{G})^{-1}$. Но, согласно (6), элементы k-й строки матрицы $\mathbf{WG}$ не превосходят μ_k. Значит, оценивая этот определитель грубо и пользуясь (7), имеем

$$|\gamma_j| \leqslant |\det \mathbf{G}|^{-1} \cdot l! \cdot 2^{l-1}(l!)^{-2}\prod \mu_k \leqslant 1, \tag{10}$$

согласно (6). Из (8), (10) получаем (2).

Теорема XVII. *Пусть $L_j(\mathbf{x})$, $M_i(\mathbf{u})$ определены так же, как в § 1, а $l = m + n$. Пусть $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$, $C > 0$, $X > 1$ заданы.*

А. *Для того чтобы*

$$\|L_j(\mathbf{a}) - \alpha_j\| \leqslant C, \qquad |a_i| \leqslant X \tag{11}$$

для некоторого целого $\mathbf{a}$, *необходимо выполнение неравенства*

$$\|\mathbf{u}\boldsymbol{\alpha}\| \leqslant \gamma \max(X \max\|M_i(\mathbf{u})\|,\ C \max|u_j|) \tag{12}$$

для всех целых $\mathbf{u}$ *с* $\gamma = l$.

В. *Для того чтобы неравенства* (11) *были разрешимы, достаточно, чтобы* (12) *выполнялось для всех целых* $\mathbf{u}$ *с* $\gamma = 2^{n-1}(l!)^{-2}$.

Доказательство. Эта теорема есть частный случай теоремы XVI с

$$\mathbf{z}=(\mathbf{x},\ \mathbf{y})=(x_1,\ \ldots,\ x_m,\ y_1,\ \ldots,\ y_n),$$

$$\mathbf{w}=(\mathbf{v},\ \mathbf{u})=(v_1,\ \ldots,\ v_m,\ u_1,\ \ldots,\ u_n),$$

$$f_k(\mathbf{z})=\begin{cases} C^{-1}(L_k(\mathbf{x})+y_k) & \text{для } k\leqslant n,\\ X^{-1}x_{k-n} & \text{для } n<k\leqslant l,\end{cases}$$

$$g_k(\mathbf{w})=\begin{cases} Cu_k & \text{для } k\leqslant n,\\ X\big(v_{k-n}-M_{k-n}(\mathbf{u})\big) & \text{для } n<k\leqslant l\end{cases}$$

и $\beta=\left(C^{-1}\boldsymbol{\alpha},\ \mathbf{0}\right)$.

Теперь получим теорему Кронекера (теорема IV гл. III) из теоремы XVII B. В наших обозначениях она утверждает, что если $\|\mathbf{u}\boldsymbol{\alpha}\|=0$ при целом $\mathbf{u}$, как только

$$\|M_i(\mathbf{u})\|=0 \qquad (1\leqslant i\leqslant m),$$

то для любого $\varepsilon>0$ существует целый вектор $\mathbf{a}$ с

$$\|L_j(\mathbf{a})-\alpha_j\|<\varepsilon \qquad (1\leqslant j\leqslant n).$$

Положим $C=\varepsilon$. Так как $\|\mathbf{u}\boldsymbol{\alpha}\|\leqslant{}^1/_2$, то условие (2) выполняется для всех векторов $\mathbf{u}$, кроме тех, у которых $\max|u_j|\leqslant \leqslant\frac{1}{2}\gamma^{-1}\varepsilon^{-1}$. Но по условию мы можем выбрать X настолько большим, что (12) будет иметь место для конечного числа остающихся $\mathbf{u}$. Поэтому теорема XVII B применима.

§ 9. Последовательный минимум[1]. Как мы вкратце покажем, использование последовательного минимума делает формальные связи между теоремами переноса из § 1—4 более ясными, хотя результаты получаются менее точными.

Пусть $f_k(\mathbf{z})$ — l линейных форм от $\mathbf{z}=(z_1,\ \ldots,\ z_l)$ с определителем $\Delta\neq 0$. Тогда $F(\mathbf{z})=\max|f_k(\mathbf{z})|$ является функцией расстояния выпуклой области, определенной неравенствами $|f_k(\mathbf{z})|\leqslant 1$ $(1\leqslant k\leqslant l)$, имеющей объем $2^l|\Delta|^{-1}$.

[1]) При первом чтении этот параграф можно опустить.

Последовательные минимумы $\lambda_1, \ldots, \lambda_l$ удовлетворяют условиям

$$\lambda_1 \leqslant \lambda_2 \leqslant \ldots \leqslant \lambda_l, \quad (l!)^{-1}|\Delta| \leqslant \prod \lambda_j \leqslant |\Delta| \tag{1}$$

по теореме V приложения B.

Положим

$$\Lambda = \sup_{\zeta}(\inf_{\mathbf{z}} F(\zeta - \mathbf{z})),$$

где ζ пробегает все векторы, а $\mathbf{z}$ пробегает все целые векторы. Так как нижняя грань достигается, то, как мы видели ранее (стр. 101), Λ есть наименьшее число, такое, что для любого ζ существует целый $\mathbf{z}$ с $F(\zeta - \mathbf{z}) \leqslant \Lambda$. Наша ближайшая цель — доказать, что

$$\lambda_l \leqslant 2\Lambda \leqslant \lambda_1 + \ldots + \lambda_l \qquad (\leqslant l\lambda_l). \tag{2}$$

Существует целый $\mathbf{x}^{(k)}$, такой, что $F(\zeta^{(k)} - \mathbf{x}^{(k)}) \leqslant \Lambda$, где $\zeta^{(k)}$ имеет $1/2$ на k-ом месте и 0 на всех остальных местах. Таким образом, $F(\mathbf{y}^{(k)}) \leqslant 2\Lambda$, где $\mathbf{y}^{(k)} = 2(\zeta^{(k)} - \mathbf{x}^k)$ имеет нечетную k-ю координату и четные все остальные. Векторы $\mathbf{y}^{(k)}$ должны быть линейно независимыми, так как определитель, составленный из их координат, есть, очевидно, число нечетное. Левая часть (2) получается теперь из определения λ_l. Обозначим через $\mathbf{z}^{(k)}$ линейно независимые целые векторы с $F(\mathbf{z}^{(k)}) = \lambda_k$. Любой вектор ζ можно представить в виде

$$\zeta = \beta_1 \mathbf{z}^{(1)} + \ldots + \beta_l \mathbf{z}^{(l)}.$$

Пусть

$$\mathbf{z} = b_1 \mathbf{z}^{(1)} + \ldots + b_l \mathbf{z}^{(l)},$$

где b_k — целые и $|b_k - \beta_k| \leqslant 1/2$. Тогда

$$F(\zeta - \mathbf{z}) = F\left(\sum (\beta_k - b_k)\,\mathbf{z}^{(k)}\right) \leqslant$$
$$\leqslant \sum |\beta_k - b_k|\, F(\mathbf{z}^{(k)}) \leqslant \frac{1}{2} \sum \lambda_k.$$

Это доказывает правую часть (2).

Легко показать, что максимум правой части (2), если $\lambda_1 \geqslant 1$ и (1) имеет место, равен $l - 1 + |\Delta|$. Это несколько слабее утверждения теоремы V, которая дает $2\Lambda \leqslant [\Delta] + 1$. С другой стороны,

$$\lambda_1 \lambda_l^{l-1} \geqslant (l!)^{-1} |\Delta| \tag{3}$$

по (1). А это совместно с (2) дает оценку для Λ снизу, когда $\lambda_1 \geqslant 1$, аналогичную оценке в § 5, но более слабую.

Пусть теперь $g_k(\mathbf{w})$ — формы, такие, что

$$\sum f_k(\mathbf{z})\, g_k(\mathbf{w}) = \sum z_k w_k. \tag{4}$$

Пусть $\mu_1, \ldots, \mu_l$ — последовательные минимумы для $G(\mathbf{w}) = \max |g_k(\mathbf{w})|$. Покажем, что

$$l^{-1} \leqslant \lambda_k \mu_{l+1-k} \leqslant (l-1)!. \tag{5}$$

Мы сохраняем соглашения, принятые в доказательстве теоремы XVI B. В частности, (8.5) сохраняет силу. Пусть $\mathbf{Z}$ — целая матрица со столбцами $\mathbf{z}^{(k)}$. Имеет место тождество

$$(\operatorname{adj} \mathbf{Z})\, \mathbf{G} = \Delta^{-1} \operatorname{adj} (\mathbf{FZ}), \tag{6}$$

где „adj“ обозначает присоединенную матрицу, т. е. транспонированную матрицу алгебраических дополнений. Элементы k-го столбца матрицы $\mathbf{FZ}$ имеют вид $f_i(\mathbf{z}^{(k)})$, и, значит, их абсолютная величина не больше λ_k. Элементы k-й строки матрицы $\operatorname{adj}(\mathbf{FZ})$ не превосходят величины[1])

$$(l-1)! \prod_{j \neq k} \lambda_j \leqslant (l-1)!\, |\Delta|\, \lambda_k^{-1}, \tag{7}$$

если оценивать их грубо и пользоваться (1). Следовательно, по (6)

$$|g_j(\overline{\mathbf{w}}^{(k)})| \leqslant (l-1)!\, \lambda_k^{-1},$$

где $\overline{\mathbf{w}}^{(k)}$ есть k-я строка матрицы $\operatorname{adj} \mathbf{Z}$. Таким образом, существует $l+1-k$ линейно независимых целых векторов $\mathbf{w}$ с $G(\mathbf{w}) \leqslant (l-1)!\, \lambda_k^{-1}$, что и доказывает правую часть (5). Пусть[2]) теперь $\mathbf{w}^{(k)}$ — линейно независимые целые векторы с $G(\mathbf{w}^{(k)}) = \mu_k$. Тогда векторы $\mathbf{z}$, для которых

$$\mathbf{w}^{(j)} \mathbf{z} = 0 \qquad (1 \leqslant j \leqslant l+1-k),$$

лежат в подпространстве размерности $k-1$, и, значит, существуют i, j с

$$\mathbf{w}^{(j)} \mathbf{z}^{(i)} \neq 0, \qquad 1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant l+1-k.$$

---

[1]) Следствие из леммы 5 гл. VIII позволяет заменить в (7) $(l-1)!$ числом $(l-1)^{1/2\,(l-1)}$.

[2]) Это отклонение от обозначения в § 8.

Следовательно, поскольку $\mathbf{w}^{(j)}$, $\mathbf{z}^{(i)}$ — целые,

$$1 \leqslant |\mathbf{w}^{(j)}\mathbf{z}^{(i)}| = \left|\sum_h f_h(\mathbf{z}^{(i)}) g_h(\mathbf{w}^{(j)})\right| \leqslant$$

$$\leqslant lF(\mathbf{z}^{(i)})\, G(\mathbf{w}^{(j)}) = l\lambda_i\mu_j \leqslant l\lambda_k\mu_{l+1-k},$$

что доказывает левую часть (5).

Условие (4) несколько сильнее, чем условие теоремы I о целочисленности коэффициентов в $\sum f_k(\mathbf{z})\, g_k(\mathbf{w})$, но оно охватывает все нужные приложения. По (3), (5) имеем $\mu_1 \leqslant \leqslant \gamma_1 |\lambda_1 d|^{1/(l-1)}$, где $d = \Delta^{-1}$ и γ_1 зависит только от l. Это — теорема I для нашего частного случая (4), если не учитывать величину γ_1. Далее, (2), (4) вместе дают $0 < \gamma_3 \leqslant \mu_1\Lambda \leqslant \gamma_2$ с γ_2, γ_3, зависящими только от l, что связывает однородную задачу для g_k с неоднородной задачей для f_k.

ЗАМЕЧАНИЯ

§ 2. Малер (1939a). Обобщение на выпуклые области см. у Малера (1939b).

§ 3. Более точную форму теоремы III см. у Давенпорта (1954), (1955). Доказательство того, что существует $\gamma > 0$, такое, что (3.1) справедливо для несчетного множества действительных θ_j и всех целых $x > 0$, см. у Касселса (1955).

§ 4. Главка (1952). Очевидно, теорема V обобщается почти сразу на все выпуклые области. Более точные результаты см. у Кнезера (1955) и Берча (1956).

§ 5. Берч (1957). У него получены более точные результаты.

§ 6. Хинчин (1948b) и Касселс (1952b). Обобщения см. у Касселса (1952b), Шаботи и Лутца (1950), Главки (1954b), а близкие к этому работы см. у Ярника (1946), (1954).

Получение наилучшей постоянной в теореме XI является интересной нерешенной задачей. Можно показать, что эта постоянная $\leqslant {}^1/_{12}$ и $> {}^1/_{45\cdot 2}$.

Одну форму леммы 2, имеющей силу для всех $k > 1$, см. у Хинчина (1926).

§ 7. Хинчин (1926) и (1948b).

§ 8. Хинчин (1948a). Приведенные здесь рассуждения предложены Берчем.

§ 9. Большинство приведенных здесь рассуждений восходит к Малеру. [См., например, Малер (1955).]

Глава VI

ПРИБЛИЖЕНИЕ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ РАЦИОНАЛЬНЫМИ. ТЕОРЕМА РОТА

§ 1. Введение. Для понимания этой главы не требуется никаких предварительных знаний из теории алгебраических чисел.

Число ξ называется *алгебраическим*, если оно удовлетворяет уравнению

$$f(\xi)=0, \qquad f(x)=a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0, \tag{1}$$

где $a_n, \ldots, a_0$ — рациональные числа. Можно считать, что $a_n, \ldots, a_0$ — целые, умножив в случае надобности $f(x)$ на подходящее целое число. Не ограничивая общности[1]), будем считать $a_n \neq 0$. Как впервые заметил Лиувилль, иррациональное алгебраическое число не может быть слишком хорошо приближено рациональными числами. Его рассуждения очень просты[2]). Пусть $\xi=\xi_1, \xi_2, \ldots, \xi_n$ являются корнями уравнения $f(x)=0$, так что $f(x)=a_n\prod(x-\xi_j)$. Предположим, что $q>0$, p — целые и что $|\xi-p/q|<1$. Тогда, с одной стороны,

$$|f(p/q)|=|a_n||\xi-p/q|\prod_{j\geqslant 2}|\xi_j-p/q|\leqslant$$
$$\leqslant|a_n||\xi-p/q|\prod_{j\geqslant 2}(|\xi|+1+|\xi_j|)=c|\xi-p/q|, \tag{2}$$

где $c>0$ — постоянная. С другой стороны,

$$q^n f(p/q)=a_n p^n + a_{n-1}p^{n-1}q + \ldots + a_0 q^n$$

является целым числом, и поэтому

$$|q^n f(p/q)|\geqslant 1, \tag{3}$$

---

[1]) Мы не предполагаем, что полином $f(x)$ неприводим, так как в этой главе понятие неприводимости нам не понадобится.

[2]) Ср. с теоремой III гл. V.

кроме, быть может, конечного числа дробей $p/q = \xi_j \neq \xi$ (равенство $p/q = \xi$ невозможно, так как ξ иррационально). Сравнивая (2) и (3), мы видим, что существует только конечное число решений неравенства

$$|\xi - p/q| < c^{-1}q^{-n}. \tag{4}$$

Эта глава посвящена доказательству более сильного результата:

Теорема I (Рот). *Пусть ξ — иррациональное алгебраическое число и $\delta > 0$ как угодно мало. Тогда существует только конечное число пар целых $q > 0$, p, таких, что*

$$|\xi - p/q| < q^{-2-\delta}. \tag{5}$$

Заметим, что степень полинома не участвует в формулировке теоремы. Так как для любого иррационального ξ существует бесконечно много решений $q > 0$, p неравенства (5) при $\delta = 0$ (см. гл. I), то эта теорема является наилучшей в своем роде. Но при $n = 2$ результат Лиувилля все же сильнее.

§ 2. Предварительные замечания. Прежде всего заметим, что теорему Рота надо доказать только для случая, когда[1]) в (1.1) коэффициент $a_n = 1$, так как $a_n\xi = \Xi$ удовлетворяет уравнению $\Xi^n + a_{n-1}\Xi^{n-1} + \ldots + a_n^{n-1}a_0 = 0$. Если (1.5) имеет место, то при достаточно большом q

$$|\Xi - a_n p/q| < |a_n| q^{-2-\delta} < q^{-2-\delta/2}. \tag{1}$$

Значит, неравенство (1) имеет бесконечно много решений, если бесконечно много решений имеет (1.5). Так как δ произвольно, то Ξ не подчинялось бы теореме Рота, если бы ей не подчинялось ξ. Поэтому мы будем считать, что

$$f(\xi) = 0, \quad f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0, \tag{2}$$

где $a_{n-1}, \ldots, a_0$ — целые. Положим

$$a = \max(1, |a_{n-1}|, \ldots, |a_0|). \tag{3}$$

Эти соглашения относительно ξ, $f(x)$, n, a сохраняются до конца данной главы.

---

[1]) То есть когда ξ — целое алгебраическое число.

В дальнейшем мы будем пользоваться полиномами

$$R(x_1, \ldots, x_m) = \sum_{\substack{0 \leqslant j_\mu \leqslant r_\mu \\ (1 \leqslant \mu \leqslant m)}} C(j_1, \ldots, j_m) x_1^{j_1}, \ldots, x_m^{j_m}$$

от m переменных x_μ $(1 \leqslant \mu \leqslant m)$ с действительными коэффициентами $C(j_1, \ldots, j_m)$. Введем следующие обозначения:

$$\overline{|R|} = \max |C(j_1, \ldots, j_m)|$$

и

$$R_{l_1 \ldots l_m} = \frac{1}{l_1! \ldots l_m!} \cdot \frac{\partial^{l_1 + \cdots + l_m} R}{\partial x_1^{l_1} \ldots \partial x_m^{l_m}}$$

для любого неотрицательного целого l_μ.

Лемма 1. *Если R имеет целые коэффициенты, то и $R_{l_1 \ldots l_m}$ тоже имеет целые коэффициенты. Если R — полином степени r_μ относительно x_μ, то $R_{l_1 \ldots l_m}$ — полином степени не выше $r_\mu - l_\mu$ (и, значит, он обращается в нуль при $l_\mu > r_\mu$ для любого μ). Наконец,*

$$\overline{|R_{l_1 \ldots l_m}|} \leqslant 2^{r_1 + \cdots + r_m} \overline{|R|}.$$

Доказательство. Прежде всего имеем

$$R_{l_1 \ldots l_m} = \sum_{l_\mu \leqslant j_\mu \leqslant r_\mu} \binom{j_1}{l_1} \ldots \binom{j_m}{l_m} C(j_1, \ldots, j_m) x_1^{j_1 - l_1} \ldots x_m^{j_m - l_m}, \tag{4}$$

где биномиальные коэффициенты $\binom{j}{l}$ — целые числа. Так как при $0 \leqslant l \leqslant j \leqslant r$

$$\binom{j}{l} \leqslant \sum_{0 \leqslant l \leqslant j} \binom{j}{l} = (1+1)^j \leqslant 2^r, \tag{5}$$

то лемма доказана.

По теореме Тейлора справедливо тождество

$$R(x_1 + y_1, \ldots, x_m + y_m) = \\ = \sum_{0 \leqslant l_\mu \leqslant r_\mu} y_1^{l_1} \ldots y_m^{l_m} R_{l_1 \ldots l_m}(x_1, \ldots, x_m). \tag{6}$$

Будем говорить, что R имеет *индекс* I *в* $(\alpha_1, \ldots, \alpha_m)$ *относительно* $(s_1, \ldots, s_m)$, где $\alpha_1, \ldots, \alpha_m$ — любые числа, $s_1, \ldots, s_m$ — целые положительные, если I есть наименьшее значение суммы $\sum i_\mu/s_\mu$, при котором $R_{i_1 \ldots i_m}(\alpha_1, \ldots, \alpha_m)$ не обращается в нуль. Из (6) следует, что такие $i_1, \ldots, i_m$ существуют, кроме случая, когда R тождественно обращается в нуль. В этом случае условимся считать индекс равным $+\infty$.

Лемма 2. *Пусть символ* ind *обозначает индекс в* $(\alpha_1, \ldots, \alpha_m)$ *относительно* $(s_1, \ldots, s_m)$. *Тогда*

(i) $\operatorname{ind} R_{i_1 \ldots i_m} \geqslant \operatorname{ind} R - \sum i_\mu/s_\mu$.

(ii) $\operatorname{ind}(R^{(1)} + R^{(2)}) \geqslant \min(\operatorname{ind} R^{(1)}, \operatorname{ind} R^{(2)})$.

(iii) $\operatorname{ind} R^{(1)}R^{(2)} = \operatorname{ind} R^{(1)} + \operatorname{ind} R^{(2)}$.

Доказательство (i) очевидно.

(ii), (iii). Положим $s = s_1 \ldots s_m$ и $I = \operatorname{ind} R$. Согласно (6), t^{sI} есть, очевидно, наименьшая степень переменной t, фактически встречающаяся в функции

$$R\left(\alpha_1 + t^{s/s_1} y_1, \ldots, \alpha_m + t^{s/s_m} y_m\right),$$

рассматриваемой как полином от независимых переменных

$$t, y_1, \ldots, y_m.$$

Доказательство теоремы I распадается на три основные части, которые мы рассматриваем отдельно в § 3, 4, 5. Выводы каждого параграфа формулируются соответственно в виде теорем II, III, IV. Наконец, в § 6 уже легко доказывается теорема I с помощью теорем II, III, IV.

§ 3. Построение полинома $R(x_1, \ldots, x_m)$.

Теорема II. *Пусть* $\varepsilon > 0$ — *любое число, и пусть целое*

$$m > 8n^2\varepsilon^{-2}, \tag{1}$$

где n — *степень полинома* $f(x)$; *пусть* $r_1, \ldots, r_m$ — *любые целые положительные числа. Тогда существует полином* $R(x_1, \ldots, x_m)$ *с целыми коэффициентами, степени не выше* r_μ *относительно* x_μ $(1 \leqslant \mu \leqslant m)$, *который*

(i) *не равен нулю тождественно,*

(ii) *имеет индекс в* $(\xi, \ldots, \xi)$ *относительно* $(r_1, \ldots, r_m)$, *который не меньше*

$$\frac{1}{2} m (1 - \varepsilon), \tag{2}$$

(iii) *удовлетворяет неравенству*

$$\overline{|R|} \leqslant \gamma^{r_1 + \ldots + r_m}, \quad \gamma = 4(a+1), \tag{3}$$

где а определяется равенством (2.3).

Замечание. Вид неравенства (1) и значение величины γ не играют роли. Для нашей дальнейшей цели достаточно того, что утверждения теоремы имеют место для всех m, бо́льших некоторой постоянной, зависящей от ξ, ε, и для некоторой величины γ, зависящей, быть может, от ε, ξ, m.

Для доказательства этой теоремы нам понадобится несколько лемм.

Лемма 3. *Пусть дано M линейных форм*

$$L_j = \sum_{1 \leqslant k \leqslant N} a_{jk} z_k \qquad (1 \leqslant j \leqslant M)$$

от $N > M$ переменных с целыми коэффициентами. Предположим, что

$$|a_{jk}| \leqslant A \qquad (1 \leqslant j \leqslant M; \quad 1 \leqslant k \leqslant N).$$

Тогда существуют целые значения переменных $z_1, \ldots, z_N$, не равные одновременно нулю, такие, что

$$L_j = 0 \ \ (1 \leqslant j \leqslant M), \ |z_k| \leqslant Z = \left[(NA)^{M/(N-M)}\right] (1 \leqslant k \leqslant N).$$

Доказательство. Имеем

$$NA < (Z+1)^{(N-M)/M},$$

и, следовательно, $NAZ + 1 \leqslant NA(Z+1) < (Z+1)^{N/M}$. Для любого множества целых значений вектора $\mathbf{z} = (z_1, \ldots, z_N)$ при $0 \leqslant z_k \leqslant Z$ $(1 \leqslant k \leqslant N)$ имеем

$$-B_j Z \leqslant L_j(\mathbf{z}) \leqslant C_j Z, \quad B_j + C_j \leqslant NA, \tag{4}$$

где $-B_j$, C_j — суммы соответственно отрицательных и положительных коэффициентов в $L_j(\mathbf{z})$. Следовательно, целое $L_j(\mathbf{z})$ может принимать самое бо́льшее $NAZ + 1$ значений.

Таким образом, существует $(Z+1)^N$ значений векторов $\mathbf{z}$, но из них может возникнуть только $(NAZ+1)^M<(Z+1)^N$ множеств значений $(L_1, \ldots, L_M)$. Поэтому должны существовать в (4) два различных вектора $\mathbf{z}^{(1)}$, $\mathbf{z}^{(2)}$, такие, что $L_j(\mathbf{z}^{(1)})=L_j(\mathbf{z}^{(2)})$ $(1\leqslant j\leqslant M)$. Очевидно, вектор $\mathbf{z}=\mathbf{z}^{(1)}-\mathbf{z}^{(2)}$ удовлетворяет утверждению леммы.

Лемма 4. *Для каждого целого $l\geqslant 0$ существуют целые рациональные $a_j^{(l)}$ $(0\leqslant j<n)$, такие, что*

$$\xi^l=a_{n-1}^{(l)}\xi^{n-1}+\ldots+a_0^{(l)}$$

и $|a_j^{(l)}|\leqslant(a+1)^l$, где a определяется по (2.3).

Доказательство. При $l<n$ лемма очевидна. При $l\geqslant n$ рассуждаем по индукции:

$$\xi^l=\xi\cdot\xi^{l-1}=a_{n-1}^{(l-1)}\xi^n+\ldots+a_0^{(l-1)}\xi,$$

и, далее,

$$\xi^n=-a_{n-1}\xi^{n-1}-\ldots-a_0.$$

Лемма 5. *Для любых целых положительных чисел $r_1, \ldots, r_m$ и действительного $\lambda>0$ число систем целых $l_1, \ldots, l_m$, таких, что*

$$\sum l_\mu/r_\mu\leqslant\frac{1}{2}(m-\lambda),\quad 0\leqslant l_\mu\leqslant r_\mu\qquad(1\leqslant\mu\leqslant m),$$

не превосходит

$$(2m)^{1/2}\lambda^{-1}(r_1+1)\ldots(r_m+1). \tag{5}$$

Доказательство. Случай $m=1$ очевиден, так как число решений не превосходит r_1+1 и равняется нулю при $\lambda>1$.

В случае $m>1$ будем считать, что

$$\lambda>(2m)^{1/2}>1, \tag{6}$$

ибо иначе лемма тривиальна. Предположим, что лемма уже доказана для $m-1$. Следовательно, при фиксированных $r=r_m$, $l=l_m$ число целых $l_1, \ldots, l_{m-1}$ не превосходит

$$(2m-2)^{1/2}(\lambda-1+2l/r)^{-1}(r_1+1)\ldots(r_{m-1}+1). \tag{7}$$

Но

$$\sum_{0 \leqslant l \leqslant r} \frac{2}{\lambda - 1 + 2l/r} < \sum \left(\frac{1}{\lambda - 1 + 2l/r} + \frac{1}{\lambda + 1 - 2l/r} \right) =$$

$$= \sum \frac{2\lambda}{\lambda^2 - (1 - 2l/r)^2} < 2(r+1)\lambda/(\lambda^2 - 1) \qquad (8)$$

и по (6)

$$\lambda^2 - 1 > \lambda^2 (1 - 1/2m) > \lambda^2 (1 - 1/m)^{1/2}. \qquad (9)$$

Справедливость леммы теперь следует из (7), (8), (9), если заставить $l = l_m$ принимать все значения $0, 1, \ldots, r = r_m$.

Доказательство теоремы II. Запишем полином

$$R(x_1, \ldots, x_m) = \sum_{0 \leqslant j_\mu \leqslant r_\mu} C(j_1, \ldots, j_m) x_1^{j_1} \ldots x_m^{j_m},$$

где подлежащие определению $C(j_1, \ldots, j_m)$ — целые числа и их всего $N = (r_1 + 1) \ldots (r_m + 1)$. Мы должны иметь

$$R_{i_1 \ldots i_m}(\xi, \ldots, \xi) = 0 \qquad (10)$$

для всех целых $i_1, \ldots, i_m$, таких, что

$$\sum i_\mu / r_\mu \leqslant \frac{1}{2} m (1 - \varepsilon). \qquad (11)$$

Так как (10) справедливо, очевидно, при $i_\mu > r_\mu$ для всех μ, то можно считать, что

$$0 \leqslant i_\mu \leqslant r_\mu \qquad (1 \leqslant \mu \leqslant m). \qquad (12)$$

Выражая согласно лемме 4 все степени числа ξ через $1, \xi, \ldots, \xi^{n-1}$, мы видим, что (10) будет иметь место, если существует решение соответствующей системы n линейных уравнений[1]) с целыми рациональными коэффициентами и с неизвестными $C(j_1, \ldots, j_m)$. По (2.4) и по лемме 4 эти коэффициенты имеют вид

$$\binom{j_1}{i_1} \ldots \binom{j_m}{i_m} a_j^{(l)} \qquad (0 \leqslant j < n), \qquad (13)$$

где $l = (j_1 - i_1) + \ldots + (j_m - i_m) \leqslant r_1 + \ldots + r_m$. Следовательно, числа в (13) — целые, не превосходящие

$$A = (2a + 2)^{r_1 + \ldots + r_m} \qquad (14)$$

---

[1]) Равенство (10) эквивалентно n уравнениям, если полином $f(x)$ неприводим, но нам нет нужды считать его неприводимым.

по абсолютной величине, согласно лемме 4 и (2.5). По лемме 5 с $\lambda = m\varepsilon$ и по (1) для числа M всех линейных уравнений справедлива оценка

$$M \leqslant n \cdot (2m)^{1/2} (m\varepsilon)^{-1} N \leqslant \frac{1}{2} N. \qquad (15)$$

Согласно лемме 3, существуют не равные нулю одновременно целые $C(j_1, \ldots, j_m)$, удовлетворяющие (10) при выполнении (11), (12), такие, что

$$|C(j_1, \ldots, j_m)| \leqslant (NA)^{M/(N-M)}.$$

Так как по (2.5)

$$N = (r_1 + 1) \ldots (r_m + 1) \leqslant 2^{r_1 + \ldots + r_m},$$

то, используя (14), (15), имеем

$$|C(j_1, \ldots, j_m)| \leqslant NA \leqslant \gamma^{r_1 + \ldots + r_m}.$$

§ 4. Поведение полинома R в рациональных точках в окрестности точки $(\xi, \ldots, \xi)$.

Теорема III. *Пусть* $q_\mu > 0$, p_μ $(1 \leqslant \mu \leqslant m)$ — *целые, и пусть*

$$\eta_\mu = \frac{p_\mu}{q_\mu} - \xi, \quad |\eta_\mu| < q_\mu^{-2-\delta}, \qquad (1)$$

где

$$0 < \delta < 1/12. \qquad (2)$$

Пусть ε — *любое число, такое, что*

$$0 < \varepsilon < \delta/20, \qquad (3)$$

$$q_\mu^\varepsilon > 64(a+1) \max(1, |\xi|) \qquad (1 \leqslant \mu \leqslant m). \qquad (4)$$

Пусть $r_1, \ldots, r_m$ — *любые целые положительные числа, такие, что*

$$r_1 \log q_1 \leqslant r_\mu \log q_\mu \leqslant (1+\varepsilon) r_1 \log q_1 \qquad (1 \leqslant \mu \leqslant m). \qquad (5)$$

Тогда индекс полинома R, построенного в теореме II, *в точке* $(p_1/q_1, \ldots, p_m/q_m)$ *относительно* $(r_1, \ldots, r_m)$ *не менее*

$$\delta m/8. \qquad (6)$$

Замечание. Вид неравенств (2) — (6) не играет особой роли. Для нас достаточно, чтобы существовала некоторая явная нижняя грань для индекса при достаточно больших q_μ и $r_\mu \log q_\mu$, мало отличающихся друг от друга.

Доказательство. Пусть $j_1, \ldots, j_m$ — любые неотрицательные числа, такие, что

$$\sum j_\mu/r_\mu < \delta m/8, \tag{7}$$

и положим

$$T(x_1, \ldots, x_m) = R_{j_1 \ldots j_m}(x_1, \ldots, x_m).$$

Мы должны показать, что

$$T(p_1/q_1, \ldots, p_m/q_m) = 0.$$

По теореме II и по лемме 1 $\overline{|T|} \leqslant (2\gamma)^{r_1+\ldots+r_m}$ и T имеет целые коэффициенты. Так как степень полинома T относительно x_μ не выше r_μ, то полином T содержит не более $(r_1+1)\ldots(r_m+1) \leqslant 2^{r_1+\ldots+r_m}$ членов. Следовательно, для любых целых положительных $l_1, \ldots, l_m$ имеем, опять используя лемму 1 и оценивая грубо,

$$\begin{gathered} |T_{l_1 \ldots l_m}(\xi, \ldots, \xi)| \leqslant \\ \leqslant (r_1+1) \ldots (r_m+1) \cdot 2^{r_1+\ldots+r_m} \cdot (2\gamma)^{r_1+\ldots+r_m} \times \\ \times (\max(1, |\xi|))^{r_1+\ldots+r_m} \leqslant \gamma_1^{r_1+\ldots+r_m}, \\ \gamma_1 = 8\gamma \max(1, |\xi|). \end{gathered} \tag{8}$$

Используя лемму 2, теорему II (ii), (3) и (7), мы видим, что индекс T в точке $(\xi, \ldots, \xi)$ относительно $(r_1, \ldots, r_m)$ не меньше

$$\frac{1}{2} m(1-\varepsilon) - \sum j_\mu/r_\mu > \frac{1}{2} m\left(1-\varepsilon-\frac{1}{4}\delta\right) > \frac{1}{2} m\left(1-\frac{1}{3}\delta\right). \tag{9}$$

Но по (2.6) и (1) имеем

$$T(p_1/q_1, \ldots, p_m/q_m) = \sum_{0 \leqslant l_\mu \leqslant r_\mu} T_{l_1 \ldots l_m}(\xi, \ldots, \xi)\, \eta_1^{l_1} \ldots \eta_m^{l_m}, \tag{10}$$

где, согласно (9), обращаются в нуль те слагаемые, для которых

$$\sum l_\mu/r_\mu \geqslant \frac{1}{2} m\left(1-\frac{1}{3}\delta\right). \tag{11}$$

Для таких $l_1, \ldots, l_m$ из неравенств (1), (5) следует, что

$$-\log|\eta_1^{l_1} \ldots \eta_m^{l_m}| \geqslant (2+\delta) \sum l_\mu \log q_\mu \geqslant$$
$$\geqslant (2+\delta) r_1 \log q_1 \sum l_\mu / r_\mu \geqslant$$
$$\geqslant (2+\delta) r_1 \log q_1 \cdot \frac{1}{2} m \left(1-\frac{1}{3}\delta\right) \geqslant$$
$$\geqslant \left(1+\frac{1}{2}\delta\right)\left(1-\frac{1}{3}\delta\right)(1+\varepsilon)^{-1} \sum r_\mu \log q_\mu.$$

Но по (2), (3)

$$\left(1+\frac{1}{2}\delta\right)\left(1-\frac{1}{3}\delta\right) = 1+\frac{1}{6}\delta(1-\delta) > 1+\frac{1}{8}\delta > (1+\varepsilon)^2,$$

и, значит,

$$|\eta_1^{l_1} \ldots \eta_m^{l_m}| < \left(q_1^{r_1} \ldots q_m^{r_m}\right)^{-1-\varepsilon}. \tag{12}$$

Так как в правой части (10) число членов не превосходит

$$(r_1+1) \ldots (r_m+1) \leqslant 2^{r_1+\ldots+r_m},$$

то из (8), (10), (12), (4) получаем

$$|q_1^{r_1} \ldots q_m^{r_m} T(p_1/q_1, \ldots, p_m/q_m)| < \prod_\mu \left(2\gamma_1 q_\mu^{-\varepsilon}\right)^{r_\mu} < 1,$$

ибо $2\gamma_1 = 16\gamma \max(1, |\xi|) = 64(a+1)\max(1, |\xi|)$, согласно (3.3) и (8). Но $q_1^{r_1} \ldots q_m^{r_m} T(p_1/q_1, \ldots, p_m/q_m)$ — число целое, и, значит, оно равняется нулю. Теорема доказана.

§ 5. Поведение полинома с целыми коэффициентами в рациональных точках.

Теорема IV. *Пусть*

$$\omega = \omega(m, \varepsilon) = 24 \cdot 2^{-m} (\varepsilon/12)^{2m-1}, \tag{1}$$

где m — целое положительное число, и

$$0 < \varepsilon < {}^1/_{12}. \tag{2}$$

Пусть $r_1, \ldots, r_m$ — целые положительные числа, подчиняющиеся условию

$$\omega r_\mu \geqslant r_{\mu+1} \qquad (1 \leqslant \mu < m), \tag{3}$$

и пусть $q_\mu > 0$, p_μ — взаимно простые целые, такие, что

$$q_\mu^{r_\mu} \geqslant q_1^{r_1} \qquad (1 \leqslant \mu \leqslant m), \tag{4}$$

$$q_\mu^{\omega} \geqslant 2^{3m} \qquad (1 \leqslant \mu \leqslant m). \tag{5}$$

Предположим, что $S(x_1, \ldots, x_m)$ — отличный от тождественного нуля полином с целыми коэффициентами степени не выше r_μ относительно x_μ $(1 \leqslant \mu \leqslant m)$ и

$$\overline{|S|} \leqslant q_1^{\omega r_1}. \tag{6}$$

Тогда S имеет индекс в $(p_1/q_1, \ldots, p_m/q_m)$ относительно $(r_1, \ldots, r_m)$ не выше ε.

Замечание. Точный вид неравенств (1) — (6) не играет особой роли. Для нас достаточно, чтобы индекс, о котором идет речь, был мал (или же ограничен сверху абсолютной постоянной), если коэффициенты многочлена S не слишком большие, q_μ достаточно велики, а r_μ убывают достаточно быстро. Что условие такого типа на r_μ необходимо, следует из того, что многочлен $(x-y)^r$ в любой точке $(p/q, p/q)$ имеет индекс относительно (r, r) не менее 1.

Доказательство проводится по индукции с использованием операторов вида

$$\Delta = \frac{\partial^{l_1 + \ldots + l_m}}{\partial x_1^{l_1} \ldots \partial x_m^{l_m}}. \tag{7}$$

Будем называть $l_1 + \ldots + l_m$ *порядком оператора* Δ. Если $\Delta_1, \ldots, \Delta_h$ имеют соответственно порядки не более чем $0, \ldots, h-1$ и $\varphi_1, \ldots, \varphi_h$ — функции от $x_1, \ldots, x_m$, то определитель

$$\det(\Delta_i \varphi_j) \qquad (1 \leqslant i,\ j \leqslant h) \tag{8}$$

назовем (обобщенным) *вронскианом*. Если $m = 1$, то существует один и только один оператор Δ порядка $i-1$, а именно d^{i-1}/dx_1^{i-1}, и, значит, единственный вронскиан, который не обращается тривиально в нуль, будет обыкновенным вронскианом

$$\det\left(\frac{d^{i-1}\varphi_j}{dx_1^{i-1}}\right).$$

Лемма 6. *Предположим, что $\varphi_1, \ldots, \varphi_h$ — рациональные функции*[1]) *от $x_1, \ldots, x_m$, и что из равенства*

$$c_1\varphi_1 + \ldots + c_h\varphi_h = 0 \tag{9}$$

при постоянных $c_1, \ldots, c_h$ следует $c_1 = \ldots = c_h = 0$. Тогда какой-нибудь вронскиан (8) *не обращается в нуль.*

Замечание. Если (9) имеет место при некоторых постоянных $c_1, \ldots, c_h$, не равных одновременно нулю, то, очевидно, все вронскианы обращаются в нуль.

Доказательство. Если $h = 1$, то единственным вронскианом является сама функция φ_1, и лемма становится тривиальной. Поэтому мы будем считать, что $h > 1$ и что для системы с меньшим числом рациональных функций лемма уже доказана.

Соотношение $\varphi_1 = 0$ имеет вид (9). Значит, $\varphi_1 \neq 0$. Обозначим

$$\varphi_j^* = \varphi_1^{-1}\varphi_j \qquad (1 \leqslant j \leqslant h).$$

По правилу дифференцирования произведения всякий вронскиан, составленный из функций $\varphi_1^*, \ldots, \varphi_h^*$, представляется в виде суммы вронскианов, составленных из функций $\varphi_1, \ldots, \varphi_h$, умноженных на рациональные функции (произведения производных от φ_1^{-1}). В частности, если какой-нибудь вронскиан, составленный из $\varphi_1^*, \ldots, \varphi_h^*$, не обращается в нуль, то не обращается в нуль и какой-нибудь вронскиан, составленный из $\varphi_1, \ldots, \varphi_h$. Так как из любого соотношения вида (9) для функций φ_j^* следует такое же соотношение для функций φ_j, то можно считать, без ограничения общности, что $\varphi_1 = 1$. Если теперь φ_h была бы постоянной, например c, то имело бы место соотношение $\varphi_h - c\varphi_1 = 0$ вида (9), вопреки предположению. Следовательно, существует какая-нибудь переменная, например x_1, такая, что

$$\frac{\partial \varphi_h}{\partial x_1} \neq 0. \tag{10}$$

С другой стороны, вполне возможно, что имеется линейная комбинация

$$c_2\varphi_2 + \ldots + c_h\varphi_h, \tag{11}$$

[1]) То есть отношения полиномов.

не зависящая от x_1. Если это так, то одно из чисел $c_2, \ldots$ $\ldots, c_{h-1}$ не равно нулю, например $c_2 \neq 0$. Не ограничивая общности, считаем $c_2 = 1$. Мы заменим φ_2 выражением (11), что не влияет на вронскианы и дает

$$\partial\varphi_2/\partial x_1 = 0.$$

Продолжая рассуждать таким путем, мы можем в конце концов утверждать, что существует некоторое k, $1 \leqslant k < h$, такое, что

$$\frac{\partial\varphi_1}{\partial x_1} = \ldots = \frac{\partial\varphi_k}{\partial x_1} = 0, \tag{12}$$

но такое, что из равенства

$$e_{k+1}\frac{\partial\varphi_{k+1}}{\partial x_1} + \ldots + e_h\frac{\partial\varphi_h}{\partial x_1} = 0 \tag{13}$$

при постоянных $e_{k+1}, \ldots, e_h$ следует $e_{k+1} = \ldots = e_h = 0$. По индуктивному предположению существуют операторы $\Delta_1^*, \ldots, \Delta_k^*$ соответственно порядка не выше $0, \ldots, k-1$, такие, что

$$W_1 = \det(\Delta_l^*\varphi_j) \neq 0 \qquad (1 \leqslant l,\ j \leqslant k).$$

Аналогично, так как (13) не имеет нетривиальных решений, то существуют операторы $\Delta_{k+1}^*, \ldots, \Delta_h^*$ соответственно порядка не выше $0, \ldots, h-k-1$, такие, что

$$W_2 = \det\left(\Delta_l^*\frac{\partial\varphi_j}{\partial x_1}\right) \neq 0 \qquad (k < l,\ j \leqslant h).$$

Положим

$$\Delta_l = \begin{cases} \Delta_l^* & (1 \leqslant l \leqslant k), \\ \Delta_l^*\dfrac{\partial}{\partial x_1} & (k < l \leqslant h), \end{cases}$$

так что Δ_l имеет порядок не выше $l-1$. Тогда по (12) имеем

$$\det(\Delta_l\varphi_j) = W_1W_2 \neq 0 \qquad (1 \leqslant l,\ j \leqslant h).$$

Лемма доказана.

Следствие. *Если $\varphi_1, \ldots, \varphi_h$ имеют рациональные коэффициенты, то в* (9) *достаточно считать $c_1, \ldots, c_h$ рациональными.*

Доказательство очевидно, так как в доказательстве теоремы встречаются только рациональные числа. (Иначе можно доказать, пользуясь леммой 2 гл. III.)

Доказательство теоремы IV ($m=1$). Если

$$S(p_1/q_1)=S'(p_1/q_1)= \ldots =S^{(t-1)}(p_1/q_1)=0 \neq S^{(t)}(p_1/q_1),$$

то

$$S(x_1)=(x_1-p_1/q_1)^t\, T(x_1),$$

где $T(x_1)$ — некоторый полином. Но

$$S(x_1)=(q_1x_1-p_1)^t\left(q_1^{-t}T(x_1)\right),$$

где $q_1^{-t}T(x_1)$ — полином с целыми коэффициентами по лемме Гаусса (приложение C), так как $S(x_1)$ имеет целые коэффициенты и н. о. д. $(p_1, q_1)=1$. Поэтому старший коэффициент полинома $S(x_1)$ делится на q_1^t и, следовательно,

$$q_1^t \leqslant \overline{|S|} \leqslant q_1^{\omega r_1}=q_1^{er_1}$$

по (1) и (6). Это доказывает теорему для $m=1$, так как индекс полинома S в точке p_1/q_1 относительно r_1 равен t/r_1 по определению.

Доказательство теоремы IV ($m>1$). Проведем индукцию по m. Будем считать, что теорема верна для меньших значений m.

Ясно, что существует представление полинома S в виде

$$S=\sum_{1\leqslant j\leqslant h}\varphi_j(x_1, \ldots, x_{m-1})\,\psi_j(x_m), \tag{14}$$

где φ_j, ψ_j — полиномы с рациональными (не обязательно целыми) коэффициентами, φ_j зависят только от $x_1, \ldots, x_{m-1}$, а ψ_j зависят только от x_m, например, $h=r_m+1$ и $\psi_j=x_m^{j-1}$. Возьмем одно такое представление с наименьшим возможным h, так что

$$h\leqslant r_m+1. \tag{14'}$$

Если существует линейное соотношение $c_1\varphi_1+\ldots+c_h\varphi_h=0$ с рациональными постоянными $c_1, \ldots, c_h$ и, например, с $c_h\neq 0$, то тогда

$$S=\sum_{1\leqslant j<h}\varphi_j(\psi_j-c_j\psi_h/c_h),$$

т. е. представление с $h-1$ слагаемыми. Так как h — минимальное, то такое линейное соотношение невозможно. Аналогично из соотношения $c_1\psi_1+\ldots+c_h\psi_h=0$ с рациональными постоянными $c_1, \ldots, c_h$ следует $c_1=\ldots=c_h=0$. По следствию из леммы 6 имеем

$$U(x_m)=\det\left(\frac{1}{(i-1)!}\frac{d^{i-1}\psi_j}{dx_m^{i-1}}\right)\neq 0 \qquad (1\leqslant i,\ j\leqslant h), \quad (15)$$

где для удобства включен числовой множитель $((i-1)!)^{-1}$. По той же лемме существуют операторы Δ_i' $(1\leqslant i\leqslant h)$ вида

$$\Delta_i'=\frac{1}{i_1!\ldots i_{m-1}!}\frac{\partial^{i_1+\ldots+i_{m-1}}}{\partial x_1^{i_1}\ldots\partial x_{m-1}^{i_{m-1}}} \quad (16)$$

с

$$i_1+\ldots+i_{m-1}\leqslant i-1\leqslant h-1\leqslant r_m, \quad (17)$$

такие, что

$$V(x_1, \ldots, x_{m-1})=\det(\Delta_i'\varphi_j)\neq 0 \qquad (1\leqslant i,\ j\leqslant h). \quad (18)$$

Определим полином W так:

$$W(x_1, \ldots, x_m)=\det\left(\Delta_i'\frac{1}{(j-1)!}\frac{\partial^{j-1}}{\partial x_m^{j-1}}S(x_1, \ldots, x_m)\right) \quad (1\leqslant i,\ j\leqslant h). \quad (19)$$

Тогда по (14), (15), (18) имеем

$$W=\det\left(\Delta_i'\frac{1}{(j-1)!}\frac{\partial^{j-1}}{\partial x_m^{j-1}}\sum_k\varphi_k\psi_k\right)=U(x_m)V(x_1, \ldots, x_{m-1}).$$

Но

$$\Delta_i'\frac{1}{(j-1)!}\frac{\partial^{j-1}S}{\partial x_m^{j-1}}=S_{i_1\ldots i_{m-1}, j-1}, \quad (20)$$

если оператор Δ_i' определен формулой (16). Поэтому, согласно (19) и лемме 1, полином W имеет целые коэффициенты. Следовательно,

$$W(x_1, \ldots, x_m)=u(x_m)v(x_1, \ldots, x_{m-1}),$$

где u, v — полиномы с целыми коэффициентами, согласно лемме Гаусса (приложение C).

Так как полином в (20) имеет степень относительно x_μ $(1 \leqslant \mu \leqslant m)$ не выше r_μ, то степень определителя W относительно x_μ не выше hr_μ, т. е. $u(x_m)$ имеет степень не выше hr_μ, $v(x_1, \ldots, x_{m-1})$ имеет степень относительно x_μ $(1 \leqslant \mu < m)$ не выше hr_μ.

Согласно (6) и лемме 1,

$$\overline{\left|S_{i_1 \ldots i_{m-1}, j-1}\right|} \leqslant 2^{r_1 + \cdots + r_m} q_1^{\omega r_1}.$$

Так как в любом полиноме $S_{i_1 \ldots i_m}$ существует не более $(r_1+1)\ldots(r_m+1) \leqslant 2^{r_1+\cdots+r_m}$ членов и так как, согласно (14′), существует не более $h! \leqslant h^{h-1} \leqslant h^{r_m} \leqslant 2^{hr_m}$ произведений в разложении определителя W, то

$$\overline{|W|} \leqslant h!\left((r_1+1)\ldots(r_m+1)\right)^h \cdot \left(2^{r_1+\cdots+r_m} q_1^{\omega r_1}\right)^h <$$
$$< \left(2^{3(r_1+\cdots+r_m)} q_1^{\omega r_1}\right)^h \leqslant \left(2^{3m} q_1^{\omega}\right)^{r_1 h} \leqslant q_1^{2\omega r_1 h}$$

согласно (5), (19) и (20). Так как u, v имеют целые коэффициенты и каждый коэффициент в $W = uv$ является произведением коэффициента из $u(x_m)$ на коэффициент из $v(x_1, \ldots, x_{m-1})$, то

$$\overline{|u|} \leqslant q_1^{2\omega r_1 h}, \quad \overline{|v|} \leqslant q_1^{2\omega r_1 h}. \tag{21}$$

Теперь мы имеем

$$\omega = \omega(m, \varepsilon) = \frac{1}{2}\,\omega(m-1, \varepsilon^2/12).$$

Таким образом, мы применяем теорему к $v(x_1, \ldots, x_{m-1})$ с $m-1$ вместо m; $hr_1, \ldots, hr_{m-1}$ вместо $r_1, \ldots, r_{m-1}$; $\varepsilon^2/12$ вместо ε и, значит, 2ω вместо ω, так как (3) и (5) сильнее, чем соответствующие неравенства с 2ω вместо ω, а (21) заменяет (6). Следовательно, индекс полинома v в точке $(p_1/q_1, \ldots, p_{m-1}/q_{m-1})$ относительно $(hr_1, \ldots, hr_{m-1})$ не более $\varepsilon^2/12$. Таким образом, по определению индекс полинома $v(x_1, \ldots, x_{m-1})$, рассматриваемого как функция от $x_1, \ldots, x_m$, не более $h\varepsilon^2/12$ в точке $(p_1/q_1, \ldots, p_m/q_m)$ относительно $(r_1, \ldots, r_m)$.

Аналогично, так как по (4) $q_1^{r_1} \leqslant q_m^{r_m}$ и так как

$$\omega = \omega(m, \varepsilon) \leqslant \frac{1}{2}\,\omega(1, \varepsilon^2/12),$$

то применяем теорему к $u(x_m)$ с 1 вместо m, hr_m вместо r_1, $\varepsilon^2/12$ вместо ε. Следовательно, как и ранее, индекс полинома $u(x_m)$ в $(p_1/q_1, \ldots, p_m/q_m)$ относительно $(r_1, \ldots, r_m)$ не выше $h\varepsilon^2/12$.

По лемме 2 для индекса Θ полинома $W = uv$ справедлива оценка

$$\Theta \leqslant \frac{h\varepsilon^2}{12} + \frac{h\varepsilon^2}{12} = \frac{h\varepsilon^2}{6} \tag{22}$$

в точке $(p_1/q_1, \ldots, p_m/q_m)$ относительно $(r_1, \ldots, r_m)$.

Теперь оценим Θ через θ, где под θ понимается индекс полинома $S(x_1, \ldots, x_m)$ в точке $(p_1/q_1, \ldots, p_m/q_m)$ относительно $(r_1, \ldots, r_m)$. По лемме 2(i) соответствующий индекс полинома $S_{i_1 \ldots i_{m-1}, j-1}$ не менее

$$\theta - \frac{i_1}{r_1} - \ldots - \frac{i_{m-1}}{r_{m-1}} - \frac{j-1}{r_m} \geqslant \theta - \frac{i_1 + \ldots + i_{m-1}}{r_{m-1}} - \frac{j-1}{r_m} \geqslant$$
$$\geqslant \theta - \frac{r_m}{r_{m-1}} - \frac{j-1}{r_m} \geqslant \theta - \omega - \frac{j-1}{r_m} \geqslant \theta - \frac{\varepsilon^2}{24} - \frac{j-1}{r_m} \quad (m > 1),$$

если использовать (17), (1), (3). Так как индекс всегда неотрицательный, то получаем, развертывая определитель (19) и используя лемму 2, что

$$\Theta \geqslant \sum_{1 \leqslant j \leqslant h} \max\left(\theta - \frac{\varepsilon^2}{24} - \frac{j-1}{r_m},\ 0\right) \geqslant$$
$$\geqslant -\frac{h\varepsilon^2}{24} + \sum_{1 \leqslant j \leqslant h} \max\left(\theta - \frac{j-1}{r_m},\ 0\right).$$

Следовательно, по (22) имеем

$$h^{-1} \sum_{1 \leqslant j \leqslant h} \max\left(\theta - \frac{j-1}{r_m},\ 0\right) \leqslant \frac{\varepsilon^2}{6} + \frac{\varepsilon^2}{24} < \frac{\varepsilon^2}{4}, \tag{23}$$

где $1 \leqslant h \leqslant r_m + 1$.

Если $\theta \geqslant (h-1)/r_m$, то левая часть (23) равняется

$$\frac{1}{2}\theta + \frac{1}{2}\left(\theta - \frac{h-1}{r_m}\right) \geqslant \frac{1}{2}\theta,$$

и, значит, из (23) следует $\theta < \frac{1}{2}\varepsilon^2 < \varepsilon$, а это и есть утверждение теоремы.

Если же $\theta < (h-1)/r_m$, то левая часть (23) равняется

$$h^{-1} \sum_{0 \leqslant j-1 \leqslant \theta r_m} \left(\theta - \frac{j-1}{r_m}\right) \geqslant h^{-1}([\theta r_m]+1)\frac{1}{2}\theta \geqslant \frac{\theta^2 r_m}{2h} \geqslant \frac{\theta^2}{4},$$

так как $h \leqslant r_m + 1 \leqslant 2r_m$. Следовательно, из (23) следует $\theta \leqslant \varepsilon$, а это опять утверждение теоремы.

§ 6. Доказательство теоремы I. Предположим, что неравенство

$$|\xi - p/q| < q^{-2-\delta}, \quad q > 0, \quad (p, q) = 1 \tag{1}$$

имеет бесконечно много решений. Теорема будет доказана, если мы получим противоречие. Не ограничивая общности, можно считать, что имеет место (4.2), а именно: $0 < \delta < 1/12$.

Выберем параметры следующим образом:

(i) ε — любое число $< \delta/20$. Тогда имеют место (4.3) и (5.2).

(ii) m — любое целое $> 8n^2\varepsilon^{-2}$, т. е. имеет место (3.1); $\omega = \omega(m, \varepsilon)$ определяется по (5.1).

(iii) (p_1, q_1) — любое решение неравенства (1) с q_1 настолько большим, что имеют место (4.4), (5.5) при $\mu = 1$ и, кроме того,

$$q_1^\omega > \gamma^m, \qquad \gamma = 4(a+1). \tag{2}$$

(iv) (p_μ, q_μ) — решения неравенства (1), которые последовательно выбираются так, что

$$\frac{1}{2}\omega \log q_{\mu+1} > \log q_\mu \qquad (1 \leqslant \mu < m). \tag{3}$$

Это можно всегда сделать, так как (1) по предположению имеет бесконечно много решений. Так как $q_m > q_{m-1} > \ldots > q_1$, то условия (4.4), (5.5) имеют место для $1 \leqslant \mu \leqslant m$ по пункту (iii).

(v) r_1 — любое целое, настолько большое, что

$$\varepsilon r_1 \log q_1 \geqslant \log q_m. \tag{4}$$

(vi) Для $2 \leqslant \mu \leqslant m$ положим

$$r_\mu = \left[\frac{r_1 \log q_1}{\log q_\mu}\right] + 1. \tag{5}$$

Тогда по (4)

$$r_1 \log q_1 \leqslant r_\mu \log q_\mu \leqslant r_1 \log q_1 + \log q_\mu \leqslant (1+\varepsilon) r_1 \log q_1, \tag{6}$$

а это есть (4.5) и (5.4). Далее, из (3), (6) следует, что

$$\omega r_\mu \geqslant 2(1+\varepsilon)^{-1} r_{\mu+1} \geqslant r_{\mu+1},$$

а это есть (5.3).

Условия теорем II, III выполняются. Далее, полином R, построенный в теореме II, удовлетворяет условиям, наложенным на S в теореме IV, так как по (3.3) и (2)

$$\overline{|R|} \leqslant \gamma^{r_1+\ldots+r_m} < \gamma^{mr_1} < q_1^{\omega r_1},$$

а как показано выше, и другие условия теоремы IV тоже выполняются. Значит, по теореме III индекс R в точке $(p_1/q_1, \ldots, p_m/q_m)$ относительно $(r_1, \ldots, r_m)$ не меньше $\delta m/8$ и не больше ε по теореме IV. Следовательно, $0 < \delta \leqslant 8\varepsilon/m$. Так как ε произвольно мало, а m можно выбрать как угодно большим, то это и есть нужное нам противоречие.

ЗАМЕЧАНИЯ

Историю теоремы I см. у Рота (1955). Несколько ранее более слабые формулировки были даны Туэ, Зигелем, Дайсоном, Гельфондом, Шнейдером; они обычно называются „теоремой Туэ — Зигеля". Явную границу для чисел p, q в теореме I см. у Давенпорта и Рота (1955). Теорема I дает возможность путем обращения рассуждений § 1 получить нижнюю границу для $|q^n f(p/q)|$, благодаря чему возможны приложения к диофантовым уравнениям (ср. Ландау (1927), 3, 58—65).

Пусть $\nu > 1$. Теорема I утверждает, что $\|q\xi\| > q^{-\nu}$ для всех q, больших некоторого $q_0(\xi, \nu)$. На первый взгляд кажется парадоксальным, что неизвестны пути для отыскания допустимого $q_0(\xi, \nu)$, если $\nu < n-1$.

Числа, не являющиеся алгебраическими, называются *трансцендентными*. Так как множество алгебраических чисел счетно, то „почти все" числа являются трансцендентными в смысле гл. VII. Теорема I (или же теорема Лиувилля в § 1) дает возможность строить трансцендентные числа: любое число ξ, такое, что неравенство

$$\|q\xi\| \leqslant q^{-\nu} \tag{*}$$

имеет бесконечно много решений для некоторого $\nu > 1$, трансцендентно, например $\xi = \sum 2^{-3^n}$. (Положить $q = 2^{3^n}$.) С другой стороны, теорема I гл. VII показывает, что (*) имеет только конечное число решений для почти всех ξ; это—критерий трансцендентности для множества меры 0. Доказательство трансцендентности e и π имеется у Харди и Райта (1938). Глубокую и богатую теорию трансцендентных чисел и родственные с ней проблемы см. у Зигеля (1949), Гельфонда (1952) или Шнейдера (1956)[1]). Последние результаты о приближении e и π рациональными числами см. у Малера (1953 a, b).

[1]) Автор видел только проспект книги Шнейдера.

Глава VII

МЕТРИЧЕСКАЯ ТЕОРИЯ

§ 1. Введение. В этой главе мы будем предполагать, что читатель знаком с элементами теории меры Лебега. Как обычно, мы будем говорить, что в данном n-мерном множестве *почти нет* точек, обладающих некоторым свойством, если мера множества точек данного множества, обладающих этим свойством, равна нулю. *Почти все* точки данного множества обладают некоторым свойством, если в этом множестве почти нет точек, не обладающих этим свойством. Меру множества $\mathscr{E}$ будем обозначать так: $|\mathscr{E}|$.

В гл. II мы показали, что неравенство

$$\|q\theta\| < C/q \tag{1}$$

имеет бесконечно много целых решений для всех иррациональных θ, если $C = 5^{-1/2}$. Утверждение становится неверным, если давать C любое значение, меньшее $5^{-1/2}$. Но, с данной точки зрения, это просто случай, обусловленный существованием числа $^1/_2(5^{1/2}-1)$ и счетностью множества чисел θ, связанных с ним. Иначе число, меньшее $5^{-1/2}$, обладало бы указанным свойством. В действительности же для любого $C > {}^1/_3$ существует только счетное множество исключительных θ, для которых неравенство (1) имеет только конечное число целых решений q. Если же $C < {}^1/_3$, то, как мы видели, множество исключительных θ несчетно. Однако, как мы сейчас покажем, неравенство (1) при $C > 0$ имеет бесконечно много решений для почти всех θ. В действительности имеет место более сильное утверждение.

Теорема I. *Пусть $\psi(q)$ — монотонно убывающая функция от целочисленного аргумента $q > 0$, и пусть $0 \leqslant \psi(q) \leqslant {}^1/_2$. Тогда если ряд $\sum(\psi(q))^n$ расходится, то* *для почти всех систем n чисел $(\theta_1, \ldots, \theta_n)$ система неравенств*

$$\|q\theta_j\| < \psi(q) \qquad (1 \leqslant j \leqslant n)$$

имеет бесконечно много решений; если же ряд $\sum (\psi(q))^n$ сходится, то таких систем n чисел $(\theta_1, \ldots, \theta_n)$ почти нет.

Например, неравенство

$$\|q\theta\| < 1/q \log q$$

имеет бесконечно много целых решений для почти всех θ, что сильнее утверждения о бесконечности целых решений неравенства (1) при любом $C > 0$ для почти всех θ. Но почти нет чисел θ, для которых неравенство

$$\|q\theta\| < 1/q \log^2 q$$

имеет бесконечно много целых решений.

Существует аналогичная теорема и для неоднородных приближений, являющаяся дополнением к теореме I, и доказывается она несколько проще:

Теорема II. *Пусть $0 \leqslant \psi(q) \leqslant 1/2$ для всех q. Тогда если ряд $\sum (\psi(q))^n$ расходится, то для почти всех $2n$-мерных систем $(\theta_1, \ldots, \theta_n, \alpha_1, \ldots, \alpha_n)$ система неравенств*

$$\|q\theta_j - \alpha_j\| < \psi(q) \quad (1 \leqslant j \leqslant n)$$

имеет бесконечно много целых решений; если ряд $\sum (\psi(q))^n$ сходится, то таких $2n$-мерных систем $(\theta_1, \ldots, \theta_n, \alpha_1, \ldots, \alpha_n)$ почти нет.

Замечание. Здесь не требуется монотонность функции $\psi(q)$.

Ясно, что достаточно рассматривать числа θ_j, α_j только из интервала $0 \leqslant \theta_j < 1$, $\theta \leqslant \alpha_j < 1$.

Ради простоты мы рассмотрим только случай $n = 1$, указав в § 7 на незначительные видоизменения, необходимые в случае $n > 1$. Все множества, которые будут встречаться в последующих рассуждениях, как легко видеть, измеримы.

§ 2. Случай сходимости ($n = 1$). Теоремы I и II в случае сходимости указанных выше рядов следуют сразу из следующей леммы.

Лемма 1. *Пусть α зафиксировано и пусть ряд $\sum \psi(q)$, где $0 \leqslant \psi(q) \leqslant {}^1/_2$, сходится. Тогда почти нет чисел θ, для которых неравенство*

$$\|q\theta - \alpha\| < \psi(q) \tag{1}$$

имеет бесконечно много целых решений $q > 0$.

Доказательство. При фиксированных α, q числа θ, удовлетворяющие неравенству (1), т. е.

$$\left|\theta - \frac{p+\alpha}{q}\right| < \frac{\psi(q)}{q} \qquad (p \text{ — целое}),$$

образуют на действительной оси множество интервалов длиной $2\psi(q)/q$ с центрами, отстоящими друг от друга на расстоянии $1/q$. Значит, множество чисел θ, $0 \leqslant \theta < 1$, удовлетворяющих неравенству (1), имеет меру $2\psi(q)$. Следовательно, множество чисел θ, для которых (1) имеет решение при $q \geqslant Q$, имеет меру, не превосходящую

$$2 \sum_{q \geqslant Q} \psi(q) < \varepsilon$$

при любом $\varepsilon > 0$ и достаточно большом Q. В частности, множество чисел θ, для которых неравенство (1) имеет бесконечно много решений, имеет меру, не превосходящую ε. Лемма доказана, так как ε произвольно мало.

§ 3. Две леммы. Пусть функции $f(x, y) \geqslant 0$, $g(x, y) \geqslant 0$ определены, например, в единичном квадрате

$$\mathcal{J}: \quad 0 \leqslant x < 1, \quad 0 \leqslant y < 1.$$

Тогда хорошо известное неравенство Шварца утверждает, что [1])

$$\left(\iint_{\mathcal{J}} fg\,dx\,dy\right)^2 \leqslant \left(\iint_{\mathcal{J}} f^2\,dx\,dy\right)\left(\iint_{\mathcal{J}} g^2\,dx\,dy\right). \tag{2}$$

---

[1]) Это интегральный аналог неравенства $\left(\sum a_j b_j\right)^2 \leqslant \left(\sum a_j^2\right)\left(\sum b_j^2\right)$. Вероятно, наиболее простое доказательство неравенства (2) получится, если заметить, что квадратичная форма $h(X, Y) = \iint (Xf + Yg)^2\,dx\,dy \geqslant 0$ и что разность между левой и правой частями неравенства (2) есть дискриминант h.

В частности ($g=1$),

$$M_1=\iint_{\mathcal{T}} f\,dx\,dy \leqslant M_2=\left(\iint_{\mathcal{T}} f^2\,dx\,dy\right)^{1/2}.$$

Лемма 2 (Пойа и Зигмунд). *Пусть* $f(x, y)\geqslant 0$, $M_1\geqslant aM_2$ *и* $0\leqslant b\leqslant a$. *Тогда множество* $\mathcal{E}$, *в котором* $f(x, y)\geqslant bM_2$ ($\geqslant bM_1$), *имеет меру* $|\mathcal{E}|\geqslant(a-b)^2$.

Замечание. Существует аналогичный результат и для функций от любого числа переменных.

Доказательство. Согласно неравенству Шварца,

$$\left(\iint_{\mathcal{E}} f\,dx\,dy\right)^2\leqslant\left(\iint_{\mathcal{E}} dx\,dy\right)\left(\iint_{\mathcal{E}} f^2\,dx\,dy\right)\leqslant$$
$$\leqslant|\mathcal{E}|\iint_{\mathcal{T}} f^2\,dx\,dy=|\mathcal{E}|\,M_2^2. \qquad (3)$$

Так как $f\leqslant bM_2$ в[1]) $\mathcal{T}-\mathcal{E}$, то

$$\iint_{\mathcal{E}} f\,dx\,dy=\iint_{\mathcal{T}} f\,dx\,dy-\iint_{\mathcal{T}-\mathcal{E}} f\,dx\,dy\geqslant$$
$$\geqslant M_1-bM_2\geqslant(a-b)\,M_2. \qquad (4)$$

Теперь лемма следует сразу из (3) и (4).

Лемма 3. *Пусть* $\delta(x)$ — *функция от действительного переменного* x *с периодом* 1. *Тогда для любого действительного* α *и целого* $q\neq 0$

$$\int_0^1 \delta(qx+\alpha)\,dx=\int_0^1 \delta(x)\,dx.$$

Доказательство.

$$\int_0^1 \delta(qx+\alpha)\,dx=\int_{\alpha/q}^{1+\alpha/q} \delta(qx)\,dx=\int_0^1 \delta(qx)\,dx=$$
$$=\frac{1}{q}\int_0^q \delta(y)\,dy=\int_0^1 \delta(x)\,dx,$$

---

[1]) $\mathcal{T}-\mathcal{E}$ есть множество точек, принадлежащих $\mathcal{T}$, но не принадлежащих $\mathcal{E}$.

так как, например, при $q > 0$

$$\int_0^q \delta(y)\,dy = \int_0^1 + \int_1^2 + \ldots + \int_{q-1}^q .$$

§ 4. Доказательство теоремы II (случай расходимости, $n = 1$). Пусть $\Delta_Q(\theta, \alpha)$ — число целых решений неравенства

$$\|q\theta - \alpha\| < \psi(q), \quad 0 < q \leqslant Q.$$

Мы применим лемму 2 к функции $\Delta_Q(\theta, \alpha)$ и обозначим

$$M_1(Q) = \int\int \Delta_Q(\theta, \alpha)\,d\theta\,d\alpha,$$

$$M_2(Q) = \left(\int\int \Delta_Q^2(\theta, \alpha)\,d\theta\,d\alpha\right)^{1/2}.$$

Здесь, если противное явно не оговорено, все интегралы вычисляются в единичном квадрате $0 \leqslant \theta < 1$, $0 \leqslant \alpha < 1$. Чтобы оценить $M_1(Q)$ и $M_2(Q)$, положим

$$\delta_q(x) = \begin{cases} 1, & \text{если } \|x\| < \psi(q), \\ 0 & \text{в противном случае,} \end{cases}$$

так что

$$\Delta_Q(\theta, \alpha) = \sum_{q \leqslant Q} \delta_q(q\theta - \alpha).$$

Сумма $\Psi(Q) = \sum_{q \leqslant Q} \psi(q) \to \infty$, так как по предположению соответствующий ряд расходится.

Лемма 4.

(i) $$\int\int \delta_q(q\theta - \alpha)\,d\theta\,d\alpha = 2\psi(q),$$

(ii) $$\int\int \delta_q(q\theta - \alpha)\,\delta_r(r\theta - \alpha)\,d\theta\,d\alpha = \begin{cases} 4\psi(q)\,\psi(r) & (q \neq r), \\ 2\psi(q) & (q = r). \end{cases}$$

Доказательство (i) тривиально в силу леммы 3 и очевидного равенства

$$\int_0^1 \delta_q(x)\,dx = 2\psi(q),$$

Доказательство (ii). Левая часть (ii) равняется

$$\int\int \delta_q(-\alpha')\,\delta_r(s\theta-\alpha')\,d\theta\,d\alpha',$$

где $s=r-q$, $\alpha'=\alpha-q\theta$. Можно считать, что α' изменяется в интервале $0\leqslant\alpha'<1$, так как δ_q, δ_r периодичны. Если $r\neq q$ (значит, и $s\neq 0$), то по лемме 3

$$\int\limits_0^1 \delta_r(s\theta-\alpha')\,d\theta=\int\limits_0^1 \delta_r(x)\,dx=2\psi(r),$$

и (ii) получается после повторного интегрирования. Если же $r=q$, то подинтегральная функция равняется $\delta_q^2(-\alpha')=\delta_q(-\alpha')$, так как $\delta_q(x)=0$ или 1. Опять (ii) получается немедленно.

Следствие. *Пусть $\varepsilon>0$ как угодно мало. Тогда для всех достаточно больших Q*

$$2\Psi(Q)=M_1(Q)\geqslant(1-\varepsilon)\,M_2(Q).$$

Доказательство. Во-первых,

$$M_1(Q)=\int\int\Delta_Q\,d\theta\,d\alpha=\sum_{q\leqslant Q}\int\int\delta_q(q\theta-\alpha)\,d\theta\,d\alpha=$$
$$=2\sum_{q\leqslant Q}\psi(q)=2\Psi(Q).$$

Во-вторых, для всех достаточно больших Q

$$M_2^2(Q)=\int\int\Delta_Q^2\,d\theta\,d\alpha=\sum_{q,\,r\leqslant Q}\int\int\delta_q(q\theta-\alpha)\,\delta_r(r\theta-\alpha)\,d\theta\,d\alpha=$$
$$=2\sum_{q\leqslant Q}\psi(q)+4\sum_{\substack{q,\,r\leqslant Q\\ q\neq r}}\psi(q)\,\psi(r)\leqslant 2\Psi(Q)+4\Psi^2(Q)\leqslant$$
$$\leqslant(1-\varepsilon)^{-2}4\Psi^2(Q),$$

так как $\Psi(Q)\to\infty$.

Доказательство теоремы II (окончание). По лемме 2 при $a=1-\varepsilon$ и $b=\varepsilon$ имеем

$$\Delta_Q(\theta,\,\alpha)\geqslant\varepsilon M_1(Q)=2\varepsilon\Psi(Q)$$

на некотором множестве, содержащемся в единичном квадрате, мера которого не менее $(1-2\varepsilon)^2 \geqslant 1-4\varepsilon$. Так как $\Delta_Q(\theta, \alpha)$ монотонно возрастает с ростом Q, то при $Q\to\infty$ $\Delta_Q(\theta, \alpha)\to\infty$ всюду в единичном квадрате, кроме, быть может, множества меры 4ε. Этим теорема доказана, так как ε произвольно мало.

§ 5. Некоторые дополнительные леммы.

Лемма 5. *Пусть множество $\mathscr{E}$, содержащееся в интервале $0\leqslant x<1$, имеет меру $|\mathscr{E}|>0$, и пусть $\varepsilon>0$ как угодно мало. Тогда существуют целые t, T, $0\leqslant t<T$, такие, что часть множества $\mathscr{E}$, содержащегося в интервале*

$$t/T\leqslant x<(t+1)/T, \tag{1}$$

имеет меру не менее $(1-\varepsilon)/T$.

Доказательство. По определению меры существует конечное или счетное множество непересекающихся интервалов $\mathscr{I}_r$, покрывающих множество $\mathscr{E}$, такое, что

$$\sum|\mathscr{I}_r|<\left(1-\frac{1}{2}\varepsilon\right)^{-1}|\mathscr{E}|.\quad \text{Но}\quad |\mathscr{E}|=\sum|\mathscr{I}_r\cap\mathscr{E}|.$$

Значит, по меньшей мере для одного номера r

$$|\mathscr{I}_r\cap\mathscr{E}|>\left(1-\frac{1}{2}\varepsilon\right)|\mathscr{I}_r|. \tag{2}$$

Теперь мы можем выбрать интервал $\mathscr{K}$: $x_0\leqslant x<x_1$ с рациональными концами x_0, x_1, содержащий интервал $\mathscr{I}_r$, и такой, что

$$|\mathscr{K}|<\left(1-\frac{1}{2}\varepsilon\right)^{-1}|\mathscr{I}_r|. \tag{3}$$

Тогда по (2) и (3)

$$|\mathscr{K}\cap\mathscr{E}|\geqslant|\mathscr{I}_r\cap\mathscr{E}|>\left(1-\frac{1}{2}\varepsilon\right)^2|\mathscr{K}|>(1-\varepsilon)|\mathscr{K}|.$$

Пусть теперь T — целое, такое, что $Tx_0=t_0$, $Tx_1=t_1$ — целые. Обозначим интервал (1) через $\mathscr{L}_t$. Ясно, что

$$\sum_{t_0\leqslant t<t_1}|\mathscr{L}_t\cap\mathscr{E}|=|\mathscr{K}\cap\mathscr{E}|>(1-\varepsilon)|\mathscr{K}|=$$
$$=(1-\varepsilon)(t_1-t_0)/T.$$

Поэтому по меньшей мере для одного числа t $|\mathscr{L}_t \cap \mathscr{E}| > (1-\varepsilon)/T$, что и требовалось доказать.

Следствие. *Почти все числа* θ_1 *имеют вид*

$$\theta_1 \equiv T\theta \pmod 1, \tag{4}$$

где T — *целое положительное число*, $\theta \in \mathscr{E}$.

Доказательство. Пусть $\mathscr{E}_1$ — множество чисел θ_1, содержащихся в интервале $0 \leqslant \theta < 1$ и имеющих вид (4); пусть $\varepsilon > 0$ как угодно мало. Если t, T — целые, указанные в лемме, то множество точек

$$\theta_1 = T\theta - t, \quad t/T \leqslant \theta < (t+1)/T, \quad \theta \in \mathscr{E}$$

принадлежит $\mathscr{E}_1$ и имеет меру $> 1-\varepsilon$. Следовательно, $|\mathscr{E}_1| > 1-\varepsilon$, что и требовалось доказать, так как ε произвольно мало.

Лемма 6. *Пусть* $\varphi(q)$[1] — *число целых* p *в интервале* $0 < p < q$, *взаимно простых с* q. *Тогда найдется постоянная* $C_1 > 0$, *такая, что для всех* $Q > 1$

$$\sum_{q \leqslant Q} q^{-1}\varphi(q) \geqslant C_1 Q.$$

Замечание. Грубо говоря, это означает, что $q^{-1}\varphi(q)$ больше C_1 „в среднем".

Доказательство. Хорошо известно (например, Харди и Райт (1938)), что

$$Q^{-2}\Phi(Q) \to 3/\pi^2, \quad \Phi(Q) = \sum_{q \leqslant Q} \varphi(q).$$

Следовательно, существует постоянная $C_1 > 0$, такая, что $Q^{-2}\Phi(Q) \geqslant C_1$ для всех $Q > 1$, так как $\Phi(Q) > 0$ при $Q > 1$. Тогда, пользуясь „частичным суммированием",

$$\sum_{q \leqslant Q} q^{-1}\varphi(q) = \sum_{q \leqslant Q} q^{-1}(\Phi(q) - \Phi(q-1)) =$$
$$= \sum_{q < Q} \Phi(q)(q^{-1} - (q+1)^{-1}) + Q^{-1}\Phi(Q) \geqslant$$
$$\geqslant Q^{-1}\Phi(Q) \geqslant C_1 Q,$$

что и требовалось доказать.

---

[1]) Функция Эйлера. — *Прим. перев.*

[Или, иначе, $q^{-1}\varphi(q)=\sum d^{-1}\mu(d)$, где суммирование проводится по всем делителям $d>0$ числа q, а $\mu(d)$ — функция Мёбиуса. Следовательно,

$$Q^{-1}\sum_{q\leqslant Q} q^{-1}\varphi(q)=\sum \mu(d)\,[d^{-1}Q]/dQ,$$

где d пробегает теперь все целые числа. Так как ряд $\sum d^{-2}$ сходится, правая часть равномерно стремится к $\sum d^{-2}\mu(d)=6\pi^{-2}$ при $Q\to\infty$.]

Лемма 7. *Пусть $\omega(q)$ — положительная монотонно убывающая функция. Тогда*

$$\sum_{q\leqslant Q} q^{-1}\varphi(q)\,\omega(q)\geqslant C_1\sum_{1<q\leqslant Q}\omega(q).$$

Доказательство. Обозначим $\chi(Q)=\sum_{q\leqslant Q} q^{-1}\varphi(q)$. Тогда, как и в предыдущей лемме,

$$\sum_{q\leqslant Q} q^{-1}\varphi(q)\,\omega(q)=\sum_{q\leqslant Q}\omega(q)\,(\chi(q)-\chi(q-1))=$$

$$=\sum_{q<Q}\chi(q)\,(\omega(q)-\omega(q+1))+\chi(Q)\,\omega(Q)\geqslant$$

$$\geqslant\sum_{1<q<Q} C_1 q\,(\omega(q)-\omega(q+1))+C_1Q\,\omega(Q)=$$

$$=C_1\omega(2)+C_1\sum_{1<q\leqslant Q}\omega(q).$$

Лемма 8. *Предположим, что функция $f(x)\geqslant 0$ возрастает при $x\leqslant 0$ и убывает при $x\geqslant 0$. Тогда*

$$\sum_{\substack{q\neq 0\\ -\infty<q<\infty}} f(q)\leqslant\int_{-\infty}^{\infty} f(x)\,dx,$$

если интеграл справа существует.

Доказательство очевидно.

§ 6. Доказательство теоремы I (случай расходимости, $n=1$). Так как ряд $\sum\psi(q)$ расходится, то можно найти функцию $\tau(q)$, $0<\tau(q)<1$, монотонно стремящуюся к нулю настолько медленно, что[1])

$$\Omega(Q) = \sum_{q \leqslant Q} \omega(q) \to \infty,$$

где $\omega(q) = \tau(q)\psi(q)$. Тогда $0 < \omega(q) \leqslant 1/2$, так как $0 < \psi(q) \leqslant 1/2$, и $\omega(q) \to 0$ монотонно в силу монотонности $\psi(q)$. Сначала мы будем оперировать с функцией $\omega(q)$ вместо $\psi(q)$.

Пусть

$$\beta_q(\theta) = \begin{cases} 1, & \text{если } |\theta| < q^{-1}\omega(q), \\ 0 & \text{в остальных случаях,} \end{cases}$$

где q — положительное целое, а θ — действительное число. Положим

$$\gamma_q(\theta) = \sum_p{}' \beta_q\left(\theta - \frac{p}{q}\right),$$

где до конца этой главы под $\sum\limits_p{}'$ понимаем сумму по всем p, удовлетворяющим условиям

$$0 < p < q; \quad (p, q) = 1. \tag{1}$$

Тогда $\gamma_q(\theta)$ — число решений неравенства $|q\theta - p| < \omega(q)$, где p подчиняется условиям (1). Значит,

$$\gamma_q(\theta) = 0 \text{ или } 1, \tag{2}$$

так как $\omega(q) \leqslant 1/2$. Мы будем применять одномерный аналог леммы 2 к $\mathbf{\Gamma}_Q(\theta) = \sum\limits_{q \leqslant Q} \gamma_q(\theta)$. Введем обозначения:

$$M_1(Q) = \int_0^1 \mathbf{\Gamma}_Q(\theta)\, d\theta, \quad M_2^2(Q) = \int_0^1 \mathbf{\Gamma}_Q^2(\theta)\, d\theta. \tag{3}$$

Лемма 9. *Существует абсолютная постоянная $C_2 > 0$, такая, что для достаточно больших Q*

$$M_1(Q) \geqslant C_2 \Omega(Q).$$

---

[1]) Так как существуют числа $1 = q_1 < q_2 < q_3 < \ldots$, такие, что $\sum\limits_{q_j \leqslant q < q_{j+1}} \psi(q) > 1$. Положим $\tau(q) = j^{-1}$, если $q_j \leqslant q < q_{j+1}$.

Доказательство.

$$\int_0^1 \gamma_q(\theta)\,d\theta = \int_0^1 \sum_p{}' \beta_q\left(\theta - \frac{p}{q}\right)d\theta =$$

$$= \varphi(q) \int_{-\infty}^{\infty} \beta_q(\theta)\,d\theta = 2q^{-1}\varphi(q)\,\omega(q). \quad (3')$$

Следовательно, по лемме 7

$$M_1(Q) = 2\sum_{q \leqslant Q} q^{-1}\varphi(q)\,\omega(q) \geqslant 2C_1(\Omega(Q) - \omega(1)) \geqslant C_2\Omega(Q)$$

для любого $C_2 < 2C_1$ при достаточно большом Q, так как $\Omega(Q) \to \infty$.

Лемма 10.

$$\int_0^1 \gamma_q(\theta)\,\gamma_r(\theta)\,d\theta \leqslant 4\omega(q)\,\omega(r) \quad (q \neq r).$$

Доказательство. Обозначим

$$\lambda_{qr}(x) = \int_{-\infty}^{\infty} \beta_q(\theta)\,\beta_r(\theta - x)\,d\theta. \quad (4)$$

Очевидно,

$$\int_{-\infty}^{\infty} \lambda_{qr}(x)\,dx = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \beta_q(\theta)\,\beta_r(\theta - x)\,d\theta\,dx =$$

$$= \left(\int_{-\infty}^{\infty} \beta_q(\theta)\,d\theta\right)\left(\int_{-\infty}^{\infty} \beta_r(y)\,dy\right) = (2q^{-1}\omega(q))(2r^{-1}\omega(r)), \quad (5)$$

полагая $y = \theta - x$. Далее, подинтегральная функция в (4) равняется 1, если одновременно $|\theta| < q^{-1}\omega(q)$, $|\theta - x| < r^{-1}\omega(r)$, и равняется 0 в противном случае. Следовательно[1]), $\lambda_{qr}(x)$ убывает при $x \geqslant 0$ и возрастает при $x \leqslant 0$. Но

---

[1]) Легко, конечно, получить оценку для $\lambda_{qr}(x)$ в явном виде,

теперь, если $\sum\limits_{s}'$ подчиняется условиям (1) и (s, r) берется вместо (p, q), получаем

$$\int\limits_0^1 \gamma_q(\theta)\,\gamma_r(\theta)\,d\theta = \sum_p{}' \sum_s{}' \int\limits_0^1 \beta_q\left(\theta - \frac{p}{q}\right) \beta_r\left(\theta - \frac{s}{r}\right) d\theta \leqslant$$

$$\leqslant \sum_{\substack{0 < p < q \\ 0 < s < r \\ p/q \neq s/r}} \lambda_{qr}\left(\frac{s}{r} - \frac{p}{q}\right), \tag{6}$$

заменяя $\theta - p/q$ на θ, и так как $p/q \neq s/r$ при p взаимно простом с q и s взаимно простом с r, $q \neq r$. Здесь

$$s/r - p/q = (qs - pr)/qr = ck/qr, \quad c = \text{н. о. д. } (q, r),$$

где $k \neq 0$ — целое. Далее, каждое k может встречаться не более c раз, так как если $q = cq_1$, $r = cr_1$, то $q_1 s - r_1 p = k$, что определяет p по $\operatorname{mod} q_1$. Значит, (6) будет

$$\leqslant c \sum_{k = \pm 1, \pm 2, \ldots} \lambda_{qr}(ck/qr) \leqslant$$

$$\leqslant c \int\limits_{-\infty}^{\infty} \lambda_{qr}(cx/qr)\,dx = 4\omega(q)\,\omega(r)$$

по (5) и по лемме 8.

Лемма 11. *При достаточно большом Q*

$$M_2^2(Q) \leqslant 5\Omega^2(Q).$$

Доказательство.

$$M_2^2(Q) = \int\limits_0^1 \left(\sum_{q \leqslant Q} \gamma_q(\theta)\right)^2 d\theta =$$

$$= \sum_{q \leqslant Q} \int\limits_0^1 \gamma_q^2(\theta)\,d\theta + \sum_{\substack{q,\, r \leqslant Q \\ q \neq r}} \int\limits_0^1 \gamma_q(\theta)\,\gamma_r(\theta)\,d\theta. \tag{7}$$

Но по (2) и (3′) первая сумма равняется

$$\sum \int_0^1 \gamma_q(\theta)\, d\theta = 2\sum q^{-1}\varphi(q)\,\omega(q) \leqslant 2\sum \omega(q) = 2\Omega(Q).$$

Вторая сумма по лемме 10 будет

$$\leqslant 4 \sum_{q,\, r \leqslant Q} \omega(q)\,\omega(r) = 4\Omega^2(Q).$$

Следовательно, при достаточно большом Q

$$M_2^2(Q) \leqslant 2\Omega(Q) + 4\Omega^2(Q) \leqslant 5\Omega^2(Q),$$

так как $\Omega(Q) \to \infty$.

Лемма 12. *$\Gamma_Q(\theta) \to \infty$ на некотором множестве $\mathfrak{E}$, содержащемся в $0 \leqslant \theta < 1$, меры $|\mathfrak{E}| > 0$.*

Доказательство. По леммам 9, 11 мы видим, что для всех достаточно больших Q

$$M_1(\Omega) \geqslant C_3 M_2(Q),$$

где $C_3 > 0$ — некоторая постоянная. Следовательно,

$$\Gamma_Q(\theta) \geqslant \frac{1}{2} C_3 M_1(Q) \geqslant \frac{1}{2} C_3 C_2 \Omega(Q)$$

на множестве меры не менее $\left(\frac{1}{2} C_3\right)^2$ по леммам 2 и 9. Так как функция $\Gamma_Q(\theta)$ монотонна относительно Q и $\Omega(Q) \to \infty$, то справедливость этой леммы имеет место при $|\mathfrak{E}| \geqslant \left(\frac{1}{2} C_3\right)^2$.

Доказательство теоремы 1 (окончание). $\Gamma_Q(\theta)$ есть число решений неравенства $|q\theta - p| < \omega(q)$ при $0 < q \leqslant Q$ и p, подчиненным условиям (1). Значит, лемма 12 показывает, что неравенство

$$\|q\theta\| < \omega(q) \tag{8}$$

имеет бесконечно много целых решений q на множестве $\mathfrak{E}$, содержащемся в $0 \leqslant \theta < 1$ с $|\mathfrak{E}| > 0$. Пусть θ_1 — любое число, такое, что

$$\theta_1 \equiv T\theta \pmod 1, \quad \theta \in \mathfrak{E} \tag{9}$$

при некотором целом $T > 0$. Из (8) следует, что при достаточно большом q

$$\|q\theta_1\| = \|Tq\theta\| < T\omega(q) = T\tau(q)\psi(q) < \psi(q),$$

так как $\tau(q) \to 0$. Следовательно, неравенство $\|q\theta_1\| < \psi(q)$ имеет бесконечно много решений. Но, согласно следствию из леммы 5, почти каждое число имеет вид θ_1 в (9).

§ 7. Случай $n \geqslant 2$. Изменения в доказательстве теоремы II и теоремы I в случае сходимости соответствующего ряда очевидны. Поэтому остается рассмотреть теорему I в случае, когда ряд $\sum \psi^n(q)$ расходится. Выберем монотонно убывающую функцию $\tau(q)$ так, чтобы и на этот раз ряд $\sum \omega^n(q)$, где $\omega(q) = \tau(q)\psi(q)$, расходился. Определим $\beta_q(\theta)$, $\gamma_q(\theta)$, как и ранее, а $M_1(\theta)$, $M_2(\theta)$ определим через

$$\Gamma_Q(\theta_1, \ldots, \theta_n) = \sum_{q \leqslant Q} \gamma_q(\theta_1) \ldots \gamma_q(\theta_n)$$

вместо $\Gamma_Q(\theta)$. Единственное сколько-нибудь глубокое изменение, требующееся в доказательстве, имеется в аналоге леммы 9, так как

$$M_1(Q) = \sum_{q \leqslant Q} q^{-n}\varphi^n(q)\,\omega^n(q).$$

Но по лемме 6 и по хорошо известному [1]) неравенству

$$\Big(Q^{-1}\sum_{q \leqslant Q} x_q^r\Big)^{1/r} \leqslant \Big(Q^{-1}\sum_{q \leqslant Q} x_q^s\Big)^{1/s},$$

справедливому для всех r, s с $0 < r \leqslant s$ и для всех положительных x_q, имеем

$$Q^{-1}\sum_{q \leqslant Q} q^{-n}\varphi^n(q) \geqslant \Big(Q^{-1}\sum_{q \leqslant Q} q^{-1}\varphi(q)\Big)^n \geqslant C_1^n$$

для всех $Q > 1$.

---

[1]) См., например, Харди, Литтльвуд, Полиа (1934), теорема 16. Это неравенство является, конечно, непосредственным следствием неравенства Гёльдера.

ЗАМЕЧАНИЯ

§ 1. Общее свойство результатов этого типа состоит в том, что нет промежуточного понятия между понятиями „почти все“ и „почти нет“. Теорема I перестает быть справедливой, если не считать $\psi(q)$ монотонной. Рассмотрение этого вопроса см. у Касселса (1950 a).

§ 5. Лемма 5 есть, конечно, следствие того, что измеримое множество имеет плотность 1 почти во всех своих точках.

Конечно, „метрический“ подход может быть осуществлен по отношению к большинству проблем. Так, отклонение D_Q по $\operatorname{mod} 1$ (в смысле гл. IV) последовательности $q\theta$ равняется $O\left(Q^{-1}\log^{1+\varepsilon} Q\right)$ при любом $\varepsilon > 0$ и почти для всех θ [Хинчин (1923)]. Много работ посвящено метрической теории равномерного распределения последовательностей вида $f(q, \theta)$ (например, $f = q^r\theta$, r фиксировано), но она находится в неудовлетворительном состоянии [например, Касселс (1950 b, c)]. Много известно о поведении неполных частных a_n числа θ для почти всех θ [Коксма (1936), гл. III, § 29; Хинчин (1935)].

Вместо того чтобы рассматривать не зависимые друг от друга $\theta_1, \ldots, \theta_n$, мы можем рассмотреть степени $\theta_j = \theta^j$ $(1 \leqslant j \leqslant n)$. Малер высказал интересное предположение о том, что $\max \|q\theta^j\| \leqslant q^{-(1/n)-\varepsilon}$ имеет только конечное число целых решений q при любом $\varepsilon > 0$ и для почти всех θ. Так как множество точек $(\theta, \ldots, \theta^n)$ имеет n-мерную меру 0, теорема I здесь неприменима. Последующие результаты см. у Касселса (1951) и Левека (1953).

Снова, если ряды $\sum \psi_j(q)$ $(j = 1,2)$ оба сходятся, множества $\mathfrak{E}_j$ точек θ, для которых $\|q\theta\| < \psi_j(q)$ $(j = 1,2)$ соответственно имеют бесконечно много решений меры 0, могут, однако, иметь совершенно разные „дробные измерения“ (см. Коксма (1936), гл. V, § 12).

Глава VIII

ЧИСЛА ПИЗО — ВИДЖАЯРАГХАВАНА

§ 1. Введение. В этой главе предполагается, что читатель имеет элементарные знания по алгебраической теории чисел.

Целое алгебраическое число $\alpha > 1$ называется *числом Пизо — Виджаярагхавана* (PV-*число*), если все его сопряженные, отличные от самого α, лежат внутри круга $|z| < 1$. В частности, если $\alpha > 1$ — целое рациональное, то у него нет никаких других сопряженных, и поэтому оно есть PV-число. Пусть α есть PV-число степени $r \geqslant 1$ с сопряженными[1] $\alpha = \alpha_1, \ldots, \alpha_r$, так что

$$\alpha = \alpha_1 > 1, \quad |\alpha_j| < 1 \quad (j \neq 1).$$

След

$$T(\alpha^n) = \alpha_1^n + \ldots + \alpha_r^n = A_n$$

является целым рациональным числом при всех целых $n \geqslant 0$, и поэтому

$$\|\alpha^n\| \leqslant |\alpha^n - A_n| \leqslant |\alpha_2|^n + \ldots + |\alpha_r|^n \to 0 \quad (n \to \infty).$$

Мы покажем, что PV-числа характеризуются этим свойством.

Более общо, пусть

$$\alpha^r + a_{r-1}\alpha^{r-1} + \ldots + a_0 = 0, \tag{1}$$

где $a_0, \ldots, a_{r-1}$ — целые рациональные числа, является неприводимым уравнением для PV-числа α, и пусть λ — такое число из поля числа α, что все следы

$$T(\lambda\alpha^N), \quad T(\lambda\alpha^{N+1}), \ \ldots, \ T(\lambda\alpha^{N+r-1})$$

---

[1]) Конечно, α_j — не обязательно действительное число при $j \neq 1$.

являются целыми числами при некотором целом $N \geqslant 0$. Для любого целого $n \geqslant N + r$ имеем по (1)

$$0 = T(\lambda\alpha^{n-r}(\alpha^r + a_{r-1}\alpha^{r-1} + \ldots + a_0)) = \\ = T(\lambda\alpha^n) + a_{r-1}T(\lambda\alpha^{n-1}) + \ldots + a_0 T(\lambda\alpha^{n-r})$$

и, значит, по индукции

$$T(\lambda\alpha^n) \text{ — целое при всех } n \geqslant N.$$

Следовательно, как и раньше,

$$\|\lambda\alpha^n\| \leqslant |\lambda_2\alpha_2^n| + \ldots + |\lambda_r\alpha_r^n| \quad (n \geqslant N)$$

и

$$\|\lambda\alpha^n\| \to 0 \quad (n \to \infty), \tag{2}$$

где $\lambda_2, \ldots, \lambda_r$ — сопряженные числа с $\lambda = \lambda_1$. Докажем следующее обратное утверждение.

Теорема I (Пизо, Виджаяраргхаван). *Пусть $\alpha > 1$ — алгебраическое число, $\lambda \neq 0$ — действительное и*

$$\|\lambda\alpha^n\| \to 0 \quad (n \to \infty). \tag{3}$$

Тогда α — PV-число, причем $\lambda = \alpha^{-N}\mu$, где $N \geqslant 0$ — некоторое целое, μ — некоторое число из поля числа α, такое, что $T(\alpha^j\mu)$ — целое $(0 \leqslant j \leqslant r-1)$, r — степень числа α.

Теорема II (Пизо). *Пусть $\alpha > 1$, $\lambda \neq 0$ — действительные числа и*

$$\sum_{0 \leqslant n < \infty} \|\lambda\alpha^n\|^2 < \infty. \tag{4}$$

Тогда α — алгебраическое число и, следовательно, справедливо утверждение теоремы I.

Конечно, (4) значительно сильнее, чем (3); из (2) следует обратное утверждение, т. е. (3) и (4) имеют место, если α есть PV-число, а λ—число, определенное в теореме I. Останется ли теорема II справедливой, если заменить условие (4) условием (3), не известно. Из теоремы II мы получим следующую замечательную теорему.

Теорема III (Салем). *Множество всех* PV-*чисел замкнуто* [1]).

§ 2. Доказательство теоремы I. В этом параграфе под α понимается алгебраическое число степени r с сопряженными $\alpha=\alpha_1, \alpha_2, \ldots, \alpha_r$, удовлетворяющими неприводимому уравнению

$$f(\alpha)=0, \quad f(x)=a_r x^r + \ldots + a_0, \tag{1}$$

где $a_r, \ldots, a_0$ — целые.

Лемма 1. *Система r уравнений*

$$y_j = x_1\alpha_1^j + \ldots + x_r\alpha_r^j \qquad (0 \leqslant j < r) \tag{2}$$

имеет единственное решение

$$\delta_j x_j = \sum_{0 \leqslant k < r} \beta_{jk} y_k \quad (1 \leqslant j \leqslant r), \tag{3}$$

где

$$\delta_j = \sum_{1 \leqslant l \leqslant r} l a_l \alpha_j^{l-1} \neq 0, \quad \beta_{jk} = \sum_{k < l \leqslant r} a_l \alpha_j^{l-k-1}. \tag{3'}$$

Замечание. Точный вид чисел δ_j, β_{jk} не играет роли. Для нас достаточно того, что они являются полиномами относительно α_j с целыми рациональными коэффициентами и что $\delta_j \neq 0$.

Доказательство. Так как числа α_j различны, то единственное решение $x_1, \ldots, x_r$ существует. Полином

$$f_j(z) = a_r \prod_{k \neq j} (z-\alpha_k) \tag{4}$$

определяется равенством

$$f_j(z) = \frac{f(z)-f(\alpha_j)}{z-\alpha_j} = \sum_{0 \leqslant l \leqslant r} a_l \frac{z^l-\alpha_j^l}{z-\alpha_j} =$$

$$= \sum_{1 \leqslant l \leqslant r} a_l\left(z^{l-1}+\alpha_j z^{l-2}+\ldots+\alpha_j^{l-1}\right) = \sum_{0 \leqslant k < r} \beta_{jk} z^k.$$

---

[1]) То есть если все $\alpha^{(n)}$ $(n=1, 2, \ldots)$ являются PV-числами и $\alpha=\lim \alpha^{(n)}$, то α — также PV-число.

Следовательно, по (2), (4) имеем

$$\sum_k \beta_{jk} y_k = f_j(\alpha_1)\, x_1 + \ldots + f_j(\alpha_r)\, x_r = \delta_j x_j,$$

где

$$\delta_j = f_j(\alpha_j) = a_r \prod_{k \neq j} (\alpha_j - \alpha_k) \neq 0.$$

Лемма 2. *Предположим, что $A_1, A_2, \ldots$ — числа и что*

$$a_0 A_n + \ldots + a_r A_{n+r} = 0 \tag{5}$$

для всех $n \geqslant N$. Тогда существуют числа $\lambda_1, \ldots, \lambda_r$, такие, что для всех $n \geqslant N$

$$A_n = \lambda_1 \alpha_1^n + \ldots + \lambda_r \alpha_r^n. \tag{6}$$

Доказательство. По лемме 1 существуют числа $\lambda_1, \ldots, \lambda_r$, такие, что (6) справедливо для $N \leqslant n < N + r$. Но правая часть равенства (6) удовлетворяет, очевидно, (5), а (5) однозначно определяет $A_{N+r}, A_{N+r+1}, \ldots$, если известны $A_N, \ldots, A_{N+r-1}$.

Лемма 3. *Предположим, что существует некоторое число $\mu \neq 0$ в поле числа α, такое, что все μ, $\mu\alpha$, $\mu\alpha^2, \ldots$ равны полиномам с целыми рациональными коэффициентами степени $r-1$ относительно α. Тогда α — целое алгебраическое число.*

Доказательство. Используя теорию идеалов, легко получить противоречие из предположения, что некоторый простой идеал встречается относительно числа α в отрицательной степени. В доказательстве, данном ниже, понятие идеала не используется.

Пусть $\mathfrak{B}$ — множество всех чисел β, которые представляются в виде суммы конечного числа выражений вида $c\mu\alpha^n$ ($n > 0$, c — целые рациональные). По условию $\beta = b_0 + b_1\alpha + \ldots + b_{r-1}\alpha^{r-1}$, где $b_0, \ldots, b_{r-1}$ — целые. Очевидно, множество всех $(b_0, \ldots, b_{r-1})$ с $\beta \in \mathfrak{B}$ является модулем в смысле приложения А. Пусть $\beta^{(1)}, \ldots, \beta^{(s)}$ ($s \leqslant r$) соответствуют очевидным образом базису этого модуля, так что $\beta^{(j)} \in \mathfrak{B}$ ($1 \leqslant j \leqslant s$), и каждое $\beta \in \mathfrak{B}$ имеет вид

$$\beta = c_1 \beta^{(1)} + \ldots + c_s \beta^{(s)} \quad (c_j \text{ — целые рациональные}).$$

Очевидно, что $\alpha\beta \in \mathfrak{B}$, если $\beta \in \mathfrak{B}$. В частности,

$$\alpha\beta^{(j)} = \sum_t c_{jt}\beta^{(t)} \quad (t,\ j = 1,\ \ldots,\ s),$$

где c_{jt} — целые рациональные числа. Перенося члены $\alpha\beta^{(j)}$ в другую сторону и приводя подобные члены, мы получаем $\det(\alpha\delta_{jt} - c_{jt}) = 0$, где $\delta_{jt} = 1$ при $t = j$ и $\delta_{jt} = 0$ при $t \neq j$. Но этот определитель есть уравнение степени $s \leqslant r$ относительно α с целыми рациональными коэффициентами, причем старший коэффициент равен 1. Значит, $s = r$ и α — целое алгебраическое число.

Доказательство теоремы I. Запишем

$$\lambda\alpha^n = A_n + \varepsilon_n, \tag{7}$$

где A_n — целое и

$$|\varepsilon_n| = \|\lambda\alpha^n\| \leqslant \frac{1}{2}, \quad \varepsilon_n \to 0 \quad (n \to \infty). \tag{8}$$

Из (1), (7), (8) имеем

$$\begin{aligned} a_0A_n + a_1A_{n+1} + \ldots + a_rA_{n+r} &= \\ = \lambda\alpha^n(a_0 + a_1\alpha + \ldots + a_r\alpha^r) &- a_0\varepsilon_n - a_1\varepsilon_{n+1} - \ldots \\ \ldots - a_r\varepsilon_{n+r} &= -a_0\varepsilon_n - \ldots - a_r\varepsilon_{n+r} \to 0. \end{aligned} \tag{9}$$

Так как левая часть (9) является целым числом, то оно равно нулю при всех $n \geqslant$ некоторого N.

По лемме 2 для всех $n \geqslant N$ имеет место равенство (6), где λ_1 не обязательно равно λ. Пусть $m \geqslant N$. Решая (6) относительно $\lambda_1, \ \ldots, \ \lambda_n$ и полагая $n = m, \ \ldots, \ m + r - 1$, получаем по лемме 1

$$\delta_j\alpha_j^m\lambda_j = \sum_{0 \leqslant k < r} \beta_{jk}A_{m+k} \quad (1 \leqslant j \leqslant r). \tag{10}$$

Следовательно, λ_j находится в поле числа α_j, так как δ_j, β_{jk} принадлежит ему; в действительности числа λ_j — сопряженные, так как δ_j, β_{jk} — сопряженные. Если какое-нибудь λ_j равнялось бы нулю, то и все они равнялись бы нулю и $A_n = 0$ при всех $n \geqslant N$ вопреки (7). Следовательно,

$$\lambda_j \neq 0 \qquad (1 \leqslant j \leqslant r). \tag{11}$$

Правая часть равенства (10) при $j = 1$ является полиномом относительно $\alpha = \alpha_1$ с целыми рациональными коэффициентами степени $r - 1$ по (3′), и $\delta_1\lambda_1\alpha_1^N = \mu \neq 0$. Следовательно, по лемме 3 α — целое алгебраическое.

По (6) и (7) имеем при всех $n \geqslant N$

$$\varepsilon_n = (\lambda - \lambda_1)\,\alpha_1^n - \lambda_2\alpha_2^n - \ldots - \lambda_r\alpha_r^n. \qquad (12)$$

Опять по лемме 1 при всех $m \geqslant N$ справедливо равенство

$$\delta_1 (\lambda - \lambda_1)\,\alpha_1^m = \sum_{0 \leqslant k < r} \beta_{1k}\varepsilon_{m+k},$$

отсюда

$$\delta_1 (\lambda - \lambda_1)\,\alpha_1^m \to 0$$

при $m \to \infty$, согласно (8). Значит, $\lambda = \lambda_1$, так как $\alpha_1 > 1$. Аналогично $\delta_j\lambda_j\alpha_j^m \to 0$ $(j > 1)$ по (12), (8). Таким образом, $|\alpha_j| < 1$ $(j > 1)$ по (11).

§ 3. Доказательство теоремы II. Будем говорить, что числа z_n $(0 \leqslant n < \infty)$ бесконечной последовательности связаны *рекуррентным соотношением*, если существуют постоянные $c_0, \ldots, c_{r-1}$, такие, что для всех достаточно больших n

$$z_{n+r} = c_{r-1}z_{n+r-1} + \ldots + c_0 z_n. \qquad (1)$$

Прежде всего мы покажем, что если все числа z_n — рациональные, то и $c_0, \ldots, c_{r-1}$ тоже можно без ограничения общности выбрать рациональными. По следствию из леммы 2 гл. III существуют числа $\mu_1 = 1$, $\mu_2, \ldots, \mu_l$, $l \leqslant r$, которые линейно независимы над полем рациональных чисел и через которые $1, c_0, \ldots, c_{r-1}$ линейно выражаются. Например,

$$c_j = c_j^* + \sum_{1 < k \leqslant l} d_{kj}\mu_k, \qquad (2)$$

где c_j^* и d_{kj} — рациональные. Если все $z_n, \ldots, z_{n+r}$ рациональные, то можно выразить c_j с помощью (2) и потом приравнять коэффициенты при $\mu_1 = 1$ с обеих сторон, т. е.

$$z_{n+r} = c_{z-1}^* z_{n+r-1} + \ldots + c_0^* z_n.$$

Это и есть нужный нам вид.

Теорема IV. *Пусть z_n $(0 \leqslant n < \infty)$ — последовательность действительных чисел и A_n $(0 \leqslant n < \infty)$ — последовательность целых чисел, причем*

$$\sum |z_n - A_n|^2 < \infty. \qquad (3)$$

Тогда если z_n связаны рекуррентным соотношением, то и A_n тоже связаны рекуррентным соотношением (но не обязательно тем же самым).

Вывод теоремы II. Сначала мы покажем, как теорема II следует из теоремы IV. Пусть λ, α удовлетворяют условию теоремы II. Определим целые A_n равенством $|A_n-\lambda\alpha^n|=\|\lambda\alpha^n\|$. Последовательность чисел $z_n=\lambda\alpha^n$ удовлетворяет рекуррентному соотношению $z_{n+1}=\alpha z_n$. По теореме IV и по условию (1.4) теоремы II, числа A_n при достаточно большом n удовлетворяют соотношению

$$A_{n+r}=c_{r-1}A_{n+r-1}+\ldots+c_0A_n, \tag{4}$$

где $c_{r-1}, \ldots, c_0$ можно считать рациональными. Положив в (4) $\lambda\alpha^m=A_m+\varepsilon_m\,(n\leqslant m\leqslant n+r)$ и разделив на $\lambda\alpha^n\neq 0$, получим

$$\alpha^r-c_{r-1}\alpha^{r-1}-\ldots-c_0=$$
$$=(\lambda\alpha^n)^{-1}(\varepsilon_{n+r}-c_{r-1}\varepsilon_{n+r-1}-\ldots-c_0\varepsilon_n)\to 0 \qquad (n\to\infty),$$

т. е. $\alpha^r-c_{r-1}\alpha^{r-1}-\ldots-c_0=0$. Значит, α — число алгебраическое, и, следовательно, справедлива теорема I.

Доказательство теоремы IV опирается на две общие леммы.

Лемма 4. *Для того чтобы члены бесконечной последовательности $z_0, z_1, \ldots$ удовлетворяли рекуррентному соотношению, необходимо и достаточно обращения в нуль определителей*

$$D_n=\det(z_{i+j}) \qquad (0\leqslant i,\ j\leqslant n)$$

для всех достаточно больших n.

Доказательство. Если такое рекуррентное соотношение существует, то при достаточно больших n строки определителя D_n связаны линейной зависимостью и поэтому $D_n=0$. Остается доказать, что если для всех достаточно больших n определитель $D_n=0$, то существует рекуррентное соотношение, которому удовлетворяют члены последовательности. Если $D_n=0$ для всех n, то

$$0=z_0=z_1=\ldots=z_n=\ldots.$$

В противном случае существует $r\geqslant 1$, такое, что

$$D_{r-1}\neq 0,\quad D_n=0 \tag{5}$$

для всех $n \geqslant r$. Так как $D_r = 0$, то существует линейная зависимость между строками соответствующей матрицы, например

$$c_r z_{n+r} + c_{r-1} z_{n+r-1} + \ldots + c_0 z_n = 0 \qquad (0 \leqslant n \leqslant r),$$

где $c_r, \ldots, c_0$ не равны нулю одновременно. Если $c_r = 0$, то мы имели бы зависимость между строками определителя D_{r-1}, т. е. $D_{r-1} = 0$, вопреки предположению. Поэтому можно считать, что $c_r = -1$. Тогда (1) имеет место для всех $0 \leqslant n \leqslant r$, и мы покажем, что это равенство справедливо для всех n. Положим

$$R_n = z_n - c_{r-1} z_{n-1} - \ldots - c_0 z_{n-r} \qquad (n \geqslant r).$$

Тогда $R_n = 0$ $(r \leqslant n \leqslant 2r)$. Пусть нам известно, что

$$R_n = 0 \qquad (r \leqslant n < N), \tag{6}$$

где $N > 2r$. Заменяя j-й столбец $(j > r)$ определителя D_{N-r} разностью [j-й столбец] $- c_{r-1}$ [$(j-1)$-й столбец] $- \ldots$ $\ldots - c_0$ [$(j-r)$-й столбец], мы заменим элемент z_{i+j} определителя D_{N-r}, стоящий в i-й строке и j-м столбце, числом R_{i+j} для $j \geqslant r$. Следовательно, если развернуть определитель D_{N-r} и использовать (6), получим $D_{N-r} = \pm D_{r-1} R_N^{N-2r+1}$. Наконец, по (5) $R_n = 0$ и по индукции $R_n = 0$ для всех $n \geqslant r$.

Лемма 5. *Пусть* $\sum \alpha_{ij} x_i x_j \geqslant 0$ $(\alpha_{ij} = \alpha_{ji})$ *для всех* $(x_1, \ldots, x_n)$. *Тогда*

$$0 \leqslant \det(\alpha_{ij}) \leqslant \prod \alpha_{ii}.$$

Доказательство. Производя последовательно дополнения до полного квадрата и изменяя в случае необходимости порядок точек $(x_1, \ldots, x_n)$, получаем

$$\sum \alpha_{ij} x_i x_j = \beta_1 (x_1 + \lambda_{12} x_2 + \ldots + \lambda_{1n} x_n)^2 + \\ + \beta_2 (x_2 + \lambda_{23} x_3 + \ldots + \lambda_{2n} x_n)^2 + \ldots + \beta_n x_n^2,$$

где λ_{ij} — действительные числа и $\beta_i \geqslant 0$ $(1 \leqslant i \leqslant n)$. Очевидно, что

$$\det(\alpha_{ij}) = \prod \beta_i \quad \text{и} \quad \alpha_{ii} = \beta_i + \sum_{k<i} \beta_k \lambda_{ki}^2 \geqslant \beta_i.$$

Следствие (Адамар). *Пусть* β_{ij} — *любые* n^2 *действительных чисел и*

$$M_i = \Big(\sum_j \beta_{ij}^2\Big)^{1/2}.$$

Тогда $|\det(\beta_{ij})| \leqslant M_1 M_2 \ldots M_n$.

Замечание. Это есть n-мерное обобщение того факта, что объем параллелепипеда не превосходит произведения ребер.

Доказательство. $\sum \alpha_{ij} x_i x_j = \sum_j \Big(\sum_i \beta_{ij} x_i\Big)^2 \geqslant 0$ для всех $(x_1, \ldots, x_n)$ и

$$\det(\alpha_{ij}) = (\det(\beta_{ij}))^2, \quad \alpha_{ii} = \sum_j \beta_{ij}^2 = M_i^2.$$

Доказательство теоремы IV. Пусть

$$\Delta_n = \det(A_{i+j}) \quad (0 \leqslant i,\ j \leqslant n), \tag{7}$$

и пусть z_n удовлетворяют равенству (1), например при $n \geqslant N - r$. Для $n \geqslant N$ запишем

$$\varepsilon_n = A_n - c_{r-1} A_{n-1} - \ldots - c_0 A_{n-r} =$$
$$= (A_n - z_n) - c_{r-1}(A_{n-1} - z_{n-1}) - \ldots - c_0 (A_{n-r} - z_{n-r}).$$

Тогда, согласно неравенству[1] Шварца,

$$\varepsilon_n^2 \leqslant d \sum_{n-r \leqslant m \leqslant n} (A_m - z_m)^2, \quad d = 1 + c_{r-1}^2 + \ldots + c_0^2,$$

и, значит, $\sum \varepsilon_n^2 < \infty$ по (3). Для $n \geqslant 2N$ запишем

$$\eta_n = \varepsilon_n - c_{r-1}\varepsilon_{n-1} - \ldots - c_0 \varepsilon_{n-r},$$

так что аналогично $\sum \eta_n^2 < \infty$. Оперируя со строками определителя (7), мы можем заменить число A_{i+j}, стоящее в i-й строке и j-м столбце, числом ε_{i+j} для всех $j \geqslant N$ и всех i. Оперируя аналогично столбцами, получаем

$$\Delta_n = \det(\delta_{ij}), \qquad \delta_{ij} = \begin{cases} A_{i+j}, & \text{если } i < N,\ j < N, \\ \eta_{i+j}, & \text{если } i \geqslant N,\ j \geqslant N, \\ \varepsilon_{i+j} & \text{в остальных случаях.} \end{cases}$$

---

[1]) См. примечание на стр. 90.

Для $i < N$

$$\sum_j \delta_{ij}^2 \leqslant \sum_{0 \leqslant j \leqslant 2N-2} A_j^2 + \sum_{j \geqslant N} \varepsilon_j^2 = \mu_i^2$$

и для $i \geqslant N$

$$\sum_j \delta_{ij}^2 \leqslant \sum_{j \geqslant i} \left(\varepsilon_j^2 + \eta_j^2\right) = \mu_i^2.$$

Тогда μ_i не зависит от n и $\mu_i \to 0$ $(i \to \infty)$, так как ряды $\sum \eta_j^2$, $\sum \varepsilon_j^2$ сходятся. Следовательно, по следствию из леммы 5

$$|\Delta_n| \leqslant \mu_1 \ldots \mu_n \to 0 \quad (n \to \infty).$$

Но по (7) Δ_n — целое число, значит, $\Delta_n = 0$ для всех достаточно больших n. Таким образом, применима лемма 4 и A_n удовлетворяют рекуррентному соотношению.

§ 4. Доказательство теоремы III. Доказательство этой теоремы опирается на тот факт, что для каждого PV-числа α существует $\lambda > 0$, такое, что λ и $\sum \|\lambda\alpha^n\|^2$ не слишком велики. В этом параграфе мы считаем $i = \sqrt{-1}$ и используем знак $(^-)$ для обозначения комплексно сопряженного числа, так что $|z|^2 = z\bar{z}$.

Лемма 6. *Предположим, что* $\sum\limits_{n \geqslant 0} \beta_n$ — *абсолютно сходящийся ряд с действительными или комплексными членами. Тогда*

$$\int_0^{2\pi} \Big| \sum_{n \geqslant 0} \beta_n e^{in\theta} \Big|^2 d\theta = 2\pi \sum_{n \geqslant 0} |\beta_n|^2.$$

Доказательство очевидно, если почленно проинтегрировать, что законно в силу абсолютной сходимости ряда.

Лемма 7. *Пусть z, β — действительные или комплексные числа, причем $|z| \leqslant 1$. Тогда*

$$|z - \bar{\beta}| \leqslant |1 - \beta z|, \text{ если } |\beta| < 1,$$
$$|z - \bar{\beta}| \geqslant |1 - \beta z|, \text{ если } |\beta| > 1.$$

В обоих случаях равенство имеет место тогда и только тогда, когда $|z| = 1$.

Доказательство. Утверждение леммы следует сразу из простого тождества

$$|1-\beta z|^2-|z-\overline{\beta}|^2=(1-|\beta|^2)(1-|z|^2).$$

Лемма 8 (Фату). *Предположим, что* $\varphi(m, n)\geqslant 0$ *при* $n\geqslant 0$, $m\geqslant 0$ *и что* $\varphi^*(n)=\lim\limits_{m\to\infty}\varphi(m, n)$ *существует* ($n\geqslant 0$). *Тогда*

$$\sum_{n\geqslant 0}\varphi^*(n)\leqslant\liminf_{m\to\infty}\sum_{n\geqslant 0}\varphi(m, n).$$

Доказательство. Для любого $N\geqslant 0$

$$\sum_{n\leqslant N}\varphi^*(n)=\lim_{m\to\infty}\sum_{n\leqslant N}\varphi(m, n)\leqslant\liminf_{m\to\infty}\sum_{n<\infty}\varphi(m, n)$$

и

$$\sum_{n\geqslant 0}\varphi^*(n)=\lim_{N\to\infty}\sum_{n\leqslant N}\varphi^*(n).$$

Лемма 9. *Пусть* α — PV-*число. Тогда существует действительное* $\lambda\neq 0$, *такое, что*

$$|\lambda|<\alpha,\quad\sum_{n}\|\lambda\alpha^n\|^2<4\alpha^2/(\alpha-1)^2. \tag{1}$$

Доказательство. Пусть α вместе со своими сопряженными $\alpha=\alpha_1, \ldots, \alpha_r$ удовлетворяют неприводимому уравнению степени r

$$f(\alpha)=0,\ f(z)=z^r+a_{r-1}z^{r-1}+\ldots+a_0, \tag{2}$$

где $a_{r-1}, \ldots, a_0$ — целые.

Мы сначала избавимся от анормального случая:

$$r=2,\ a_0=\pm 1,\ \text{поэтому}\ \alpha_2=\pm\alpha^{-1}. \tag{3}$$

В случае (3) положим

$$\lambda=1<\alpha.$$

Тогда

$$\|\lambda\alpha^n\|\leqslant|\alpha^n-T(\alpha^n)|=|\alpha_2^n|=\alpha^{-n},$$

и, значит,

$$\sum\|\lambda\alpha^n\|^2\leqslant\sum_{n\geqslant 0}\alpha^{-2n}=\frac{\alpha^2}{\alpha^2-1}<\frac{4\alpha^2}{(\alpha-1)^2}.$$

Теперь мы можем случай (3) исключить. Запишем

$$g(z)=a_0z^r+a_1z^{r-1}+\ldots+1=z^rf(z^{-1}) \tag{4}$$

и положим

$$h(z)=\frac{f(z)}{g(z)}=\sum_{n\geqslant 0}A_nz^n, \tag{5}$$

где ряд справа сходится при достаточно малых z. Согласно (2) и (4), числа A_n — целые рациональные. Так как полином $f(z)$ неприводим, то или $f(z)$ и $g(z)$ не имеют общих корней, или $g(z)=a_0f(z)$. Если $r>2$, то вторая альтернатива невозможна, так как вне $|z|<1$ лежит только один из корней α_j полинома $f(z)$ и $r-1$ корней α_j^{-1} полинома $g(z)$. Если же $r=2$, то вторая альтернатива приводит к исключенному уже случаю (3).

Таким образом, мы можем считать, что

$$\alpha_j\alpha_l\neq 1 \quad (1\leqslant j,\ l\leqslant r). \tag{6}$$

Разлагая полиномы $f(z)$, $g(z)$ на линейные множители, получаем

$$h(z)=\prod_{1\leqslant j\leqslant r}\left(\frac{z-\bar{\alpha}_j}{1-\alpha_jz}\right), \tag{7}$$

так как комплексные корни встречаются сопряженными парами. Разложим $h(z)$ на простейшие дроби:

$$h(z)=\frac{1}{a_0}+\sum_{1\leqslant j\leqslant r}\frac{\lambda_j}{1-\alpha_jz},$$

где

$$\lambda_j=\lim_{z\to\alpha_j^{-1}}(1-\alpha_jz)\,h(z)=(\alpha_j^{-1}-\bar{\alpha}_j)\prod_{l\neq j}\left(\frac{\alpha_j^{-1}-\bar{\alpha}_l}{1-\alpha_j^{-1}\alpha_l}\right)\neq 0$$

по (6). В частности, $\lambda=\lambda_1$ — число действительное и

$$0<|\lambda|<|\alpha^{-1}-\alpha|<\alpha, \tag{8}$$

так как по лемме 7 при $z=\alpha^{-1}$, $\beta=\alpha_l$

$$|\alpha^{-1}-\bar{\alpha}_l|<|1-\alpha^{-1}\alpha_l| \quad (l\neq 1).$$

Степенной ряд

$$F(z)=\sum_{n\geqslant 0}(A_n-\lambda\alpha^n)z^n=h(z)-\frac{\lambda}{1-\alpha z}=$$

$$=\frac{1}{a_0}+\sum_{j>1}\frac{\lambda_j}{1-\alpha_j z}$$

абсолютно сходится при $z=1$, так как $|\alpha_j|<1 \quad (j\neq 1)$. Но по (7) и по лемме 7

$$|h(z)|=1,$$

если $|z|=1$, и по (8)

$$\left|\frac{\lambda}{1-\alpha z}\right|<\frac{|\lambda|}{\alpha-1}<\frac{\alpha}{\alpha-1},$$

если $|z|=1$. Следовательно,

$$|F(z)|<1+\frac{\alpha}{\alpha-1}<\frac{2\alpha}{\alpha-1},$$

если $|z|=1$. Наконец, по лемме 6

$$\sum_{n\geqslant 0}\|\lambda\alpha^n\|^2\leqslant\sum_{n\geqslant 0}|A_n-\lambda\alpha^n|^2=\frac{1}{2\pi}\int_0^{2\pi}|F(e^{i\theta})|^2 d\theta<\left(\frac{2\alpha}{\alpha-1}\right)^2.$$

Следствие. *Мы можем считать, следовательно, что* $1\leqslant\lambda<\alpha$.

Доказательство. Мы можем считать, что $\lambda>0$, так как $-\lambda$ удовлетворяет (1), если ему удовлетворяет λ. Согласно (1), существует целое $N\geqslant 0$, такое, что

$$\lambda'=\lambda\alpha^N<\alpha\leqslant\lambda\alpha^{N+1}.$$

Тогда $1\leqslant\lambda'<\alpha$ и

$$\sum_{n\geqslant 0}\|\lambda'\alpha^n\|^2=\sum_{n\geqslant N}\|\lambda\alpha^n\|^2\leqslant\sum_{n\geqslant 0}.$$

Доказательство теоремы III. Пусть $\alpha(m)$ $(m=1, 2, \ldots)$ — последовательность PV-чисел и $\beta=\lim\alpha(m)$. Нам надо показать, что β есть PV-число. Соответствующая последовательность чисел $\lambda(m)$, определенная следствием из леммы 9, ограничена. Поэтому можно считать, что и $\mu=\lim\lambda(m)$ существует, переходя в случае необходимости к подпоследовательности. Очевидно, что $1 \leqslant \mu \leqslant \beta$. В частности, $\mu \neq 0$. Если $\beta > 1$, то по леммам 8, 9 имеем

$$\sum_{n \geqslant 0} \|\mu\beta^n\|^2 \leqslant \liminf_{m \to \infty} \sum_{n \geqslant 0} \|\lambda(m)\alpha^n(m)\|^2 \leqslant$$
$$\leqslant \liminf_{m \to \infty} \frac{4\alpha^2(m)}{(\alpha(m)-1)^2} = \frac{4\beta^2}{(\beta-1)^2} < \infty$$

и по теореме II β есть PV-число.

Так как 1 не является PV-числом, то остается доказать, что $\beta \neq 1$. Если α есть PV-число, то по определению и α^k есть PV-число при любом целом $k > 0$. Пусть γ — любое число > 1, не являющееся PV-числом (например, $\gamma = {}^3/_2$). Тогда $\alpha(m) < \gamma$ для всех достаточно больших m, если $\beta = 1$. Для таких m мы можем выбрать целое $k(m) > 0$, такое, что

$$\delta(m) = (\alpha(m))^{k(m)} < \gamma \leqslant \delta(m)\,\alpha(m).$$

Числа $\delta(m)$ являются PV-числами, и $\gamma = \lim \delta(m)$. Это противоречит тому, что уже доказано. Значит, $\beta \neq 1$.

ЗАМЕЧАНИЯ

Так как множество PV-чисел замкнуто, то оно должно содержать наименьший элемент. Фактически наименьший элемент и наименьшая предельная точка известны. Последние сведения об этом, а также другие факты см. у Дюфренуа и Пизо (1954), а обобщения см. у Пизо (1946), Гельфонда (1941), Келли (1950) и Самета (1953).

Приложение А

БАЗИСЫ В НЕКОТОРЫХ МОДУЛЯХ

Назовем множество $\mathfrak{M}$ n-мерных векторов *модулем*, если из принадлежности $\mathbf{x}^{(1)}$ и $\mathbf{x}^{(2)}$ множеству $\mathfrak{M}$ следует, что $\mathbf{x}^{(1)} \pm \mathbf{x}^{(2)}$ также принадлежит $\mathfrak{M}$. В частности, (при $\mathbf{x}^{(1)} = \mathbf{x}^{(2)}$), вектор $\mathbf{0}$ принадлежит $\mathfrak{M}$. По индукции

$$\mathbf{y} = a_1\mathbf{x}^{(1)} + \ldots + a_m\mathbf{x}^{(m)} \tag{1}$$

принадлежит $\mathfrak{M}$, если только $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(m)}$ принадлежат $\mathfrak{M}$ и $a_1, \ldots, a_m$ — целые рациональные числа. Мы будем говорить, что $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(m)}$ — *базис* модуля, если, во-первых, каждый вектор модуля имеет вид (1) и, во-вторых, при $\mathbf{y} = \mathbf{0}$ уравнение (1) имеет единственное решение

$$a_1 = \ldots = a_m = 0$$

в целых числах $a_1, \ldots, a_m$. Тогда, очевидно, представление (1) всегда однозначно.

Мы будем иметь дело только с модулями, все векторы которых имеют целые координаты.

Лемма 1. *Если все векторы модуля $\mathfrak{M}$, содержащего хотя бы один вектор, отличный от нуля, имеют целые рациональные координаты, то $\mathfrak{M}$ имеет базис.*

Доказательство. Воспользуемся методом индукции. Предположим, что лемма справедлива для $(n-1)$-мерных векторов, и докажем ее справедливость для n-мерных векторов. Переставляя в случае необходимости соответствующим образом порядок координат, можно считать, что модуль содержит вектор

$$\mathbf{x}^{(1)} = (x_{11}, \ldots, x_{1n}), \quad x_{11} \neq 0.$$

Выберем $\mathbf{x}^{(1)}$ так, чтобы целое $|x_{11}| \neq 0$ было наименьшим. Если $\mathbf{y} = (y_1, \ldots, y_n)$ — какой-нибудь другой вектор модуля $\mathfrak{M}$, то существует целое a_1, такое, что $|y_1 - a_1 x_{11}| < |x_{11}|$. Тогда

$$\mathbf{y}' = \mathbf{y} - a_1 \mathbf{x}^{(1)} \in \mathfrak{M}.$$

Но абсолютная величина первой координаты вектора $\mathbf{y}'$ меньше, чем $|x_{11}|$. Таким образом, по определению $\mathbf{x}^{(1)}$ имеем $\mathbf{y}' = (0, y_2', \ldots, y_n')$ при некоторых целых $y_2', \ldots, y_n'$. Векторы $\mathbf{y}'$ такого вида образуют, очевидно, $(n-1)$-мерный модуль[1]) $\mathfrak{M}'$, и, следовательно, по индуктивному предположению $\mathfrak{M}'$ имеет базис, скажем, $\mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(m)}$ при некотором $m \geqslant 1$ (где $m = 1$ означает, что $\mathfrak{M}'$ состоит только из нуля). Тогда

$$\mathbf{y} = a_1 \mathbf{x}^{(1)} + \mathbf{y}' = a_1 \mathbf{x}^{(1)} + \ldots + a_m \mathbf{x}^{(m)}$$

при целых $a_1, \ldots, a_m$. С другой стороны, из равенства $\mathbf{0} = a_1 \mathbf{x}^{(1)} + \ldots + a_m \mathbf{x}^{(m)}$, сравнивая первые координаты, получаем, что $a_1 = 0$. Тогда и $a_2 = \ldots = a_m = 0$, так как $\mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(m)}$ — базис модуля $\mathfrak{M}'$. Следовательно, $\mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(m)}$ — базис. Тем самым лемма доказана, так как при $n = 1$ она тривиальна.

Следствие. *После надлежащей перестановки координат базис может быть представлен в виде*

$$\mathbf{x}^{(j)} = (0, \ldots, 0, x_{jj}, \ldots, x_{jn}), \qquad x_{jj} \neq 0 \qquad (1 \leqslant j \leqslant m),$$

(т. е. $x_{jk} = 0$, если $k < j$). Если $m = n$, то перестановка не нужна.

Доказательство очевидно.

Модуль $\mathfrak{M}_0$ всех целых векторов имеет базис

$$\mathbf{e}^{(j)} = (0, \ldots, 0, 1, 0, \ldots, 0),$$

где 1 стоит на j-м месте $(1 \leqslant j \leqslant n)$. Но существуют и другие базисы, как показывает следующая

Лемма 2. *Для того чтобы множество векторов*

$$\mathbf{x}^{(j)} = (x_{j1}, \ldots, x_{jn}) \quad (1 \leqslant j \leqslant n) \tag{2}$$

[1]) Точнее, векторы $(y_2', \ldots, y_n')$.

с целыми x_{jk} *было базисом модуля* $\mathfrak{M}_0$ *всех целых векторов, необходимо и достаточно, чтобы*

$$\det(x_{jk}) = \pm 1. \tag{3}$$

Доказательство. Если векторы $x^{(j)}$ образуют базис, то существуют целые рациональные d_{kj}, такие, что

$$\mathbf{e}^{(j)} = \sum_k d_{jk}\mathbf{x}^{(k)},$$

т. е.

$$\sum_k d_{jk}x_{kl} = \begin{cases} 1, & \text{если} \quad j = l, \\ 0, & \text{если} \quad j \neq l. \end{cases}$$

Следовательно, $\det(d_{jk})\det(x_{kl}) = 1$. Так как значения определителей есть целое число, то отсюда следует справедливость (3). Обратно, если (3) имеет место и $\mathbf{y}$ имеет целые координаты, то решение уравнения $\mathbf{y} = \sum\limits_j a_j\mathbf{x}^{(j)}$ с помощью определителей дает целые a_j. Далее, из равенства $\mathbf{0} = \sum a_j\mathbf{x}^{(j)}$ следует, что $a_1 = \ldots = a_n = 0$, так как определитель соответствующей системы линейных уравнений отличен от нуля.

Лемма 3. *Пусть* $\mathbf{y}^{(1)}, \ldots, \mathbf{y}^{(n)}$ — *векторы модуля* $\mathfrak{M}_0$ *всех* n*-мерных целых векторов и положим, что из* $\sum b_j\mathbf{y}^{(j)} = 0$ *следует, что* $b_j = 0$ $(1 \leqslant j \leqslant n)$ *(т. е. векторы линейно независимы). Тогда в* $\mathfrak{M}_0$ *существует базис* $\mathbf{x}^{(j)}$, *такой, что*

$$\mathbf{y}^{(j)} = c_{j1}\mathbf{x}^{(1)} + \ldots + c_{jj}\mathbf{x}^{(j)} \quad (1 \leqslant j \leqslant n), \tag{4}$$

где c_{jk} — *целые и* $c_{jk} = 0$, *если* $k > j$. *Далее,* $c_{jj} \neq 0$.

Доказательство. Пусть $d = \det(y_{jk})$, причем d — целое число и $d \neq 0$. Тогда каждый целый вектор $\mathbf{x}$ можно представить в виде

$$d\mathbf{x} = \sum t_j\mathbf{y}^{(j)}$$

с целыми $t_1, \ldots, t_n$. Множество целых векторов $\mathbf{t} = (t_1, \ldots, t_n)$, которые могут получаться таким путем, образуют, очевидно, модуль $\mathfrak{M}$, и, значит, по следствию из леммы 1 (с обратным порядком записи индексов) в $\mathfrak{M}$ существует базис

$$\mathbf{t}^{(j)} = (t_{j1}, \ldots, t_{jj}, 0, \ldots, 0) \quad (t_{jj} \neq 0).$$

Ясно, что целые векторы $\mathbf{x}^{(j)}$, определенные равенствами

$$d\mathbf{x}^{(j)} = t_{j1}\mathbf{y}^{(1)} + \ldots + t_{jj}\mathbf{y}^{(j)}, \tag{5}$$

образуют базис модуля $\mathfrak{M}_0$. Решая последовательно (5) относительно $\mathbf{y}^{(1)}, \ldots, \mathbf{y}^{(n)}$, получаем уравнения вида (4) с рациональными c_{jk}. В частности, $c_{jj} = d/t_{jj} \neq 0$. Наконец, c_{jk} — целые, так как $\mathbf{x}^{(j)}$ — базис.

Приложение В

НЕКОТОРЫЕ СВЕДЕНИЯ ИЗ ГЕОМЕТРИИ ЧИСЕЛ

В тексте нам приходится несколько раз устанавливать существование целых $x_1, \ldots, x_n$, не равных одновременно нулю и удовлетворяющих системе неравенств вида

$$|a_{i1}x_1 + \ldots + a_{in}x_n| \leqslant c_i \quad \text{или} \quad < c_i \tag{1}$$

при $1 \leqslant i \leqslant$ некоторого m, где a_{ij} — действительные числа и $c_i > 0$. Существование таких целых чисел может быть истолковано как существование в области $\mathfrak{R}$, определенной неравенствами (1), точки с целыми координатами, не совпадающей с началом, причем $x_1, \ldots, x_n$ рассматриваются как обычные прямоугольные координаты в n-мерном эвклидовом пространстве[1]). Простейшая форма теории, которую мы здесь изложим, утверждает, что в области $\mathfrak{R}$ обязательно найдутся точки с целыми координатами, не совпадающие с началом, если $\mathfrak{R}$ имеет объем $V > 2^n$.

Мы используем векторные обозначения (см. стр. 7) и обозначаем[2]) через $\lambda\mathfrak{R}$ множество точек $\lambda\mathbf{x}$, где $\mathbf{x}$ содержится в $\mathfrak{R}$. Нас интересуют только области очень простого описанного выше вида, и поэтому мы не будем заниматься глубокими общими вопросами. В частности, будем считать, что все рассматриваемые области имеют объем (возможно, равный ∞), который обладает естественными свойствами.

В дальнейшем удобнее рассматривать области более общего вида, чем те, которые определяются неравенствами (1), а именно: области выпуклые и симметричные относительно начала. Область $\mathfrak{R}$ называется *симметричной* (относительно начала), если $-\mathfrak{R} = \mathfrak{R}$, т. е. $-\mathbf{x} \in \mathfrak{R}$, как только $\mathbf{x} \in \mathfrak{R}$.

---

[1]) Фактически все свойства, которые мы рассматриваем, являются аффинными инвариантами.

[2]) Таким образом, если $\mathfrak{R}$ определяется неравенствами (1), то $\lambda\mathfrak{R}$ определяется заменой всех c_i на λc_i.

Область $\mathfrak{R}$ называется *выпуклой*, если $\lambda\mathbf{x}+\mu\mathbf{y}\in\mathfrak{R}$ при $\lambda\geqslant 0$, $\mu\geqslant 0$, $\lambda+\mu=1$ и $\mathbf{x}, \mathbf{y}\in\mathfrak{R}$. Смысл последнего определения состоит в том, что если область $\mathfrak{R}$ содержит $\mathbf{x}$ и $\mathbf{y}$, то она содержит и весь отрезок, соединяющий их.

Заметим, что оба определения не зависят от системы координат и что если $\mathfrak{R}$ обладает обоими свойствами, то ими же обладает и $\lambda\mathfrak{R}$ при всех λ.

Лемма 1. *Область $\mathfrak{R}$, определенная неравенствами* (1), *выпукла и симметрична относительно начала.*

Доказательство. Симметричность относительно начала очевидна. Докажем теперь выпуклость. Пусть $\mathbf{x}$, $\mathbf{y}$ — две точки из $\mathfrak{R}$ и

$$\mathbf{z}=\lambda\mathbf{x}+\mu\mathbf{y}, \quad \lambda\geqslant 0, \quad \mu\geqslant 0, \quad \lambda+\mu=1.$$

Тогда

$$\begin{gathered}|a_{i1}z_1+\ldots+a_{in}z_n|\leqslant\\ \leqslant\lambda|a_{i1}x_1+\ldots+a_{in}x_n|+\mu|a_{i1}y_1+\ldots+a_{in}y_n|\leqslant\\ \leqslant\max(|a_{i1}x_1+\ldots+a_{in}x_n|, \quad |a_{i1}y_1+\ldots+a_{in}y_n|).\end{gathered}$$

Значит, если $\mathbf{x}$, $\mathbf{y}$ удовлетворяют неравенствам (1), то им же удовлетворяет и $\mathbf{z}$.

Лемма 2. *Если область $\mathfrak{R}$ выпукла и симметрична относительно начала, то $\lambda\mathbf{x}\in\mathfrak{R}$, как только $|\lambda|\leqslant 1$ и $\mathbf{x}\in\mathfrak{R}$.*

Доказательство. В силу симметрии $-\mathbf{x}\in\mathfrak{R}$, а значит, в силу выпуклости

$$\rho\mathbf{x}+\sigma(-\mathbf{x})=\lambda\mathbf{x}\in\mathfrak{R},$$

где

$$\rho=\frac{1}{2}(1+\lambda)\geqslant 0, \quad \sigma=\frac{1}{2}(1-\lambda)\geqslant 0, \quad \rho+\sigma=1.$$

Лемма 3. *Если $\mathfrak{R}$ выпукла и симметрична, то $\lambda\mathbf{x}+\mu\mathbf{y}\in\mathfrak{R}$, как только $|\lambda|+|\mu|\leqslant 1$ и $\mathbf{x}\in\mathfrak{R}$, $\mathbf{y}\in\mathfrak{R}$.*

Замечание. Геометрически это означает, что если область $\mathfrak{R}$ содержит точки $\mathbf{x}$ и $\mathbf{y}$, то она содержит целиком параллелограм с вершинами $\pm\mathbf{x}$, $\pm\mathbf{y}$ и с центром в начале.

Доказательство. По лемме 2

$$\mathbf{x}'=\eta_1(|\lambda|+|\mu|)\,\mathbf{x}\in\mathfrak{R}, \quad \mathbf{y}'=\eta_2(|\lambda|+|\mu|)\,\mathbf{y}\in\mathfrak{R},$$

где η_1, η_2 — знаки чисел соответственно λ, μ. Следовательно, силу выпуклости

$$\lambda\mathbf{x}+\mu\mathbf{y}=\rho\mathbf{x}'+\sigma\mathbf{y}'\in\mathfrak{R},$$

где

$$\rho=\frac{|\lambda|}{|\lambda|+|\mu|},\quad \sigma=\frac{|\mu|}{|\lambda|+|\mu|},\quad \rho+\sigma=1.$$

Теперь мы можем приступить к доказательству главных результатов, первый из которых не требует от области $\mathfrak{R}$ ни выпуклости, ни симметричности.

Теорема I (Блихфельдт). *Предположим, что $\mathfrak{R}$ — область в n-мерном пространстве, объем которой $V>1$ (возможно, $V=\infty$). Тогда существуют две различные точки $\mathbf{x}'\in\mathfrak{R}$, $\mathbf{x}''\in\mathfrak{R}$, такие, что $\mathbf{x}''-\mathbf{x}'$ имеет целые координаты.*

Доказательство. Рассмотрим все возможные целые точки $\mathbf{u}=(u_1,\ \ldots,\ u_n)$ и определим $\mathfrak{R}_\mathbf{u}$ как часть области $\mathfrak{R}$, находящуюся в гиперкубе

$$u_i\leqslant x_i<u_i+1\quad(1\leqslant i\leqslant n).$$

Обозначим через $\mathscr{S}_\mathbf{u}$ множество точек в гиперкубе $0\leqslant x_i<1$, полученных из $\mathfrak{R}_\mathbf{u}$ путем переноса $-\mathbf{u}$ (т. е. $\mathscr{S}_\mathbf{u}$ — множество точек $\mathbf{x}-\mathbf{u}$, где $\mathbf{x}\in\mathfrak{R}_\mathbf{u}$). Тогда $\mathscr{S}_\mathbf{u}$ имеет объем $V_\mathbf{u}$, где $\sum V_\mathbf{u}=V>1$. Так как объем гиперкуба $0\leqslant x_i<1$ равен 1, то по меньшей мере два множества среди множеств $\mathscr{S}_\mathbf{u}$, скажем $\mathscr{S}_{\mathbf{u}'}$, $\mathscr{S}_{\mathbf{u}''}$, должны перекрыться. Следовательно, существуют две точки $\mathbf{x}'$, $\mathbf{x}''$, принадлежащие соответственно $\mathfrak{R}_{\mathbf{u}'}$, $\mathfrak{R}_{\mathbf{u}''}$ (а значит, и $\mathfrak{R}$), такие, что $\mathbf{x}'-\mathbf{u}'=\mathbf{x}''-\mathbf{u}''$. Отсюда $\mathbf{x}'$, $\mathbf{x}''$ имеет целые координаты.

Теорема II (Минковский). *Пусть $\mathfrak{R}$ — выпуклая область, симметричная относительно начала, объем которой $V>2^n$ (возможно, $V=\infty$). Тогда $\mathfrak{R}$ содержит точку с целыми координатами, не совпадающую с началом.*

Доказательство. Область $\frac{1}{2}\mathfrak{R}$ имеет объем $\left(\frac{1}{2}\right)^n V>1$. Значит, по теореме I существуют $\mathbf{x}'$, $\mathbf{x}''\in\frac{1}{2}\mathfrak{R}$, такие, что вектор $\mathbf{x}'-\mathbf{x}''=\mathbf{u}$ имеет целые координаты. Но тогда по лемме 3 точка $\frac{1}{2}\mathbf{x}' - \frac{1}{2}\mathbf{x}'' = \frac{1}{2}\mathbf{u} \in \frac{1}{2}\mathfrak{R}$, т. е. $\mathbf{u} \in \mathfrak{R}$, что и требовалось доказать.

Теорема II перестает действовать, когда $V = 2^n$, как показывает пример области $\mathfrak{R}$, определенной неравенствами $|x_i| < 1$ $(1 \leqslant i \leqslant n)$. Объем этой области равен 2^n, но, очевидно, внутри нее нет ни одной целой точки, отличной от начала. Однако если $\mathfrak{R}$ удовлетворяет некоторым дополнительным требованиям, то теорема II сохраняет силу. Рассмотрим сначала частный случай. Область $\mathfrak{R}$ называется *ограниченной*, если существует число $R > 0$, такое, что все точки области $\mathfrak{R}$ лежат в гиперкубе $|x_i| \leqslant R$ $(1 \leqslant i \leqslant n)$.

Лемма 4. *Область $\mathfrak{R}$, определенная n соотношениями вида*

$$|a_{i1}x_1 + \ldots + a_{in}x_n| \leqslant c_i \quad \text{или} \quad < c_i, \tag{2}$$

где $d = |\det(a_{ij})| > 0$, ограничена и имеет объем

$$V = 2^n d^{-1} c_1 c_2 \ldots c_n.$$

Доказательство. Обозначим $\xi_i = \sum a_{ij}x_j$. Тогда, если α_{ij} — матрица, обратная для матрицы a_{ij} и $\mathbf{x} \in \mathfrak{R}$, то имеем

$$|x_i| = |\sum \alpha_{ij}\xi_j| \leqslant \sum |\alpha_{ij}| c_j \leqslant \text{ некоторого } R,$$

не зависящего от $\mathbf{x}$ и i. Объем V находится сразу простым интегрированием или иным способом.

Следствие 1. *Область $\mathfrak{R}$, определенная более чем n соотношениями вида* (2), *ограничена, если какие-нибудь n из этих соотношений удовлетворяют условиям леммы.*

Следствие 2. *Если область $\mathfrak{R}$ определяется $m < n$ соотношениями вида* (2) *или n соотношениями этого же вида* с $\det(a_{ij}) = 0$, *то $V = \infty$ и $\mathfrak{R}$ неограничена.*

Доказательство очевидно.

Следствие 3. *Предположим, что или $m < n$, или $m = n$, а* $\det(a_{ij}) = 0$. *Пусть $c_1, \ldots, c_m$ — любые положительные числа, как угодно малые. Тогда существуют целые $x_1, \ldots, x_n$, не равные нулю одновременно, такие, что*

$$\left|\sum a_{ij}x_j\right| < c_i \quad (1 \leqslant i \leqslant m).$$

Доказательство следует сразу из следствия 2 и теоремы II.

Теорема III (Минковский). *Существуют целые* x_j, *не все разные нулю, такие, что*

$$\left|\sum a_{1j}x_j\right| \leqslant c_1, \quad \left|\sum a_{ij}x_j\right| < c_i \quad (2 \leqslant i \leqslant n) \tag{3}$$

при условии, что

$$c_1 \ldots c_n \geqslant \left|\det(a_{ij})\right|. \tag{4}$$

Доказательство. Если в (4) имеет место знак $>$, то теорема III получается сразу из теоремы II и из последней леммы. Предположим теперь, что в (4) имеет место знак $=$. По теореме II для любого ε $(0 < \varepsilon < 1)$ можно найти целые $\mathbf{x}^{(\varepsilon)} \neq \mathbf{0}$, такие, что

$$\left|\sum a_{1j}x^{(\varepsilon)}\right| < c_1 + \varepsilon < c_1 + 1, \quad \left|\sum a_{ij}x_j^{(\varepsilon)}\right| < c_i \ (i \neq 1). \tag{5}$$

По лемме 4 все $x_j^{(\varepsilon)}$ удовлетворяют условию $\left|x_j^{(\varepsilon)}\right| \leqslant R$ $(1 \leqslant j \leqslant n)$, где R — некоторое число, не зависящее от ε. Таким образом, только конечное число векторов $\mathbf{x} \neq \mathbf{0}$ может встречаться в роли $\mathbf{x}^{(\varepsilon)}$. Некоторый целый вектор, скажем $\mathbf{x}^{(0)} \neq \mathbf{0}$, должен встречаться в роли $\mathbf{x}^{(\varepsilon)}$ при любом как угодно малом ε. Записывая в (5) $x_j^{(0)}$ вместо $x_j^{(\varepsilon)}$ и полагая $\varepsilon \to 0$, получаем доказательство теоремы.

Распространим теперь теорему II на случай, когда $V = 2^n$. Область $\mathfrak{R}$ называется *замкнутой*, если всякий раз, когда точки $\mathbf{x}^{(m)}$ $(m = 1, 2, \ldots)$ принадлежат $\mathfrak{R}$ и $\mathbf{x}^{(0)} = \lim \mathbf{x}^{(m)}$ существует (в том смысле, что каждая координата точки $\mathbf{x}^{(m)}$ стремится к соответствующей координате точки $\mathbf{x}^{(0)}$), $\mathbf{x}^{(0)}$ также принадлежит $\mathfrak{R}$.

Таким образом, если область $\mathfrak{R}$ определяется только неравенствами вида $\left|\sum a_{ij}x_j\right| \leqslant c_i$, то $\mathfrak{R}$ замкнута. Грубо говоря, область $\mathfrak{R}$ замкнута, если она содержит свою границу.

Теорема IV (Минковский). *Предположим, что выпуклая симметричная относительно начала область* $\mathfrak{R}$ *замкнута, ограничена*[1]) *и имеет объем* $V \geqslant 2^n$. *Тогда в* $\mathfrak{R}$ *существует точка* $\mathbf{x} \neq \mathbf{0}$ *с целыми координатами.*

---

[1]) Можно доказать, что ограниченность следует из выпуклости, если $0 < V < \infty$.

Доказательство. Область $(1+\varepsilon)\mathfrak{R}$ при $0<\varepsilon<1$ имеет объем

$$(1+\varepsilon)^n V > 2^n.$$

По теореме II в области $(1+\varepsilon)\mathfrak{R}$, а следовательно, и в $2\mathfrak{R}$ существует целая точка $\mathbf{x}^{(\varepsilon)} \neq \mathbf{0}$. В силу ограниченности области $\mathfrak{R}$ только конечное число целых точек может встречаться в роли $\mathbf{x}^{(\varepsilon)}$, а следовательно, одна из них, скажем $\mathbf{x}^{(0)} \neq \mathbf{0}$, должна встречаться в $(1+\varepsilon)\mathfrak{R}$ при любом произвольно малом ε. Значит,

$$(1+\varepsilon)^{-1}\mathbf{x}^{(0)} \in \mathfrak{R}$$

при любом как угодно малом ε. Следовательно, $\mathbf{x}^{(0)} \in \mathfrak{R}$, так как $\mathfrak{R}$ замкнута.

Заметим, что теорема III сообщает нам больше, чем теорема IV, в своем специальном случае, так как область, определенная неравенствами (3), не замкнута.

Иногда[1] бывает недостаточно знать, что область $\mathfrak{R}$ содержит одну целую точку, не совпадающую с началом координат. Точки $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(J)}$ множества J называются *линейно независимыми*, если из равенства

$$\mu_1\mathbf{x}^{(1)} + \ldots + x_J\mathbf{x}^{(J)} = \mathbf{0}$$

следует, что $\mu_1 = \ldots = \mu_J = 0$. Мы рассмотрим случай, когда $\mathfrak{R}$ содержит J линейно независимых точек. В дальнейшем для простоты считаем, что

$$\left.\begin{array}{l}\text{Область } \mathfrak{R} \text{ выпукла, симметрична относительно} \\ \text{начала и замкнута: она имеет объем } V,\ 0<V<\infty.\end{array}\right\} \quad (6)$$

[Если область $\mathfrak{R}$ не замкнута, то будем рассматривать вместо $\mathfrak{R}$ множество $\overline{\mathfrak{R}}$, состоящее из $\mathfrak{R}$ вместе с его граничными точками.]

Для любого вектора $\mathbf{x}$ определим *функцию расстояния* $F(\mathbf{x})$ относительно $\mathfrak{R}$ как нижнюю грань чисел λ, таких, что $\lambda^{-1}\mathbf{x} \in \mathfrak{R}$; если таких λ не существует, то условно[2] считаем $F(\mathbf{x}) = \infty$. Тогда $0 \leqslant F(\mathbf{x}) \leqslant \infty$ и $F(\mathbf{x}) = 0$ только для $\mathbf{x} = \mathbf{0}$, так как $\mathfrak{R}$ ограничена. Например, если область $\mathfrak{R}$

[1]) Конец этого приложения требуется только для гл. V, § 8, 9.

[2]) Мы увидим позднее, что этого не случится.

определена неравенствами $\left|\sum a_{ij}x_j\right| \leqslant c_i$, то

$$F(\mathbf{x}) = \max_i c_i^{-1}\left|\sum_j a_{ij}x_j\right|.$$

Часто бывает удобнее иметь дело с $F(\mathbf{x})$, чем непосредственно с областью $\mathfrak{R}$. В следующих двух леммах доказаны главные свойства этой функции.

Лемма 5. *Для того чтобы* $\mathbf{x} \in \lambda\mathfrak{R}$ *при* $\lambda \geqslant 0$, *необходимо и достаточно выполнение неравенства* $\lambda \geqslant F(\mathbf{x})$.

Доказательство. По определению $(F(\mathbf{x}))^{-1}\mathbf{x} \in \mathfrak{R}$, так как $\mathfrak{R}$ замкнута. По лемме 2 $\lambda^{-1}\mathbf{x} \in \mathfrak{R}$ для $\lambda \geqslant F(\mathbf{x})$. Наконец, $\lambda^{-1}\mathbf{x} \notin \mathfrak{R}$ для $\lambda < F(\mathbf{x})$ по определению.

Лемма 6. (i) $F(\lambda\mathbf{x}) = |\lambda| F(\mathbf{x})$ *для всех векторов* $\mathbf{x}$ *и чисел* λ.

(ii) $F(\mathbf{x}^{(1)} + \mathbf{x}^{(2)}) \leqslant F(\mathbf{x}^{(1)}) + F(\mathbf{x}^{(2)})$ *для всех векторов* $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}$.

Доказательство (i) тривиально.

(ii) Положим $\mu_j = F(\mathbf{x}^{(j)})$, так что $\mu_j^{-1}\mathbf{x}^{(j)} \in \mathfrak{R}$ $(j = 1,2)$. Тогда

$$(\mu_1 + \mu_2)^{-1}(\mathbf{x}^{(1)} + \mathbf{x}^{(2)}) = \frac{\mu_1}{\mu_1 + \mu_2}(\mu_1^{-1}\mathbf{x}^{(1)}) + \frac{\mu_2}{\mu_1 + \mu_2}(\mu_2^{-1}\mathbf{x}^{(2)})$$

принадлежит $\mathfrak{R}$ по определению выпуклости, т. е.

$$F(\mathbf{x}^{(1)} + \mathbf{x}^{(2)}) \leqslant \mu_1 + \mu_2,$$

что и требовалось доказать.

Так как $V > 0$, то в области $\mathfrak{R}$ должно быть n линейно независимых точек $\mathbf{z}^{(1)}, \ldots, \mathbf{z}^{(n)}$ (не обязательно целых). Для любых чисел $\mu_1, \ldots, \mu_n$ имеем по лемме 6

$$F(\mu_1\mathbf{z}^{(1)} + \ldots + \mu_n\mathbf{z}^{(n)}) \leqslant |\mu_1| F(\mathbf{z}^{(1)}) + \ldots$$
$$\ldots + |\mu_n| F(\mathbf{z}^{(n)}) \leqslant |\mu_1| + \ldots + |\mu_n|.$$

Таким образом, область $\mathfrak{R}$ содержит целиком „обобщенный восьмигранник“

$$\mu_1\mathbf{z}^{(1)} + \ldots + \mu_n\mathbf{z}^{(n)}, \qquad |\mu_1| + \ldots + |\mu_n| \leqslant 1.$$

В частности, $\lambda\mathcal{R}$ содержит любую данную точку, если λ достаточно велико.

По лемме 5 для каждого J, $1 \leqslant J \leqslant n$, существует наименьшее λ, например λ_J, такое, что $\lambda\mathcal{R}$ содержит J линейно независимых точек. Будем называть λ_J J-м *последовательным минимумом* области $\mathcal{R}$. Теорема II показывает, что $\lambda_1^n V \leqslant 2^n$, так как при всех $\lambda < \lambda_1$ область $\lambda\mathcal{R}$ имеет объем $\lambda^n V$ и не содержит ни одной целой точки, кроме нуля. Если рассмотреть область $\mathcal{R}$, определенную неравенствами $|x_1| \leqslant M$, $|x_i| \leqslant 1$ $(2 \leqslant i \leqslant n)$, где M велико, и имеющую объем $V = 2^n M$, $\lambda_1 = M^{-1}$, $\lambda_J = 1$ $(2 \leqslant J)$, то легко, однако, проверить, что оценка для λ_J $(2 \leqslant J)$ в терминах V невозможна. Следующая теорема дает оценку для произведения $\lambda_1 \ldots \lambda_n$.

Теорема V (Минковский). *Последовательные минимумы удовлетворяют неравенству*

$$2^n/n! \leqslant V\lambda_1 \ldots \lambda_n \leqslant 2^n.$$

Замечание. Из этой теоремы сразу следует теорема IV, так как если $V \geqslant 2^n$, то $\lambda_1^n \leqslant \lambda_1\lambda_2 \ldots \lambda_n \leqslant 1$, $\lambda_1 \leqslant 1$, т. е. $\mathcal{R} = 1\mathcal{R}$ содержит целую точку, отличную от нуля.

Доказательство. Левая часть неравенства доказывается непосредственно. Выберем последовательно n точек $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(n)}$ с целыми координатами, таких, что $\mathbf{x}^{(J)}$ лежит в области $\lambda_J\mathcal{R}$ и линейно зависит от

$$\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(J-1)}.$$

Ясно, что это возможно. Пусть $\mathbf{x}^{(J)}$ имеет координаты $(\mathbf{x}_{J1}, \ldots, \mathbf{x}_{Jn})$, такие, что $\det(x_{ji}) \neq 0$ и, следовательно,

$$|\det(x_{ji})| \geqslant 1,$$

так как числа x_{ji} — целые. При любых постоянных $\mu_1, \ldots, \mu_n$ имеем по лемме 6

$$F(\mu_1\mathbf{x}^{(1)} + \ldots + \mu_n\mathbf{x}^{(n)}) \leqslant |\mu_1| F(\mathbf{x}^{(1)}) + \ldots + |\mu_n| F(\mathbf{x}^{(n)}) \leqslant \leqslant |\mu_1|\lambda_1 + \ldots + |\mu_n|\lambda_n.$$

Значит,

$$\mu_1\mathbf{x}^{(1)} + \ldots + \mu_n\mathbf{x}^{(n)} \tag{7}$$

содержится в области $\mathfrak{R}$ при условии, что

$$|\mu_1|\lambda_1 + \ldots + |\mu_n|\lambda_n \leqslant 1. \tag{8}$$

Но легко установить, что множество точек (7) при наличии (8) имеет объем[1])

$$\frac{2^n|\det(x_{ji})|}{n!\,\lambda_1 \ldots \lambda_n} \geqslant \frac{2^n}{n!\,\lambda_1 \ldots \lambda_n}.$$

Этот объем не превосходит объема V области $\mathfrak{R}$, что и доказывает первую половину этой теоремы.

Доказательство правой части неравенства много труднее. Удобно ввести замену координат такого вида:

$$x'_i = t_{i1}x_1 + \ldots + t_{in}x_n, \tag{9}$$

где числа t_{ij} — целые и

$$\det(t_{ij}) = \pm 1. \tag{10}$$

Выражая x_i через x'_i, получаем

$$x_j = s_{i1}x'_1 + \ldots + s_{in}x'_n, \tag{11}$$

где числа s_{ij} — опять целые по (10). Следовательно, равенство (9) переводит целые координаты в целые координаты и наоборот. Таким образом, когда мы говорим о точках с целыми координатами, то неважно, какая система имеется в виду, старая или новая. Как мы уже отмечали, определения выпуклости и симметрии не зависят от системы координат.

Лемма 7. *Если* $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(n)}$ — n *линейно независимых точек с целыми координатами, то существует такое преобразование координат вида* (9), (10), *что точка* $\mathbf{x}^{(i)}$ *имеет новые координаты вида*

$$(x'_{i1}, x'_{i2}, \ldots, x'_{ii}, 0, \ldots, 0)$$

для $1 \leqslant i \leqslant n$.

Доказательство. Эта лемма является перефразировкой лемм 2 и 3 приложения А. По лемме 3 (приложение А) существуют n целых векторов $\mathbf{s}^{(i)} = (s_{i1}, \ldots, s_{in})$,

[1]) Например, принимая $\mu_1, \ldots, \mu_n$ за переменные интегрирования.

образующих базис в модуле всех целых векторов, таких, что $\mathbf{x}^{(i)} = x'_{i1}\mathbf{s}^{(1)} + \ldots + x'_{ii}\mathbf{s}^{(i)}$ при целых x'_{ij}. Так как по лемме 2 (приложение A) $\det(s_{ij}) = \pm 1$, то преобразование (11) с такими s_{ij} обеспечивает справедливость леммы.

Поэтому мы будем предполагать, что точки $\mathbf{x}^{(i)}$, дающие последовательные минимумы, имеют координаты

$$\mathbf{x}^{(i)} = (x_{i1}, \ldots, x_{ii}, 0, \ldots, 0).$$

Лемма 8. *Если* $\mathbf{x}$ — *целая точка и* $F(\mathbf{x}) < \lambda_J$, *то*

$$x_J = x_{J+1} = \ldots = x_n = 0.$$

Доказательство очевидно, так как точка $\mathbf{x}$ не может быть линейно независимой от

$$\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(J-1)}.$$

Следствие. *Пусть* $\mathbf{x}'' - \mathbf{x}'$ — *целая точка и*

$$F(\mathbf{x}') < \frac{1}{2}\lambda_J, \qquad F(\mathbf{x}'') < \frac{1}{2}\lambda_J.$$

Тогда $x'_j = x''_j \quad (J \leqslant j \leqslant n)$.

Доказательство. $F(\mathbf{x}'' - \mathbf{x}') \leqslant F(\mathbf{x}'') + F(\mathbf{x}') < \lambda_J$.

Доказательство теоремы V (продолжение). Положим $\mathscr{W}_0(\lambda) = \lambda\mathfrak{R}$ и для каждого целого J $(1 \leqslant J \leqslant n)$ определим $\mathscr{W}_J(\lambda)$ как множество точек[1])

$$(\{x_1\}, \ldots, \{x_J\}, x_{J+1}, \ldots, x_n),$$

где $\mathbf{x} \in \lambda\mathfrak{R}$. Если $\lambda \geqslant \lambda'$, то $\mathscr{W}_J(\lambda)$ содержит $\mathscr{W}_J(\lambda')$, так как $\lambda\mathfrak{R}$ содержит $\lambda'\mathfrak{R}$, но разность между объемами множеств $\mathscr{W}_J(\lambda)$ и $\mathscr{W}_J(\lambda')$ не превосходит, очевидно, разности между объемами областей $\lambda\mathfrak{R}$ и $\lambda'\mathfrak{R}$, т. е. $(\lambda^n - \lambda'^n)V$. Следовательно, объем $V_J(\lambda)$ множества $\mathscr{W}_J(\lambda)$ возрастает непрерывно с ростом λ. Так как $\mathscr{W}_n(\lambda)$ лежит целиком в единичном кубе, то имеем

$$V_n(\lambda) \leqslant 1 \tag{12}$$

для всех λ.

---

[1]) Обозначение $\{x\}$ см. на стр. 7.

Лемма 9. $V_n(\lambda) = V_J(\lambda)$, *если* $\lambda \leqslant \frac{1}{2}\lambda_{J+1}$ $(J < n)$.

Доказательство. Если $\lambda < \frac{1}{2}\lambda_{J+1}$, то лемма следует непосредственно из следствия леммы 8. При $\lambda = \frac{1}{2}\lambda_{J+1}$ она справедлива в силу непрерывности.

В частности,

$$V_n(\lambda) = V_0(\lambda) = \lambda^n V \qquad \left(\lambda \leqslant \frac{1}{2}\lambda_1\right). \tag{13}$$

Лемма 10. *Пусть* $\mathscr{S}$ — *некоторая область единичного J-мерного куба* $0 \leqslant x_j < 1$ $(1 \leqslant j \leqslant J)$, *и пусть* $\mathscr{S}'$ — *множество точек* $(\{b_j + x_j\})$ $(1 \leqslant j \leqslant J)$, *где* $b_1, \ldots, b_J$ *фиксированы и* $(x_1, \ldots, x_J) \in \mathscr{S}$. *Тогда* $\mathscr{S}$ *и* $\mathscr{S}'$ *имеют один и тот же объем.*

Доказательство очевидно.

Лемма 11. $V_J(\lambda) \geqslant (\lambda/\lambda')^{n-J} V_J(\lambda')$, *если* $\lambda \geqslant \lambda'$.

Доказательство. Для любых $a_{J+1}, \ldots, a_n$ через $v(a_{J+1}, \ldots, a_n)$ обозначим J-мерный объем части множества $\mathscr{W}_J(\lambda)$, лежащей в

$$x_{J+1} = a_{J+1}, \ldots, x_n = a_n,$$

так что

$$V_J(\lambda) = \int \ldots \int v(x_{J+1}, \ldots, x_n)\, dx_{J+1} \ldots dx_n. \tag{14}$$

Пусть объем $v'(a_{J+1}, \ldots, a_n)$ аналогично определяется относительно области $\mathscr{W}_J(\lambda')$. Для доказательства леммы, в силу (14), достаточно, очевидно, доказать, что

$$v\left(\frac{\lambda}{\lambda'} a_{J+1}, \ldots, \frac{\lambda}{\lambda'} a_n\right) \geqslant v'(a_{J+1}, \ldots, a_n) \tag{15}$$

для каждого $(a_{J+1}, \ldots, a_n)$.

Это неравенство заведомо справедливо, если правая часть равна нулю. Если же она отлична от нуля, то существует некоторая точка, например $(a_1, \ldots, a_J, a_{J+1}, \ldots, a_n) \in \lambda'\mathfrak{R}$, с выбранными последними $n - J$ координатами. Мы до конца рассуждений будем считать их фиксированными. Пусть теперь $(x_1, \ldots, x_J, a_{J+1}, \ldots, a_n) \in \mathscr{W}_J(\lambda')$, так что, в частности,

$0 \leqslant x_j < 1$ $(1 \leqslant j \leqslant J)$. Тогда существуют целые точки $(u_1, \ldots, u_J)$, такие, что

$$(x_1 + u_1, \ldots, x_J + u_J, a_{J+1}, \ldots, a_n) \in \lambda' \mathcal{R}.$$

Следовательно,

$$\left(\frac{\lambda}{\lambda'} - 1\right)(a_1, \ldots, a_n) + \\ + (x_1 + u_1, \ldots, x_J + u_J, a_{J+1}, \ldots, a_n) \in \lambda \mathcal{R}$$

по лемме 6. Значит, окончательно

$$\left(y_1, \ldots, y_J, \frac{\lambda}{\lambda'} a_{J+1}, \ldots, \frac{\lambda}{\lambda'} a_n\right) \in \mathscr{W}^\circ_J(\lambda),$$

где

$$y_j = \{b_j + x_j\}, \qquad b_j = \left(\frac{\lambda}{\lambda'} - 1\right) a_j.$$

Теперь (15) непосредственно следует из леммы 10, если $x_1, \ldots, x_J$ пробегают все значения, такие, что вектор $(x_1, \ldots, x_J, a_{J+1}, \ldots, a_n) \in \mathscr{W}^\circ_J(\lambda')$. Как было уже замечено, это и доказывает лемму.

Доказательство теоремы V (окончание). Прежде всего

$$V_n\left(\frac{1}{2}\lambda_1\right) = V_0\left(\frac{1}{2}\lambda_1\right) = \left(\frac{1}{2}\lambda_1\right)^n V$$

по (13). По лемме 9 имеем $V_n(\lambda) = V_1(\lambda)$, если $\frac{1}{2}\lambda_1 \leqslant \lambda \leqslant \frac{1}{2}\lambda_2$, и, значит, по лемме 11

$$V_n\left(\frac{1}{2}\lambda_2\right) \geqslant (\lambda_2/\lambda_1)^{n-1} V_n\left(\frac{1}{2}\lambda_1\right).$$

Аналогично

$$V_n\left(\frac{1}{2}\lambda_3\right) \geqslant (\lambda_3/\lambda_2)^{n-2} V_n\left(\frac{1}{2}\lambda_2\right),$$

$$\vdots$$

$$V_n\left(\frac{1}{2}\lambda_n\right) \geqslant (\lambda_n/\lambda_{n-1})^1 V_n\left(\frac{1}{2}\lambda_{n-1}\right).$$

Перемножив эти неравенства, получим

$$V_n\left(\frac{1}{2}\lambda_n\right)\geqslant 2^{-n}\lambda_1\ldots\lambda_n V,$$

а это неравенство совместно с (12) дает $\lambda_1 \ldots \lambda_n V\leqslant 2^n$.

Теорема VI (Малер). *Существует множество n целых точек* $\mathbf{y}^{(r)}$ $(1\leqslant r\leqslant n)$, *такое, что* $\det(y_{rj})=\pm 1$ *и* $V\prod F(\mathbf{y}^{(r)})\leqslant 2\cdot n!$[1]).

Доказательство. Согласно лемме 7, мы можем считать, что

$$\mathbf{x}^{(r)}=(x_{r1},\ \ldots,\ x_{rr}, 0,\ \ldots,\ 0),$$

где $x_{rr}\neq 0$, так как точки $\mathbf{x}^{(r)}$ линейно независимы. Мы покажем, что можно брать точки

$$\mathbf{y}^{(r)}=(y_{r1},\ \ldots,\ y_{r,r-1}, 1,0,\ \ldots,\ 0)$$

при подходящих целых $y_{r1},\ \ldots,\ y_{r,r-1}$, такие, что $F(\mathbf{y}^{(r)})\leqslant \mu_r$, где

$$\mu_1=\lambda_1, \mu_r=\frac{1}{2}r\lambda_r \qquad (r\geqslant 2).$$

Тогда теорема VI следует из теоремы V.

Очевидно, что точка $\mathbf{y}^{(1)}=x_{11}^{-1}\mathbf{x}^{(1)}=(1, 0,\ \ldots,\ 0)$ — искомая. Аналогично, если при $r>1$ имеем $x_{rr}=\pm 1$, то можно положить

$$\mathbf{y}^{(r)}=x_{rr}^{-1}\mathbf{x}^{(r)},$$

где координаты — целые числа и $F(\mathbf{y}^{(r)})=\lambda_r\leqslant\mu_r$. Таким образом, мы можем предполагать, что $|x_{rr}|\geqslant 2$. Заведомо существуют постоянные $\beta_1,\ \ldots,\ \beta_{r-1}$, такие, что

$$\mathbf{e}^{(r)}=(0,\ \ldots,\ 0,1,0,\ \ldots,\ 0)= \\ =\beta_1\mathbf{x}^{(1)}+\ \ldots\ +\beta_{r-1}\mathbf{x}^{(r-1)}+x_{rr}^{-1}\mathbf{x}^{(r)},$$

---

[1]) Постоянная $2\cdot n!$ не является постоянной Малера, и она, очевидно, может быть улучшена. Важно, что она зависит только от n.

где 1 стоит на r-м месте. Выберем целые $b_1, \ldots, b_{r-1}$ так, что $|\beta_j - b_j| \leqslant 1/2$, и положим

$$\mathbf{y}^{(r)} = \mathbf{e}^{(r)} - b_1\mathbf{x}^{(1)} - \ldots - b_{r-1}\mathbf{x}^{(r-1)} =$$
$$= x_{rr}^{-1}\mathbf{x}^{(r)} + (\beta_1 - b_1)\,\mathbf{x}^{(1)} + \ldots + (\beta_{r-1} - b_{r-1})\,\mathbf{x}^{(r-1)}.$$

Тогда из первого выражения $\mathbf{y}^{(r)}$ имеет целые координаты и из второго выражения

$$F(\mathbf{y}^{(r)}) \leqslant |x_{rr}|^{-1} F(\mathbf{x}^{(r)}) +$$
$$+ |\beta_1 - b_1| F(\mathbf{x}^{(1)}) + \ldots + |\beta_{r-1} - b_{r-1}| F(\mathbf{x}^{(r-1)}) \leqslant$$
$$\leqslant \frac{1}{2}(\lambda_1 + \ldots + \lambda_r) \leqslant \frac{1}{2} r\lambda_r = \mu_r.$$

ЗАМЕЧАНИЯ

Доказательства теорем V, VI переделаны из доказательства Вейля [см. Вейль (1942)]. Распространение на произвольные множества точек см. у Роджерса (1949) и Малера (1949) или Шаботи (1949).

Приложение С

ЛЕММА ГАУССА

Лемма (Гаусс). *Пусть* $f = f(x_1, \ldots, x_m)$ *и* $g = g(x_1, \ldots, x_m)$ — *полиномы от любого числа переменных* $x_1, \ldots, x_m$. *Предположим, что каждый из* f, g *имеет целые рациональные коэффициенты без общего делителя. Тогда коэффициенты произведения* fg — *тоже целые без общего делителя.*

Доказательство. Можно записать

$$f = \sum_I a_I I, \qquad g = \sum_I b_I I, \tag{1}$$

где I пробегает все одночлены

$$I = x_1^{i_1} \ldots x_m^{i_m}.$$

Тогда

$$fg = \sum c_I I, \tag{2}$$

где

$$c_I = \sum_{JK = I} a_J b_K. \tag{3}$$

Будем говорить, что одночлен $I = x_1^{i_1} \ldots x_m^{i_m}$ *ниже* одночлена $J = x_1^{j_1} \ldots x_m^{j_m}$, если первая не равная нулю разность в последовательности $j_1 - i_1, \ldots, j_m - i_m$ положительна. Если $IJ = I_0 J_0$, то, очевидно, или $I = I_0$, $J = J_0$, или I ниже I_0, или J ниже J_0.

Пусть p — любое простое. По предположению p не делит сразу все a_I. Пусть I_0 — наинизший одночлен, такой, что $p \nmid b_{J_0}$. Аналогично существует наинизший J_0 одночлен, такой, что $p \nmid b_{J_0}$. Тогда

$$c_{I_0 J_0} = \sum a_I b_J \qquad (IJ = I_0 J_0). \tag{4}$$

Если I ниже I_0, то $p \mid a_I$, и если J ниже J_0, то $p \mid b_J$ по предположению. Следовательно, p делит все слагаемые в (4), кроме $a_{I_0}b_{J_0}$. Таким образом,

$$p \nmid c_{I_0 J_0}, \quad p \nmid \text{н. о. д. } (c_I).$$

Так как p — любое простое, то тем самым лемма доказана.

Следствие 1. *Предположим теперь, что коэффициенты полиномов f, g могут иметь общий делитель. Тогда*

$$\text{н. о. д. } (c_I) = \text{н. о. д. } (a_I) \cdot \text{н. о. д. } (b_I).$$

Доказательство. Рассматриваем полиномы

$$(\text{н. о. д. } (a_I))^{-1} f, \quad (\text{н. о. д. } (b_I))^{-1} g \quad \text{вместо } f, \ g.$$

Следствие 2. *Пусть полином $f(x_1, \ldots, x_m)$ имеет целые коэффициенты без общего делителя, а полином $g(x_1, \ldots, x_m)$ имеет рациональные коэффициенты. Если fg имеет целые коэффициенты, то коэффициенты полинома g — целые.*

Доказательство. Пусть t — целое, такое, что коэффициенты полинома tg — целые. Тогда $t \cdot fg = f \cdot tg$ имеет целые коэффициенты, делящиеся на t по предположению. Значит,

$$t \mid \text{н. о. д. } (a_I) \text{ н. о. д. } (tb_I)$$

по предыдущему следствию. Так как н. о. д. $(a_I) = 1$ по предположению, то b_I должны быть целыми.

Следствие 3. *Предположим, что f, g имеют рациональные коэффициенты, а fg имеет целые коэффициенты. Тогда существует рациональное число k, такое, что kf, $k^{-1}g$ имеют целые коэффициенты.*

Доказательство. Ясно, что существует рациональное число k, такое, что коэффициенты полинома kf — целые без общего делителя. Так как $fg = (kf)(k^{-1}g)$, то применимо предыдущее следствие к kf, $k^{-1}g$.

ЛИТЕРАТУРА

Барнс (Barnes E. S.)
(1956) On linear inhomogeneous Diophantine approximation, *J. Lond. Math. Soc.*, **31**, 73—79.

Барнс и Суиннертон-Дайер (Barnes E. S. and Swinnerton-Dyer H. P. F.)
(1952) The inhomogeneous minima of binary quadratic forms I, II, *Acta Math., Stockh.*, **87**, 259—323; **88**, 279—316.
(1955) The inhomogeneous minima of binary quadratic forms III, *Acta Math., Stockh.*, **92**, 199—234.

Берч (Birch B. J.)
(1956) A transference theorem of the geometry of numbers, *J. Lond. Math. Soc.*, **31**, 248—251.
(1957) Transference theorems of the geometry of numbers, II, *Proc. Camb. Phil. Soc.* (в печати).

Блэни (Blaney H.)
(1950) Some asymmetric inequalities, *Proc. Camb. Phil. Soc.*, **46**, 359—376.

Ван дер Корпут (van der Corput J. G.)
(1931) Diophantische Ungleichungen. I, Zur Gleichverteilung modulo Eins, *Acta Math., Stockh.*, **56**, 373—456. II, Rythmische Systeme A und B, *Acta Math., Stockh.*, **59**, 209—328. (Обещанные части C и D еще не появились.)

Вейль (Weyl H.)
(1942) On geometry of numbers, *Proc. Lond. Math. Soc.* (2), **47**, 268—289.

Виноградов И. М.
(1947) Метод тригонометрических сумм в теории чисел, *Труды матем. ин-та им. В. А. Стеклова*, **23**, XXIII.

Гельфонд А. О.
(1941) О дробных долях линейных комбинаций полиномов и показательных функций, *Матем. сб.* (нов. сер.), 9, 721—726.
(1952) Трансцендентные и алгебраические числа, Гостехиздат, М.

Главка (Hlawka E.)
(1952) Zur Theorie des Figurengitters, *Math. Ann.*, **125**, 183—207.

(1954a) Zur Theorie der Überdeckung durch konvexe Körper, *Monatshefte Math. Phys.*, **58**, 287—291.

(1954b) Inhomogene Minima von Sternkörpern, *Monatshefte Math. Phys.*, **58**, 292—305.

Давенпорт (Davenport H.)

(1954) Simultaneous Diophantine approximation, *Proceedings International Conference of Mathematicians, Amsterdam*, **3**, 9—12.

(1955) On a theorem of Furtwängler, *J. Lond. Math. Soc.*, **30**, 186—195.

Давенпорт и Рот (Davenport H. and Roth K. F.)

(1955) Rational approximations to algebraic numbers, *Mathematika*, **2**, 160—167.

Дейвис (Davies C. S.)

(1950) The minimum of an indefinite binary quadratic form, *Quart. J.* (2), **1**, 241—242.

Диксон (Dickson L. E.)

(1930) Studies in the theory of numbers (especially chapter VII), *Chicago Univ. Press.*

Дюфренуа и Пизо (Dufresnoy J. and Pisot C.)

(1953) Sur un ensemble fermé d'entiers algébriques, *Ann. Sci. Éc. Norm. Sup., Paris* (3), **70**, 105—134.

Зигель (Siegel C. L.)

(1949) Transcendental numbers (Annals of Mathematics Studies, 16), *Princeton Univ. Press.*

Канагасабапатхи (Kanagasabapathy P.)

(1952) Note on Diophantine approximation, *Proc. Camb. Phil. Soc.*, **48**, 365—366.

Касселс (Cassels J. W. S.)

(1950a) Some metrical theorems in Diophantine approximation I, *Proc. Camb. Phil. Soc.*, **46**, 209—218.

(1950b) Some metrical theorems in Diophantine approximation III, *Proc. Camb. Phil. Soc.*, **46**, 219—225.

(1950c) Some metrical theorems in Diophantine approximation IV, *Proc. K. Ned. Akad. Wet. Amst.*, **53**, 176—187 (= *Indag. Math.*, 12, 14—25).

(1951) Some metrical theorems in Diophantine approximation V. On a conjecture of Mahler., *Proc. Camb. Phil. Soc.*, **47**, 18—21.

(1952a) The product of n inhomogeneous linear forms in n variables, *J. Lond. Math. Soc.*, **27**, 485—492.

(1952b) The inhomogeneous minimum of binary quadratic, ternary cubic and quaternary quartic forms, *Proc. Camb. Phil. Soc.*, **48**, 72—86, 519—520.

(1953) A new inequality with application to the theory of Diophantine approximation, *Math. Ann.*, **26**, 108—118.

(1954a) Über $\lim\limits_{x\to+\infty} x\,|\,\theta x+\alpha-y\,|$, *Math. Ann.*, **127**, 288—304.

(1954b) On the product of two inhomogeneous forms, *J. reine angew. Math.*, 193, 65—83.

(1955) Simultaneous Diophantine approximation II, *Proc. Lond. Math. Soc.* (3), 5, 435—448.

Касселс и Суиннертон-Дайер (Cassels J. W. S. and Swinnerton-Dyer H. P. F.)

(1955) On the product of three homogeneous linear forms and indefinite ternary quadratic forms, *Phil. Trans.* A, 248, 73—96.

Келли (Kelly J. B.)

(1950) A closed set of algebraic integers, *Amer. J. Math.*, 72, 565—572.

Кнезер (Kneser M.)

(1955) Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen, *Math. Z.*, 61, 429—434.

Коксма (Koksma J. F.)

(1936) Diophantische Approximationen. Ergebnisse d. Math. u. ihrer Grenzgebiete 4,4, Berlin und Leipzig.

(1937) Über einen Dirichlet-Minkowskischen Approximationssatz, *Mathematica B, Zutphen*, 6, 113—131, 171—181.

Кон (Cohn H.)

(1955) Approach to Markoff's minimal forms through modular functions, *Ann. Math., Princeton* (2), 61, 1—12.

Ландау (Landau E.)

(1927) Vorlesungen über Zahlentheorie (3 Bände), Leipzig.

Левек (Leveque W. J.)

(1953) Note on *S*-numbers, *Proc. Amer. Math. Soc.*, 4, 189—190.

Лутц (Lutz É.)

(1951) Sur les approximations diophantiennes linéaires *P*-adiques. Thèse, Strasbourg (= *Actualités Sci. Ind.*, 1224, 1955).

Малер (Mahler K.)

(1939a) Ein Übertragungsprinzip für lineare Ungleichungen, *Čas. Pěst. Mat.*, 68, 85—92.

(1939b) Ein Übertragungsprinzip für konvexe Körper, *Čas. Pěst. Mat.*, 68, 93—102.

(1946) On lattice points in *n*-dimensional star bodies. I. Existence theorems, *Proc. Roy. Soc.* A, 187, 151—187.

(1949) On the minimum determinant of a special point set, *Proc. K. Ned. Akad. Wet. Amst.*, 52, 633—642 (= *Indag. Math.*, 11, 195—204).

(1953a) On the approximation of logarithms of algebraic numbers, *Phil. Trans. A*, 245, 371—398.

(1953b) On the approximation of π, *Proc. K. Ned. Akad. Wet. Amst. A*, 56 (= *Indag. Math.*, 15), 29—42.

(1955) On compound convex bodies I, II, *Proc. Lond. Math. Soc.* (3), 5, 358—384.

Марков (Markoff A.)
(1879) Sur les formes quadratiques binaires indéfinies, *Math. Ann.*, **15**, 381—409.

Морделл (Mordell L. J.)
(1951) On the product of two non-homogeneous linear forms, IV, *J. Lond. Math. Soc.*, **26**, 93—95.

Перрон (Perron O.)
(1913) Die Lehre von den Kettenbrüchen, Leipzig und Berlin; 3rd edition, Stuttgart, 1954.
(1921) Irrationalzahlen, Berlin und Leipzig.

Пизо (Pisot C.)
(1946) Répartition (mod 1) des puissances successives des nombres réels, *Comm. Math. Helv.*, **19**, 153—160.

Понтрягин Л. С.
(1938) Непрерывные группы, изд. 2, Гостехиздат, М., 1954.

Пуату (Poitou G.)
(1953) Sur l'approximation des nombers complexes par les nombres des corps imaginaires quadratiques, etc., *Ann. Sci. Éc. Norm. Sup., Paris* (3), **70**, 199—265.

Ремак (Remak R.)
(1924) Über indefinite binäre quadratische Minimalformen, *Math. Ann.*, **92**, 155—182.
(1925) Über die geometrische Darstellung der indefiniten binären quadratischen Minimalformen, *Iber. Dtsch. MatVer.*, **33**, 228—245.

Роджерс (Rogers C. A.)
(1949) The product of the minima and the determinant of a set, *Proc. K. Ned. Akad. Wet. Amst.*, **52**, 256—263 (= *Indag. Math.*, **11**, 71—78).
(1954) The product of n non-homogeneous linear forms, *Proc. Lond. Math. Soc.* (3), **4**, 50—83.

Рот (Roth K. F.)
(1954) On irregularities of distribution, *Mathematika*, **1**, 73—79.
(1955) Rational approximations to algebraic numbers, *Mathematika*, **2**, 1—20 (with corrigendum p. 168).

Самет (Samet P. A.)
(1953) Algebraic integers with two conjugates outside the unit circle, I, II, *Proc. Camb. Phil. Soc.*, **49**, 421—436 and **50**, 346 (1954).

Сегре (Segre B.)
(1945) Lattice points in infinite domains and asymmetric diophantine approximations, *Duke Math. J.*, **12**, 337—365.

Сойер (Sawyer D. B.)
(1950) A note on the product of two non-homogeneous linear forms, *J. Lond. Math. Soc.*, **25**, 239—240.

Торнхейм (Tornheim L.)

(1955) Asymmetric minima of quadratic forms and asymmetric diophantine approximation, *Duke Math. J.*, 22, 287—294.

Туран (Turán P.)

(1953) Eine neue Methode in der Analysis und deren Anwendungen, Budapest.

Фробениус (Frobenius G.)

(1913) Über die Markoffschen Zahlen, *Preuss. Akad. Wiss. Sitzungsberichte*, 458—487.

Харди, Литтльвуд и Полиа (Hardy G. H., Littlewood J. E. and Pólya G.)

(1934) Inequalites, Cambridge: 2nd ed, 1952. [Имеется русский перевод: Харди Г. Х., Литтльвуд Дж. Е., Полиа Е., Неравенства, ИЛ, М., 1948.]

Харди и Райт (Hardy G. H. and Wright E. M.)

(1938) The Theory of Numbers, Oxford: 3rd ed., 1954.

Хинчин А. Я. (Khintchine A. Ya.)

(1923) Ein Satz über Kettenbrüche mit arithmetischen Anwendungen, *Math. Z.*, 18, 289—306.

(1926) Über eine Klasse linearer Diophantischer Approximationen, *Rendiconti Circ. Mat. Palermo*, 50, 170—195.

(1935) Цепные дроби (изд. 2, 1949).

(1948a) Количественная концепция аппроксимационной теории Кронекера, *Изв. АН СССР* (сер. матем.), 12, 113—122.

(1948b). Регулярные системы линейных уравнений и общая задача Чебышева, *Изв. АН СССР* (сер. матем.), 12, 249—258.

Холл (Hall M.)

(1947) On the sum and product of continued fractions, *Ann. Math., Princeton* (2), 48; 966—993.

Шаботи (Chabauty C.)

(1949) Sur les minima arithmétiques des formes, *Ann. Sci. Éc. Norm. Sup., Paris* (3), 66, 367—394.

Шаботи и Лутц (Chabauty C. and Lutz E.)

(1950) Sur les approximations linéaires réelles, *C. R. Acad. Sci., Paris*, 231, 938—939.

Шнейдер (Schneider T.)

(1956) Einführung in die transzendenten Zahlen, Berlin, Göttingen und Heidelberg.

Эрдёш и Туран (Erdös P. and Turán P.)

(1948) On a problem in the theory of uniform distribution (especially Theorem III), *Proc. K. Ned. Akad. Wet. Amst.*, **51**, 1146—1154, 1262—1269 (= *Indag. Math.*, **10**, 370—382; 406—413).

Ярник (Jarnìk V.)

(1946) Sur les approximations Diophantiques linéares non homogènes, *Bull. Intern. de l'Acad. Tchèque des Sciences*, 16.

(1954) К теории однородных линейных диофантовых приближений, *Чехословацкий матем. журн.*, **4** (79), 330—353.

ДОПОЛНЕНИЕ РЕДАКТОРА ПЕРЕВОДА

О ТЕОРЕМЕ МИНКОВСКОГО ДЛЯ ЛИНЕЙНЫХ ФОРМ И ТЕОРЕМАХ ПЕРЕНОСА

Существует много доказательств теоремы Минковского о линейных формах. Мы остановимся на доказательстве этой теоремы, принадлежащем К. Зигелю, получившему формулу, позволяющую установить также связь между числом точек решетки, попавших в параллелепипед, соответствующий данной системе линейных форм, и числом точек, попавших в параллелепипед, соответствующий системе обратных транспонированных форм.

Мы дадим здесь формулу К. Зигеля в несколько обобщенной форме, упростив при этом доказательство.

Пусть $\psi(x)$ будет функцией действительного x, $p \geqslant 1$ действительно и

$$\psi(x)=\begin{cases} x^P, & \text{если} \quad x \geqslant 0 \\ 0, & \text{если} \quad x \leqslant 0 \end{cases} \tag{1}$$

Пусть также

$$Y_k = Y_k(x_1, \ldots, x_q)=\sum_{n=s}^{q} a_{n,k}x_n, \quad k=1, \ldots, q, \tag{2}$$

будет система линейных форм с детерминантом $\Delta > 0$, а система линейных форм

$$Z_k=\sum_{n=1}^{q} A_{k,n}x_n = Z_k(x_1, \ldots, x_q), \quad k=1, \ldots, q,$$

будет обратной системой, транспонированной к данной системе (2). Другими словами, система

$$X_k=\sum_{n=1}^{q} A_{n,k}x_n, \quad k=1, \ldots, q,$$

будет обратной к (2). Тогда имеет место соотношение

$$\prod_{k=1}^{q} t_k^p + \sum_{x_1=-\infty}^{\infty} \cdots \sum_{x_q=-\infty}^{\infty}{}' \prod_{k=1}^{q} \psi[t_k - |Y_k(x_1, \ldots, x_q)] =$$

$$= \frac{\prod_1^q t_k^p}{\Delta} \left(\frac{2}{p+1}\right) \left[1 + \sum_{x_1=-\infty}^{\infty} \cdots \sum_{x_q=-\infty}^{\infty}{}' \prod_{k=1}^{q} \times \right.$$

$$\left. \times \frac{(p+1)p}{2\pi t_k |Z_k(x_1, \ldots, x_q)|} \int_0^1 (1-x)^{p-1} \sin 2\pi x t_k |Z_k| \, dx \right], \qquad (3)$$

$$t_k > 0, \qquad 1 \leqslant k \leqslant q,$$

где знак $'$ при многократных суммах означает пропуск точки $x_1 = \ldots = x_q = 0$; суммирование идет по всем целым $x_1, \ldots, x_q$, а линейные формы $y_k(x_1, \ldots, x_q)$ и $z_k(x_1, \ldots, x_q)$ — данная и обратная транспонированная системы. Интегралы в правой части при $p \geqslant 1$ неотрицательны. При $p = 1$ мы получаем формулу К. Зигеля

$$\prod_{k=1}^{q} t_k + \sum_{x_1=-\infty}^{\infty} \cdots \sum_{x_q=-\infty}^{\infty} \prod_{k=1}^{q} \psi[t_k - |Y_k(x_1, \ldots, x_q)|] =$$

$$= \frac{1}{\Delta} \prod_1^q t_k \cdot \left[1 + \sum_{x_1=-\infty}^{\infty} \cdots \sum_{x_q=-\infty}^{\infty} \prod_{k=1}^{q} \left[\frac{\sin \pi t_k z_k}{\pi t_k z_k}\right]^2 \right]. \qquad (4)$$

Из последней формулы следует непосредственно теорема Минковского относительно линейных форм. Действительно, из (4) следует неравенство

$$1 + \sum_{x_1=-\infty}^{\infty} \cdots \sum_{x_q=-\infty}^{\infty}{}' \prod \frac{\psi[t_k - |Y_k(x_1, \ldots, x_q)|]}{t_k} \geqslant \frac{t_1 \ldots t_k}{\Delta},$$

которое показывает, что если правая часть больше единицы, то сумма слева содержит хотя бы одно слагаемое, отличное от нуля. Другими словами, существует хотя бы один нетривиальный гиттерпункт. Существование гиттерпункта (нетривиального) в случае $|y_1| \leqslant t_1$, $|y_k| < t_k$, $t_1 \ldots t_q \geqslant \Delta$ следует непосредственно из конечности точек решетки в фиксированном объеме и возможности непрерывного изменения $t_1, \ldots, t_q$. Доказательство формулы (3) получится непосредственно, если функцию

$$\sum_{x_1=-\infty}^{\infty} \cdots \sum_{x_q=-\infty}^{\infty} \prod_{1}^{q} \psi\left[t_k - |Y_k(x_1+\alpha_1, \ldots, x_q+\alpha_q)|\right]$$

разложить в ряд Фурье по переменным $\alpha_1, \ldots, \alpha_q$ и после простого вычисления коэффициентов положить $\alpha_1 = \ldots = \alpha_q = 0$. Эти действия возможны в силу периодичности функции и того, что при $p \geqslant 1$ $\psi(x)$ удовлетворяет условиям Липшица с показателем 1. Положительность интегралов в правой части (3) при $p \geqslant 1$ следует из монотонного невозрастания $(1-x)^{p-1}$ и простейших свойств $\sin x$.

Из формулы К. Зигеля (4) легко следует теорема, дающая возможность получать различные теоремы переноса для однородного случая, в частности теорему А. Я. Хинчина.

Теорема I. *Пусть $q \geqslant 2$ — целое, система линейных форм $y_1, \ldots, y_q$ (2) от переменных $x_1, \ldots, x_q$ имеет детерминант $\Delta > 0$, система линейных форм $z_1, \ldots, z_q$ будет обратной транспонированной к системе форм $y_1, \ldots, y_q$ и $t_1, \ldots, t_q$ будут действительные и положительные числа. Тогда если существует нетривиальная точка целочисленной решетки $(x_1, \ldots, x_q)$, такая, что выполняются неравенства*

$$\left.\begin{aligned} t_k|z_k| &\leqslant \rho, \quad 1 \leqslant k \leqslant q, \\ 0 < \rho \leqslant \theta_q &\leqslant \frac{1}{\pi}\left(1 - \frac{1}{4q+1}\right)^{2q}\sqrt{\frac{6}{4q+1}} \end{aligned}\right\} \tag{5}$$

и одновременно

$$\prod_{1}^{q} t_k \geqslant \frac{\rho}{\theta_q}\Delta, \tag{6}$$

то существует нетривиальная целочисленная точка решетки, такая, что

$$|y_k| \leqslant t_k, \qquad k = 1, 2, \ldots, q.$$

Доказательство. Из формулы (4), оставляя в левой части единицу после деления на t, а в правой, кроме единицы, — только значения $(z_1, \ldots, z_q)$ для точек решетки $(x_1, \ldots, x_q), \ldots, (px_1, \ldots, px_q)$, $p = \left[\frac{1}{\pi\rho}\sqrt{\frac{6}{4q+1}}\right]$ и точек с обратными знаками координат, мы получаем неравенство

$$\frac{\prod\limits_{k=1}^{q} t_k}{\Delta}\left[1 + 2\sum_{n=1}^{p}\prod_{k=1}^{q}\left(\frac{\sin \pi n t_k z_k}{\pi n t_k z_k}\right)^2\right] >$$

$$> \frac{\prod\limits_{k=1}^{q} t_k}{\Delta}\left[1 + 2p\left(\frac{\sin \pi\rho p}{\pi\rho p}\right)^{2q}\right] >$$

$$> \frac{\prod\limits_{k=1}^{q} t_k}{\Delta}\left[\frac{2}{\pi\rho}\sqrt{\frac{6}{4q+1}}\left(\frac{\sin\sqrt{\frac{6}{4q+1}}}{\sqrt{\frac{6}{4q+1}}}\right)^{2q} - 1\right] >$$

$$> \frac{\prod\limits_{k=1}^{q} t_k}{\Delta}\left[\frac{2}{\pi\rho}\sqrt{\frac{6}{4q+1}}\left(1 - \frac{1}{4q+1}\right)^{2q} - 1\right] \geqslant \frac{\theta_q}{\rho\Delta}\prod_{k=1}^{q} t_k,$$

если для точки решетки $(x_1, \ldots, x_q)$ выполняются неравенства (5). Это неравенство противоречит условию (6) нашей теоремы, откуда и следует, что в левой части формулы (4) имеется не менее двух слагаемых. Этим теорема доказана.

Наша теорема является одной из общих форм теорем переноса в однородном случае. Рассмотрим частные случаи.

Две системы форм

$$\begin{aligned} &y_k = x_k, \quad 1 \leqslant k \leqslant q-1, \quad y_q = x_q + \sum_{k=1}^{q-1}\alpha_k x_k, \\ &z_k = x_k - \alpha_k x_q, \quad 1 \leqslant k \leqslant q-1, \quad z_q = x_q, \end{aligned} \tag{9}$$

где α_k — постоянные, связаны между собой тем, что одна из них является обратной транспонированной для другой, причем для этих форм $\Delta = 1$.

Применяя к этим системам форм нашу теорему, мы получаем теоремы переноса А. Я. Хинчина. Действительно, если существует для некоторой системы чисел $t_1, \ldots, t_q$, $\prod_{k=1}^{q} t_k \neq 0$ точка целочисленной решетки, такая, что

$$t_k |x_k| \leqslant \rho, \quad 1 \leqslant k \leqslant q-1; \quad t_q \left| x_q + \sum_{k=1}^{q-1} \alpha_k x_k \right| \leqslant \rho, \qquad \prod_1^q t_k \geqslant \frac{\rho}{\theta_q}, \tag{10}$$

то для некоторой точки решетки $(x_1', \ldots, x_q')$ верны неравенства

$$|x_k' - \alpha_k x_q'| \leqslant t_k, \quad 1 \leqslant k \leqslant q-1, \quad |x_q'| \leqslant t_q. \tag{11}$$

В частности, пусть для некоторой точки $(x_1, \ldots, x_q)$ и достаточно большого x

$$\left| x_q + \sum_{k=1}^{q-1} \alpha_k x_k \right| \leqslant x^{-q+1-\omega}, \quad |x_k| \leqslant x, \quad 1 \leqslant k \leqslant q-1,$$

где $\omega > 0$. Тогда, полагая

$$\rho = \theta_q^{-1/(q-1)} x^{-\omega/(q-1)}; \quad t_k = \frac{\rho}{x}, \quad 1 \leqslant k \leqslant q-1, \qquad t_q = x^{\omega(q-2)/(q-1)+q-1} \theta_q^{-1/(q-1)} = \rho x^{q-1+\omega}, \tag{12}$$

мы видим, что выполняются условия (10), а значит, верны неравенства (11); другими словами, неравенства

$$|x_k' - \alpha_k x_q'| < c_q y^{-\frac{q-1+\omega}{(q-1)^2+(q-2)\omega}}, \quad 1 \leqslant k \leqslant q-1,$$
$$|x_q'| \leqslant y, \quad y = \theta_q^{-1/(q-1)} x^{q-1+\omega(q-2)/(q-1)}, \tag{13}$$
$$c_q = \theta_q^{-\frac{q+\omega}{(q-1)^2+(q-2)\omega}}.$$

Это первая часть теоремы А. Я. Хинчина. Обратно, если существует точка решетки, для которой

$$t_k |x_k - \alpha_k x_q| \leqslant \rho, \quad 1 \leqslant k \leqslant q-1; \qquad t_q |x_q| \leqslant \rho, \quad \prod_{k=1}^{q} t_k \geqslant \frac{\rho}{\theta_q}, \tag{14}$$

то для некоторой точки решетки $(x'_1, \ldots, x'_q)$

$$\left|x'_q + \sum_{k=1}^{q} \alpha_k x'_k\right| \leqslant t_k; \quad |x'_k| \leqslant t_k, \quad 1 \leqslant k \leqslant q-1. \tag{15}$$

В частности, если для некоторой точки $(x_1, \ldots, x_q)$ и достаточно большого x

$$|x_k - \alpha_k x_q| \leqslant x^{-1/(q-1)-\omega}, \quad |x_q| \leqslant x, \quad 1 \leqslant k < q-1, \tag{16}$$

то существует точка $(x'_1, \ldots, x'_q)$, для которой

$$\left|\sum_{k=1}^{q-1} \alpha_k x'_k + x'_q\right| < c_q y^{-(q-1)(1+\omega)}, \quad |x'_k| \leqslant y, \tag{17}$$
$$1 \leqslant k \leqslant q-1, \quad y = \theta_q^{-1/(q-1)} x^{1/(q-1)}, \quad c_q = \theta_q^{-q/(q-1)-\omega}.$$

Это вторая часть теоремы А. Я. Хинчина, которая получается, если положить в неравенствах (14) и (15)

$$\rho = x^{-\omega} \theta_q^{-1/(q-1)}, \quad t_q = \frac{\rho}{x},$$
$$t_k = \rho x^{1/(q-1)+\omega} = \theta_q^{-1/(q-1)} x^{1/(q-1)}, \quad 1 \leqslant k \leqslant q-1.$$

Рассмотрим теперь другой частный пример. Пусть α — действительное положительное и иррациональное число. Две системы форм, у которых детерминант $\Delta = 1$,

$$\begin{gathered} y_k = x_k - \alpha x_{k+1}, \quad 1 \leqslant k \leqslant q-1; \quad y_q = x_q, \\ z_k = \alpha^{k-1} x_1 + \ldots + \alpha x_{k-1} + x_k, \quad 1 \leqslant k \leqslant q, \end{gathered} \tag{18}$$

являются обратными транспонированными друг для друга. Поэтому прямым следствием теоремы I является

Теорема I′. *Если существует отличная от начала точка целочисленной решетки $(x_1, \ldots, x_q)$, такая, что при заданных $t_1, \ldots, t_q$*

$$t_k \left|\sum_{s=1}^{k} \alpha^{k-s} x_s\right| \leqslant \rho, \quad 1 \leqslant k \leqslant q-1; \quad t_q \left|\sum_{s=1}^{q} \alpha^{q-s} x_s\right| \leqslant \rho,$$
$$\prod_{k=1}^{q} t_k \geqslant \frac{\rho}{\theta_q}, \tag{19}$$

где θ_q имеет прежнее значение, то существует нетривиальная точка решетки $(x'_1, \ldots, x'_q)$, такая, что

$$|x'_k - \alpha x'_{k+1}| \leqslant t_k, \quad 1 \leqslant k \leqslant q-1, \quad |x'_q| \leqslant t_q. \tag{20}$$

Опять, в частности, допуская, что для точки $(x_1, \ldots, x_q)$ верны неравенства

$$\left|\sum_{s=1}^{q} \alpha^{q-s} x_s\right| \leqslant x^{-q+1-\omega}, \quad \omega > 0;$$
$$\left|\sum_{s=1}^{k} \alpha^{k-s} x_s\right| \leqslant x, \quad 1 \leqslant k \leqslant q-1, \quad x > x_0, \tag{21}$$

и выбирая ρ и $t_1, \ldots, t_q$ по формулам (12), мы, так же как и выше, получаем, что верны неравенства

$$|x'_k - \alpha x'_{k+1}| < c_q y^{-\frac{q-1+\omega}{(q-1)^2+(q-2)\omega}},$$
$$1 \leqslant k \leqslant q-1; \quad |x'_q| < q, \tag{22}$$
$$y = \theta_q^{-1/(q-1)} x^{q-1+\omega(q-2)/(q-1)},$$

где c_q имеет прежнее значение. Обратно, из существования точки $(x_1, \ldots, x_q)$, для которой выполняются неравенства, аналогичные (14), именно

$$t_k |x_k - \alpha x_{k+1}| \leqslant \rho; \quad 1 \leqslant k \leqslant q-1;$$
$$t_q |x_q| \leqslant \rho, \quad \prod_{k=1}^{q} t_k \geqslant \frac{\rho}{\theta_q}, \tag{23}$$

следует существование точки для неравенств

$$\left|\sum_{k=1}^{q} \alpha^{q-k} x_k\right| \leqslant t_q; \quad \left|\sum_{s=1}^{k} \alpha^{k-s} x_s\right| \leqslant t_k, \quad 1 \leqslant k \leqslant q-1. \tag{24}$$

Снова из этой последней теоремы совершенно так же, как, и в случае А. Я. Хинчина, следует, что если есть точка $(x_1, \ldots, x_q)$, такая, что при $x > x_0$

$$|x_k - \alpha x_{k+1}| \leqslant x^{-1/(q-1)-\omega}, \quad |x| \leqslant^{b} x, \quad 1 \leqslant k \leqslant q-1, \tag{25}$$

то существует точка $(x_1', \ldots, x_q')$, для которой

$$\left|\sum_{k=1}^{q} \alpha^{q-k} x_k'\right| \leqslant c_q y^{-(q-1)(\omega+1)}; \quad \left|\sum_{s=1}^{k} \alpha^{k-s} x_s'\right| \leqslant y; \ 1 \leqslant k \leqslant q-1,$$

$$y = \theta_q^{-1/(q-1)} x^{1/(q-1)}, \quad c_q = \theta_q^{-q/(q-1)-\omega}.$$

Теорема I позволяет получить и другие частные следствия в виде конкретных теорем переноса.

ЛИТЕРАТУРА

1. Siegel K., Neuer Beweis des Satzes von Minkowski über lineare Formen, *Math. Ann.*, **87** (1922), 36—38.
2. Гельфонд А. О., Об одном обобщении неравенства Минковского, *Докл. АН СССР*, **17** (1937), 443—446.
3. Тамарин И. А., Об общих теоремах переноса А. Я. Хинчина, *Вестн. Моск. университета*, **12** (1951), 13—20.

ОГЛАВЛЕНИЕ

УКАЗАТЕЛЬ