З.И. Боревич, И.Р. Шафаревич

ТЕОРИЯ ЧИСЕЛ

З.И. Боревич, И.Р. Шафаревич

ТЕОРИЯ ЧИСЕЛ

З.И.Боревич, И.Р.Шафаревич

ТЕОРИЯ ЧИСЕЛ

М.: Наука. Главная редакция физико-математической литературы.— 1985.— 504 с., 3-е изд.доп.

Излагается ряд методов современной теории чисел. Изложение иллюстрируется рассмотрением большого - числа конкретных теоретико-числовых вопросов, относящихся главным образом к неопределенным уравнениям. Основное внимание уделено алгебраическим методам, но заметное место занимают также геометрический и аналитический методы. В третьем издании (второе вышло в 1972 г.) нашли отражение некоторые наиболее существенные новые результаты последнего десятилетия, примыкающие к излагаемым в книге вопросам.

Для студентов, аспирантов и научных работников, работающих в области алгебры и теории чисел.

ОГЛАВЛЕНИЕ

МОСКВА
«МИР»

ПРЕДИСЛОВИЕ

Развитие теории чисел состоит в переплетении двух тенденций. Первая из них — это создание общих концепций и теорий, таких, например, как понятие идеала или теория полей классов. Вторая тенденция состоит в обращении к конкретным числовым фактам. Ее влияние можно видеть в большом количестве теоретико-числовых результатов, которые были подсказаны и стимулированы эмпирическими наблюдениями, изучением таблиц. Именно соединение двух таких разнородных точек зрения определяет роль, которую теория чисел играет в математике: «мир чисел» наряду с физическим миром явился той почвой, на которой возникло большинство математических теорий.

В нашей книге мы хотели дать представление о том, как теория чисел возникает из синтеза этих двух тенденций. В связи с этим стилю изложения, при котором систематическое развертывание аппарата предшествует каким бы то ни было приложениям, мы предпочли более свободное изложение, при котором задачи и методы их решения тесно переплетаются. Исходным пунктом обычно являются конкретные задачи о целых числах. Общие теории возникают как аппарат для решения этих задач. Как правило, эти теории развиваются достаточно далеко для того, чтобы читатель мог составить себе представление об их красоте и стройности и научился их применять.

Вопросы, которые разбираются в книге, относятся главным образом к теории неопределенных уравнений, т. е. к теории решения в целых числах уравнений от нескольких неизвестных. Впрочем, рассматриваются и вопросы другого характера — примерами могут служить теорема Дирихле о простых числах в арифметической прогрессии или теоремы о росте числа решений сравнения.

Методы, которые мы излагаем, по преимуществу алгебраические. Точнее говоря, это теория конечных расширений полей и определенных в них метрик. Однако заметное место уделено аналитическим методам: им посвящена глава V, и к ним же следует отнести метод аналитических p-адических функций, изложенный в главе IV. Геометрические рассмотрения также играют большую роль в ряде мест.

Книга не предполагает у читателя больших знаний. Для понимания большей ее части вполне достаточно двух курсов университета и самых основ теории чисел: общей теории сравнений

и теории квадратичных вычетов до квадратичного закона взаимности. Только в последней главе используется несколько фактов из теории аналитических функций.

Необходимые сведения чисто алгебраического характера даны нами в «Алгебраическом дополнении», помещенном в конце книги. В нем даны точные определения, формулировки, а иногда и доказательства всего того, что может встретиться в книге и в то же время не входит в университетский курс высшей алгебры.

Третье издание книги отличается от предыдущих (вышедших в 1964 и 1972 годах) рядом дополнений, в которых мы попытались отразить достижения последних лет. Внесены наиболее существенные результаты, связанные с вопросами, излагаемыми в книге. Значительно расширены таблицы.

Мы глубоко благодарны Дмитрию Константиновичу Фаддееву за многочисленные и очень полезные беседы, за ряд ценных советов и замечаний.

Авторы

Глава I

СРАВНЕНИЯ

Эта глава посвящена теории сравнений и ее приложениям к неопределенным уравнениям. Связь между неопределенными уравнениями и сравнениями основывается на том простом замечании, что если неопределенное уравнение

$$F(x_1, \ldots, x_n) = 0, \tag{1}$$

где F — многочлен с целыми коэффициентами, имеет решение в целых числах, то сравнение

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{m} \tag{2}$$

разрешимо при любом модуле m. Так как вопрос о разрешимости сравнения всегда можно решить хотя бы методом перебора, ввиду конечности числа классов вычетов, то это дает нам серию эффективных необходимых условий для разрешимости уравнения (1) в целых числах.

Гораздо сложнее вопрос о достаточности этих условий. Утверждение: «неопределенное уравнение разрешимо тогда и только тогда, когда оно разрешимо как сравнение по любому модулю» неверно в общем случае (см., например, задачу 4), но справедливо для некоторых частных классов уравнений. Так, в этой главе мы докажем его для случая, когда F — форма второй степени, присоединив при этом к нашим условиям еще одно очевидным образом необходимое требование — разрешимость уравнения (1) в вещественных числах. (Заметим, что если F — форма, то под разрешимостью уравнения $F = 0$ понимают существование ненулевого решения.)

Основное понятие, которое мы будем в этой главе сначала изучать, а потом применять к теории сравнений и неопределенных уравнений,— это p-адические числа. Их роль в рассматриваемом вопросе заключается в следующем. Из элементарной теории чисел известно, что для модуля $m = p_1^{k_1} \ldots p_r^{k_r}$ ($p_1, \ldots, p_r$ — различные простые числа) разрешимость сравнения (2) равносильна разрешимости сравнений

$$F(x_1, \ldots, x_n) \equiv 0 \left(\mathrm{mod}\ p_i^{k_i}\right)$$

для всех $i = 1, \ldots, r$. Таким образом, разрешимость сравнений

(2) для всех модулей m эквивалентна разрешимости этих сравнений только для модулей, являющихся степенями простых чисел. Зафиксируем простое число p и поставим вопрос о разрешимости сравнений

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p^k} \tag{3}$$

для всех натуральных показателей k. В связи с этой задачей Хензель построил для каждого простого числа p новый вид чисел, названных им p-адическими, и доказал, что разрешимость сравнений (3) для всех k равносильна разрешимости уравнения (1) в p-адических числах. В силу этого отмеченная нами связь между сравнениями (2) и (3) позволяет сказать, что разрешимость сравнений (2) по всем модулям m равносильна разрешимости уравнения (1) в p-адических числах для всех простых чисел p.

Используя понятие p-адического числа, можно, следовательно, упомянутой нами теореме о формах второй степени придать следующую формулировку (ее доказательство и является целью настоящей главы): если $F(x_1, \ldots, x_n)$ — целочисленная квадратичная форма, то уравнение (1) разрешимо в целых числах тогда и только тогда, когда оно разрешимо в p-адических числах для всех p и в вещественных числах.

В формулировке этой теоремы, называемой теоремой Минковского — Хассе, и во многих других вопросах p-адические числа появляются на равных правах с вещественными. Если вещественные числа необходимы для изучения рациональных чисел с точки зрения их величины, то p-адические числа играют совершенно аналогичную роль в вопросах, связанных с делимостью на степень простого числа p. Аналогия между p-адическими и вещественными числами проявляется и в другом отношении. Оказывается, что p-адические числа могут быть построены, исходя из рациональных, при помощи той же самой конструкции, при помощи которой строятся вещественные числа: путем присоединения пределов фундаментальных последовательностей. То, что мы приходим при этом к разным видам чисел, объясняется различными положенными в основу понятиями сходимости.

Сделаем еще одно замечание. Если F — форма, то разрешимость уравнения (1) в целых числах эквивалентна, конечно, его разрешимости в произвольных рациональных числах. В силу этого в теореме Минковского — Хассе можно говорить о рациональной разрешимости вместо целочисленной. Этот очевидный факт приобретает значение благодаря тому, что для случая, когда F — произвольный многочлен второй степени, аналогичная теорема сохраняется лишь при условии, что речь идет о разрешимости уравнения в рациональных числах. В связи с этим при изучении неопределенных уравнений второй степени мы будем рассматривать не только целочисленные, но и рациональные решения.

Задачи

1. Доказать, что уравнение $15x^2 - 7y^2 = 9$ не имеет решения в целых числах.

2. Доказать, что уравнение $5x^3 + 11y^3 + 13z^3 = 0$ не имеет других решений в целых числах, кроме $x = 0$, $y = 0$, $z = 0$.

3. Доказать, что целое число вида $8n + 7$ не может быть представлено в виде суммы квадратов трех целых чисел.

4. Используя свойства символа Лежандра, доказать, что сравнение $(x^2 - 13)(x^2 - 17)(x^2 - 221) \equiv 0 \pmod m$ разрешимо при любом модуле m. Очевидно, что уравнение $(x^2 - 13)(x^2 - 17)(x^2 - 221) = 0$ неразрешимо в целых числах.

5. Доказать, что неопределенное уравнение $a_1x_1 + \ldots + a_nx_n = b$ с целыми $a_1, \ldots, a_n, b$ разрешимо в целых числах тогда и только тогда, когда разрешимо соответствующее сравнение по любому модулю m.

6. Доказать аналогичное утверждение для системы целочисленных линейных уравнений.

§ 1. Сравнения по простому модулю

1. Суммы степеней вычетов. Мы начнем с рассмотрения сравнений по простому модулю p. Классы вычетов по модулю p образуют, как известно, конечное поле из p элементов (мы его будем обозначать через $\mathbb{F}_p$), и всякое сравнение по модулю p можно рассматривать как равенство в этом поле. Решение сравнений по модулю p равносильно, следовательно, решению уравнений в поле $\mathbb{F}_p$. Поле $\mathbb{F}_p$ является только одним из примеров конечного поля. Все рассуждения этого параграфа буквально переносятся и на случай любого конечного поля (см. задачи 5 и 6). Мы ограничимся, однако, случаем поля $\mathbb{F}_p$ и будем вместо равенств писать сравнения. Только для построения примера к теореме 3 мы должны будем привлечь другие конечные поля.

При изучении вопроса о числе решений сравнений по простому модулю важную роль играет следующий простой факт.

Теорема 1. *Пусть m — натуральное число. Сумма*

$$S = \sum_{x \bmod p} x^m,$$

в которой x пробегает полную систему вычетов по модулю p, сравнима по модулю p с -1, если m делится на $p-1$, и сравнима с 0, если m не делится на $p-1$.

Доказательство. Значение $x \equiv 0 \pmod p$ в сумме S можно, разумеется, опустить. Пусть $p-1$ делит m. Так как $x^{p-1} \equiv 1 \pmod p$ для всякого x, не делящегося на p, то в этом случае $x^m \equiv 1 \pmod p$, и, следовательно, $S \equiv p-1 \equiv -1 \pmod p$. Пусть теперь $p-1$ не делит m. Тогда существует такое число a, не делящееся на p, что $a^m \not\equiv 1 \pmod p$ (в качестве a можно взять первообразный корень по модулю p). Так как вместе с x произведение ax также будет пробегать полную систему вычетов по

модулю p, то

$$a^m S = \sum_{x \bmod p} (ax)^m \equiv S \pmod p,$$

откуда $(a^m - 1)S \equiv 0 \pmod p$, и, следовательно, $S \equiv 0 \pmod p$.

Следствие. *Пусть $\Phi(x_1, \ldots, x_n)$ — целочисленный многочлен степени меньшей, чем $n(p-1)$. Тогда*

$$\sum_{x_1, \ldots, x_n} \Phi(x_1, \ldots, x_n) \equiv 0 \pmod p. \qquad (1)$$

где в сумме слева $x_1, \ldots, x_n$ независимо друг от друга пробегают полную систему вычетов по модулю p.

Доказательство. Достаточно рассмотреть случай, когда Φ есть одночлен $x_1^{k_1} \ldots x_n^{k_n}$. Имеем

$$\sum_{x_1, \ldots, x_n} x_1^{k_1} \ldots x_n^{k_n} = \left(\sum_{x_1} x_1^{k_1}\right) \ldots \left(\sum_{x_n} x_n^{k_n}\right).$$

По условию $k_1 + \ldots + k_n < n(p-1)$, поэтому хоть при одном i выполнены неравенства $0 \leqslant k_i < p-1$. Следовательно, хоть одна из сумм справа будет $\equiv 0 \pmod p$ (в случае $k = 0$ все слагаемые x^0 равны 1, включая $x = 0$, поэтому $\sum_x x^0 \equiv 0 \pmod p$.)

Замечание. Мультипликативная группа поля $\mathbb{F}_p$ есть циклическая группа порядка $p-1$ (ее образующим элементом является класс вычетов, содержащий первообразный корень по модулю p). Сумму в теореме 1 можно поэтому интерпретировать как сумму m-х степеней всех (содержащихся в $\mathbb{F}_p$) корней степени $p-1$ из 1. Если $(p-1, m) = d$, то такая сумма распадается на d сумм, каждая из которых равна сумме всех корней степени $(p-1)/d$ из 1. Утверждение теоремы 1 является по существу следствием того факта, что сумма всех корней степени r из 1 равна 1 при $r = 1$ и равна 0 при $r \geqslant 2$.

2. Теоремы о числе решений сравнений. Результаты п. 1 мы применим к доказательству следующего утверждения.

Теорема 2 (теорема Варнинга). *Если степень r целочисленного многочлена $F(x_1, \ldots, x_n)$ меньше числа переменных n, то число решений сравнения $F(x_1, \ldots, x_n) \equiv 0 \pmod p$ делится на p.*

Доказательство. Пусть N обозначает число решений сравнения $F \equiv 0 \pmod p$. Рассмотрим многочлен

$$\Phi(x_1, \ldots, x_n) = 1 - F(x_1, \ldots, x_n)^{p-1},$$

степень которого меньше чем $n(p-1)$. Если $F(a_1, \ldots, a_n) \equiv 0 \pmod p$, то

$$\Phi(a_1, \ldots, a_n) \equiv 1 \pmod p.$$

Если же $F(a_1, \ldots, a_n) \not\equiv 0 \pmod p$, то

$$\Phi(a_1, \ldots, a_n) \equiv 0 \pmod p.$$

Суммируя все значения $\Phi(x_1, \ldots, x_n)$, когда $x_1, \ldots, x_n$ независимо друг от друга пробегают полную систему вычетов по модулю p, мы получим, следовательно, сравнение

$$\sum_{x_1, \ldots, x_n} \Phi(x_1, \ldots, x_n) \equiv N \pmod{p}.$$

Теорема 2 следует теперь из сравнения (1).

Теорема 3 (теорема Шевалле). *Если $F(x_1, \ldots, x_n)$ — форма степени $r < n$, то сравнение*

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p}$$

имеет нетривиальное решение.

Доказательство. Так как в случае однородного многочлена F степени $r \geqslant 1$ всегда имеется тривиальное решение $x_i \equiv 0 \pmod{p}$, то для числа решений N сравнения $F \equiv 0 \pmod{p}$ имеем неравенство $N \geqslant 1$. С другой стороны, по теореме Варнинга $N \equiv 0 \pmod{p}$. Следовательно, $N \geqslant p \geqslant 2$.

Докажем для полноты картины, что неравенство $r < n$ нельзя заменить более слабым так, чтобы теорема Шевалле оставалась верной. Для этого построим для любого n форму $F(x_1, \ldots, x_n)$ степени n такую, что сравнение

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p} \tag{2}$$

имеет только нулевое решение.

Мы воспользуемся тем фактом, что для любого $n \geqslant 1$ существует конечное поле Σ из p^n элементов, содержащее $\mathbb{F}_p$ в качестве подполя (см. Дополнение, § 3, теорема 2). Пусть $\omega_1, \ldots, \omega_n$ — базис поля Σ над $\mathbb{F}_p$. Рассмотрим линейную форму $x_1\omega_1 + \ldots + x_n\omega_n$, в которой под $x_1, \ldots, x_n$ будем понимать произвольные значения из $\mathbb{F}_p$. Ее норма $N_{\Sigma/\mathbb{F}_p}(x_1\omega_1 + \ldots + x_n\omega_n) = \varphi(x_1, \ldots, x_n)$ *является, очевидно, формой степени n от $x_1, \ldots, x_n$ с коэффициентами из поля $\mathbb{F}_p$.* Из определения нормы $N(\alpha)$ (см. Дополнение, § 2, п. 2) элемента $\alpha = x_1\omega_1 + \ldots + x_n\omega_n$ $(x_i \in \mathbb{F}_p)$ следует, что равенство $N(\alpha) = 0$ возможно только при $\alpha = 0$, т. е. только при $x_1 = 0, \ldots, x_n = 0$. Форма φ обладает, стало быть, тем свойством, что уравнение $\varphi(x_1, \ldots, x_n) = 0$ имеет в поле $\mathbb{F}_p$ только нулевое решение. Заменим теперь каждый коэффициент формы φ, являющийся классом вычетов по модулю p, каким-нибудь вычетом из этого класса. Мы получим целочисленную форму $F(x_1, \ldots, x_n)$ степени n от n переменных, и для этой формы F сравнение (2) будет, очевидно, иметь лишь нулевое решение.

Теорема 4. *Пусть $F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)$ — целочисленные многочлены степеней $r_1, \ldots, r_m$ соответственно. Если $r_1 + \ldots + r_m < n$, то число решений N системы сравнений*

$$F_1(x_1, \ldots, x_n) \equiv 0 \pmod{p},$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$F_m(x_1, \ldots, x_n) \equiv 0 \pmod{p}$$

делится на p.

Доказательство. Рассмотрим многочлен

$$\Phi(x_1, \ldots, x_n) = \prod_{i=1}^{m} (1 - F_i(x_1, \ldots, x_n)^{p-1})$$

степени $(r_1 + \ldots + r_m)(p-1) < n(p-1)$. Так же как и при доказательстве теоремы 2, убеждаемся в том, что

$$\sum_{x_1, \ldots, x_n} \Phi(x_1, \ldots, x_n) \equiv N \pmod{p},$$

а значит, ввиду (1) $N \equiv 0 \pmod{p}$.

Замечание. Теорема Варнинга допускает следующее обобщение [56]. Пусть $F(x_1, \ldots, x_n)$ — многочлен степени $r < n$ с коэффициентами из конечного поля $\Sigma = GF(q)$, $q = p^m$, и a — наибольшее натуральное число, для которого $a < n/r$. Тогда число $N(F)$ решений уравнения $F(x_1, \ldots, x_n) = 0$ в поле Σ делится на q^a. При этом показатель ma в сравнении $N(F) \equiv 0 \pmod{p^{ma}}$ в общем случае не может быть увеличен. Именно, для фиксированных r и n (с условием $r < n$) существует многочлен $F_0 \in \Sigma[x_1, \ldots, x_n]$ степени r, для которого $N(F_0) \not\equiv 0 \pmod{p^{ma+1}}$. С другой стороны, имеет место следующий факт. Если уравнение $F(x_1, \ldots, x_n) = 0$ имеет в поле Σ хоть одно решение, то $N(F) \geqslant q^{n-r}$ [143].

3. Квадратичные формы по простому модулю. Применим полученные нами результаты к случаю квадратичных форм. Следующий факт непосредственно вытекает из теоремы Шевалле.

Теорема 5. *Пусть $f(x_1, \ldots, x_n)$ — целочисленная квадратичная форма. Если $n \geqslant 3$, то сравнение*

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{p}$$

имеет ненулевое решение.

Случай квадратичных форм от одной переменной не представляет интереса (если $a \not\equiv 0 \pmod{p}$, то сравнение $ax^2 \equiv 0 \pmod{p}$ имеет только нулевое решение).

Рассмотрим оставшийся случай бинарных квадратичных форм.

Мы будем считать, что $p \neq 2$ (при $n = 2$, $p = 2$ легко непосредственно перебрать все имеющиеся квадратичные формы). В этом случае форма может быть записана в виде

$$f(x, y) = ax^2 + 2bxy + cy^2.$$

Ее определитель $ac - b^2$ мы обозначим через d.

Теорема 6. *Сравнение*

$$f(x, y) \equiv 0 \pmod{p}, \qquad p \neq 2, \tag{3}$$

тогда и только тогда имеет ненулевое решение, когда $-d$ или делится на p, или является квадратичным вычетом по модулю p.

Доказательство. Очевидно, что для двух форм f и f_1, эквивалентных в поле $\mathbb{F}_p$ (см. Дополнение, § 1, п. 1), сравнения

(3) либо одновременно имеют, либо одновременно не имеют ненулевое решение. Так как, сверх того, при переходе к эквивалентной форме ее определитель умножается на квадрат ненулевого элемента поля $\mathbb{F}_p$, то мы можем и в доказательстве теоремы 6 заменить форму f любой, ей эквивалентной. Всякая форма эквивалентна диагональной форме (Дополнение, § 1, теорема 3); мы можем поэтому считать, что

$$f = ax^2 + cy^2, \quad d = ac.$$

Если $a \equiv 0$ или $c \equiv 0 \pmod p$, то теорема очевидна. Если же $ac \not\equiv 0 \pmod p$ и сравнение (3) имеет ненулевое решение (x_0, y_0), то из сравнения

$$ax_0^2 + cy_0^2 \equiv 0 \pmod p$$

получаем

$$-ac \equiv \left(\frac{cy_0}{x_0}\right)^2 \pmod p$$

(дробь $w \equiv \frac{u}{v} \pmod p$ означает результат деления в поле $\mathbb{F}_p$ т. е. решение сравнения $vw \equiv u \pmod p$). Таким образом, $\left(\frac{-d}{p}\right) = 1$. Наоборот, если $\left(\frac{-d}{p}\right) = 1$ и $-ac \equiv u^2 \pmod p$, то мы можем положить $(x_0, y_0) = (u, a)$.

Задачи

1. Пусть $F(x_1, \ldots, x_n)$ — целочисленный многочлен степени $r < n(p-1)$. Положим $a = n - \left[\frac{r}{p-1}\right]$. Доказать, что сумма $\sum_{x_1, \ldots, x_n} F(x_1, \ldots, x_n)$, в которой $x_1, \ldots, x_n$ независимо друг от друга пробегают полную систему вычетов по модулю p, делится на p^a.

2. Пусть $1 \leqslant n \leqslant p-1$, и пусть $a_1, \ldots, a_n$ — произвольные целые числа. Построить целочисленный многочлен $f(x_1, \ldots, x_n)$ степени $p-1$, для которого сравнение $f \equiv 0 \pmod p$ имеет единственное решение $x_i \equiv a_i \pmod p$, $1 \leqslant i \leqslant n$.

3. Определить число решений сравнения $x^3 + y^3 + z^3 + u^3 \equiv 0 \pmod 7$.

4. Построить кубическую форму $F(x_1, x_2, x_3)$, для которой сравнение $F(x_1, x_2, x_3) \equiv 0 \pmod 2$ имеет только нулевое решение.

5. Пусть Σ — конечное поле характеристики p, содержащее $q = p^n$ элементов. Для $m \geqslant 1$ положим

$$S(m) = \sum_{\xi \in \Sigma} \xi^m.$$

Доказать, что сумма $S(m)$ равна -1, если m делится на $q-1$, и равна нулю в противном случае.

6. Пусть $F(x_1, \ldots, x_n)$ — многочлен степени $r < n$ с коэффициентами из конечного поля Σ характеристики p. Доказать, что число решений уравнения $F(x_1, \ldots, x_n) = 0$ в поле Σ делится на p. Доказать далее, что число

решений системы

$$F_1(x_1, \ldots, x_n) = 0,$$
$$\ldots\ldots\ldots$$
$$F_m(x_1, \ldots, x_n) = 0$$

в поле Σ делится на p, если только степени $r_1, \ldots, r_m$ многочленов $F_1, \ldots, F_m$ (с коэффициентами из Σ) удовлетворяют условию $r_1 + \ldots + r_m < n$.

7. Доказать, что если f — квадратичная форма в поле $\mathbb{F}_p$ ранга $\geqslant 2$ и $a \not\equiv 0 \pmod p$, то сравнение $f \equiv a \pmod p$ разрешимо.

8. Используя теоремы 2 и 3 § 1 Дополнения, доказать, что две неособенные квадратичные формы в поле $\mathbb{F}_p$, $p \neq 2$, эквивалентны тогда и только тогда, когда произведение их определителей является квадратом.

9. Определить группу классов Витта квадратичных форм в поле $\mathbb{F}_p$, $p \neq 2$ (см. задачу 5 § 1 Дополнения).

10. Доказать, что число ненулевых решений сравнения $f(x, y) \equiv 0 \pmod p$, где $f(x, y)$ — квадратичная форма с определителем $d \not\equiv 0 \pmod p$, равно $(p-1)\left(1 + \left(\frac{-d}{p}\right)\right)$.

11. Используя теорему 7 § 1 Дополнения, доказать, что для квадратичной формы $f(x_1, \ldots, x_n)$ с определителем $d \not\equiv 0 \pmod p$ при $p \neq 2$ число ненулевых решений сравнения $f(x_1, \ldots, x_n) \equiv 0 \pmod p$ равно

$$p^{n-1} - 1 + (p-1)\left(\frac{(-1)^{n/2}d}{p}\right)p^{\frac{n}{2}-1} \quad \text{при } n \text{ четном},$$
$$p^{n-1} - 1 \quad \text{при } n \text{ нечетном}.$$

12. В предположении задачи 11 найти число решений сравнения $f(x_1, \ldots, x_n) \equiv a \pmod p$.

§ 2. Тригонометрические суммы

1. Сравнения и тригонометрические суммы. В этом параграфе (как и в предшествующем) также будут рассматриваться сравнения по простому модулю p, однако с несколько иной точки зрения. В теоремах § 1 делались определенные заключения о числе решений сравнения в зависимости от степени многочлена и числа его переменных. Здесь же главную роль будет играть величина простого модуля p.

В начале главы мы говорили, что для разрешимости неопределенного уравнения $F(x_1, \ldots, x_n) = 0$ необходимо, чтобы для всех модулей m были разрешимы сравнения $F \equiv 0 \pmod m$. Даже если мы ограничимся рассмотрением только простых модулей m, то и в этом случае мы будем иметь бесконечно много необходимых условий. Ясно, что эти условия могут быть полезны лишь в том случае, если у нас будет финитный (использующий конечное число действий) способ для их фактической проверки. Оказывается, что для одного весьма важного класса многочленов такой способ (и притом очень простой) существует. Именно, при заданном целочисленном многочлене F из этого класса сравнения $F \equiv 0 \pmod p$ автоматически разрешимы для всех модулей p,

бо́льших некоторой границы. Многочлены, о которых идет речь, выделяются следующим определением.

Определение. *Многочлен $F(x_1, \ldots, x_n)$ с рациональными коэффициентами называется абсолютно неприводимым, если он не может быть разложен на нетривиальные множители ни в каком расширении поля рациональных чисел.*

Имеет место следующая фундаментальная

Теорема А. *Если $F(x_1, \ldots, x_n)$ — абсолютно неприводимый многочлен с целыми коэффициентами, то сравнение*

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p} \tag{1}$$

разрешимо для всех простых чисел p, бо́льших некоторой границы, зависящей только от многочлена F.

Аналогичный результат справедлив и для ненулевых решений, если рассматривать однородный многочлен F, а также для системы сравнений (при надлежащем понимании абсолютной неприводимости).

При $n = 1$ теорема А тривиальна (всякий многочлен от одной переменной степени выше первой приводим в поле комплексных чисел, а для многочленов первой степени утверждение очевидно). Но уже при $n = 2$ для ее доказательства потребовалось привлечение глубоких методов алгебраической геометрии. Впервые доказательство теоремы А для $n = 2$ было получено в 1948 г. А. Вейлем [39]. Наилучшие из имеющихся сейчас вариантов доказательств этой теоремы содержатся в книге С. Ленга [29] и в работе [107]. Элементарное доказательство без использования средств алгебраической геометрии (правда, при некотором ограничении на многочлен $F(x, y)$) получено в 1972 г. С. А. Степановым [51]. Изложение его метода для произвольного $F(x, y)$ с привлечением минимальных сведений из алгебраической геометрии приведено в работе Бомбьери [65]. Переход от $n = 2$ к произвольному случаю оказался намного проще. Это сделано в работах [48] и [94].

В упомянутых работах доказано на самом деле гораздо больше, чем утверждается в теореме А. Именно, в них показано, что если фиксировать многочлен F и менять простой модуль p, то число решений N сравнения (1) будет стремиться к бесконечности при неограниченном увеличении p и даже оценена скорость возрастания N. Точная формулировка этого результата выглядит следующим образом.

Теорема В. *Для числа $N(F, p)$ решений сравнения* (1) *выполняется неравенство*

$$|N(F, p) - p^{n-1}| < C(F)p^{n-1-1/2},$$

где константа $C(F)$ зависит только от многочлена F и не зависит от p.

Единственный известный сейчас способ доказательства теоремы A — это выведение ее из теоремы B. Для доказательства же теоремы B требуется алгебраический аппарат гораздо более сложный, чем тот, которым мы пользуемся в этой книге. Поэтому мы не можем привести здесь доказательства теорем A и B, но вместо этого изложим метод, при помощи которого удается получить теоремы в частных случаях, и разберем один такой частный случай.

Все наши рассуждения будут основываться на том, что для числа решений сравнения (1) можно дать «явную формулу», точнее говоря, представить это число как сумму некоторых корней степени p из единицы. Суммы такого вида называются тригонометрическими.

Условимся о следующих обозначениях. Для комплекснозначных функций $f(x)$ или $f(x_1, \ldots, x_n)$, значения которых зависят только от классов вычетов целых чисел x, x_1, ..., x_n по модулю p, через $\sum\limits_x f(x)$ и $\sum\limits_{x_1,\ldots,x_n} f(x_1, \ldots, x_n)$ мы будем обозначать суммы, распространенные на все значения x или x_1, ..., x_n из полной системы вычетов по модулю p, а через $\sum\limits_x{}' f(x)$ — сумму, распространенную на все значения x из приведенной системы вычетов.

Пусть ζ — некоторый фиксированный первообразный корень степени p из 1. Тогда, как легко видеть,

$$\sum_x \zeta^{xy} = \begin{cases} p & \text{при } y \equiv 0 \pmod p, \\ 0 & \text{при } y \not\equiv 0 \pmod p. \end{cases} \tag{2}$$

Эти равенства и дают возможность найти «явную формулу» для числа решений сравнения (1).

Рассмотрим сумму $S = \sum\limits_{x_1,\ldots,x_n} \sum\limits_x \zeta^{xF(x_1,\ldots,x_n)}$. Если значения x_1, ..., x_n дают решение сравнения (1), то согласно (2)

$$\sum_x \zeta^{xF(x_1,\ldots,x_n)} = p.$$

Сумма всех таких членов, входящих в S, равна Np, где N — число решений сравнения (1). Если же $F(x_1, \ldots, x_n) \not\equiv 0 \pmod p$, то по второй части формулы (2)

$$\sum_x \zeta^{xF(x_1,\ldots,x_n)} = 0.$$

Сумма всех таких членов в S поэтому равна нулю, и мы получаем, что $S = Np$. Нами доказана, таким образом,

Теорема 1. *Для числа N решений сравнения* (1) *имеет место формула*

$$N=\frac{1}{p}\sum_{x,x_1,\ldots,x_n}\zeta^{xF(x_1,\ldots,x_n)}. \tag{3}$$

Выделим в сумме (3) все слагаемые, для которых $x\equiv 0 \pmod p$. Так как каждое такое слагаемое равно 1, а число их равно p^n (каждый из аргументов $x_1, \ldots, x_n$ независимо друг от друга принимает p значений), то

$$N = p^{n-1} + \frac{1}{p}\sum_{x}{}' \sum_{x_1,\ldots,x_n}\zeta^{xF(x_1,\ldots,x_n)}. \tag{4}$$

В этом виде формула для N уже подсказывает теорему В. Из числа N уже выделен член p^{n-1}. Надо только доказать (но в этом и состоит вся трудность!), что при возрастании p сумма всех остальных слагаемых по модулю растет медленнее этого главного члена.

2. Суммы степеней. Общие соображения, изложенные в п. 1, мы применим к случаю, когда многочлен F равен сумме степеней переменных, т. е.

$$F(x_1, \ldots, x_n) = a_1x_1^{r_1} + \ldots + a_nx_n^{r_n}, \quad a_i \not\equiv 0 \pmod p.$$

Мы будем предполагать, что $n \geqslant 3$, так как при $n=1$ и $n=2$ число решений сравнения $F\equiv 0 \pmod p$ находится очевидным образом.

Согласно формуле (4) число N решений сравнения $a_1x_1^{r_1} + \ldots + a_nx_n^{r_n} \equiv 0 \pmod p$ выражается равенством

$$N = p^{n-1} + \frac{1}{p}\sum_{x}{}' \sum_{x_1,\ldots,x_n}\zeta^{x\left(a_1x_1^{r_1}+\ldots+a_nx_n^{r_n}\right)},$$

которое может быть переписано также в виде

$$N = p^{n-1} + \frac{1}{p}\sum_{x}{}' \prod_{i=1}^{n}\sum_{x_i}\zeta^{a_ixx_i^{r_i}}. \tag{5}$$

Полученная формула приводит нас к необходимости исследования сумм вида $\sum\limits_{y}\zeta^{ay^r}$ $(a \not\equiv 0 \pmod p)$. Легко видеть, что

$$\sum_{y}\zeta^{ay^r} = \sum_{x} m(x)\,\zeta^{ax}, \tag{6}$$

где $m(x)$ равно числу решений сравнения $y^r \equiv x \pmod p$ относительно y. Очевидно также, что $m(0) = 1$. Найдем $m(x)$ в явном виде при $x \not\equiv 0 \pmod p$.

Если g — некоторый первообразный корень по модулю p, то

$$x \equiv g^k \pmod{p}, \tag{7}$$

где показатель k однозначно определен по модулю $p-1$. Пусть $y \equiv g^u \pmod{p}$. Сравнение $y^r \equiv x \pmod{p}$ равносильно, очевидно, сравнению

$$ru \equiv k \pmod{p-1}. \tag{8}$$

Согласно общей теории сравнений первой степени сравнение (8) имеет $d=(r, p-1)$ решений относительно u или не имеет ни одного решения в зависимости от того, будет ли k делиться на d или нет. Следовательно,

$$m(x) = \begin{cases} d, & \text{если } k \equiv 0 \pmod{d}, \\ 0, & \text{если } k \not\equiv 0 \pmod{d}. \end{cases} \tag{9}$$

Дадим для числа $m(x)$ другую, более удобную в аналитическом отношении формулу. Выберем для этого первообразный корень ε степени d из 1 и определим на целых числах x, взаимно простых с p, функции χ_s ($s=0, 1, \ldots, d-1$), полагая

$$\chi_s(x) = \varepsilon^{ks}, \tag{10}$$

где k определено сравнением (7) (ввиду равенства $\varepsilon^{p-1}=1$ значение ε^{ks} не зависит от выбора k). Если $k \equiv 0 \pmod{d}$, то $\varepsilon^{ks}=1$ при всех $s=0, 1, \ldots, d-1$ и, следовательно, сумма $\sum_{s=0}^{d-1} \chi_s(x)$ равна d. Если же $k \not\equiv 0 \pmod{d}$, то $\varepsilon^k \neq 1$ и поэтому

$$\sum_{s=0}^{d-1} \varepsilon^{ks} = \frac{\varepsilon^{kd}-1}{\varepsilon^k - 1} = 0.$$

Сопоставляя это с равенствами (9), мы получаем (для x, не делящихся на p) формулу

$$m(x) = \sum_{s=0}^{d-1} \chi_s(x).$$

Найденное выражение для $m(x)$ позволяет равенство (6) переписать в виде

$$\sum_y \zeta^{ay^r} = 1 + \sum_x{}^{*} \sum_{s=0}^{d-1} \chi_s(x) \zeta^{ax}. \tag{11}$$

Введенные нами функции χ_s, обладающие, очевидно, свойством

$$\chi_s(xy) = \chi_s(x)\chi_s(y), \tag{12}$$

называются *мультипликативными характерами* по модулю p. Распространим их на все целые x, полагая $\chi_s(x)=0$, если x делится на p. Ясно, что после такого доопределения свойство (12) сохра-

няется. Характер χ_0, значения которого $\chi_0(x)$ при $p \nmid x$ равны 1, называется *единичным характером*.

Выделим в сумме (11) слагаемые, соответствующие единичному характеру χ_0. Так как $1 + \sum_x{}' \zeta^{ax} = \sum_x \zeta^{ax} = 0$, то равенство (11) можно переписать в виде

$$\sum_y \zeta^{ay^r} = \sum_{s=1}^{d-1} \sum_x \chi_s(x)\,\zeta^{ax} \tag{13}$$

(здесь можно считать, что x пробегает полную систему вычетов по модулю p, так как $\chi_s(x) = 0$ при $x \equiv 0 \pmod p$).

Пусть χ — один из характеров χ_s и a — целое число. Выражение $\sum_x \chi(x)\,\zeta^{ax}$ называется *гауссовой суммой* и обозначается через $\tau_a(\chi)$.

Формулы (5) и (13) дают нам возможность сформулировать следующую теорему.

Теорема 2. *Для числа N решений сравнения*

$$a_1 x_1^{r_1} + \ldots + a_n x_n^{r_n} \equiv 0 \pmod p, \quad a_i \not\equiv 0 \pmod p, \tag{14}$$

имеет место формула

$$N = p^{n-1} + \frac{1}{p} \sum_x{}' \prod_{i=1}^{n} \sum_{s=1}^{d_i - 1} \tau_{a_i x}(\chi_{i,s}), \tag{15}$$

в которой $d_i = (r_i,\ p-1)$, а характеры $\chi_{i,s}$ определены равенством (10) при $d = d_i$.

Заметим, что если хоть одно из d_i окажется равным 1, т. е. r_i будет взаимно просто с $p-1$, то в формуле (15) соответствующая внутренняя сумма будет равна нулю (как сумма пустого множества слагаемых) и, следовательно, в этом случае имеем формулу $N = p^{n-1}$. Это, впрочем, ясно и без вычислений, ибо для любых значений $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ найдется одно и только одно значение для x_i, при котором сравнение (14) будет удовлетворяться.

Теорема 2 приобретает значение благодаря тому, что модуль гауссовой суммы может быть точно вычислен. Именно, в следующем пункте мы покажем, что

$$|\tau_a(\chi)| = \sqrt{p} \quad \text{при} \quad a \not\equiv 0 \pmod p \text{ и } \chi \neq \chi_0$$

(см. также задачу 8).

Посмотрим, что дает теорема 2 в сочетании с этим фактом. Из формулы (15) следует, что

$$|N-p^{n-1}|\leqslant\frac{1}{p}\sum_{x}{}'\prod_{i=1}^{n}\sum_{s=1}^{d_i-1}|\tau_{a_ix}(\chi_{i,s})|=$$

$$=\frac{1}{p}(p-1)\prod_{i=1}^{n}(d_i-1)\,p^{1/2}=(p-1)\,p^{n/2-1}\prod_{i=1}^{n}(d_i-1).$$

Мы получили, таким образом, следующую теорему.

Теорема 3. *Число N решений сравнения*

$$a_1x_1^{r_1}+\ldots+a_nx_n^{r_n}\equiv 0\pmod p$$

для всех простых p, не делящих $a_1, \ldots, a_n$, удовлетворяет неравенству

$$|N-p^{n-1}|\leqslant C(p-1)p^{n/2-1},\qquad(16)$$

где $C=(d_1-1)\ldots(d_n-1)$, $d_i=(r_i, p-1)$.

Из теоремы 3 при $n\geqslant 3$ (а мы предположили, что это так) для многочленов рассмотренного вида очевидным образом следует теорема B. В самом деле, $|N-p^{n-1}|\leqslant Cp^{n/2}\leqslant Cp^{n-1-1/2}$, что и утверждается теоремой B.

Отметим попутно, что полученное нами неравенство (16) при $n>3$ оказывается гораздо более точным, чем неравенство теоремы B.

Замечание. Для доказательства теоремы 3 нам достаточно было бы ввиду (5) знать оценку для модуля суммы $\sum_x \zeta^{axr}$. Такая оценка может быть получена, и притом более коротким путем, без использования гауссовых сумм (см. задачи 9—12). Мы изложили доказательство, опирающееся на свойства гауссовых сумм, так как гауссовы суммы имеют много других применений в теории чисел.

3. Модуль гауссовой суммы. Рассмотрим совокупность $\mathfrak{F}$ всех комплекснозначных функций $f(x)$, заданных на целых рациональных числах x и удовлетворяющих условию: $f(x)=f(y)$, если только $x\equiv y\pmod p$. Так как каждая функция $f(x)\in\mathfrak{F}$ определена своими значениями на полной системе вычетов по модулю p, то $\mathfrak{F}$ является p-мерным линейным пространством над полем всех комплексных чисел. Введем в $\mathfrak{F}$ эрмитово скалярное произведение, положив

$$(f, g)=\frac{1}{p}\sum_x f(x)\,\overline{g(x)},\quad f, g\in\mathfrak{F}.$$

Простая проверка показывает, что относительно введенного скалярного умножения p функций

$$f_a(x)=\zeta^{-ax}\qquad(a\text{ — вычет mod }p)\qquad(17)$$

образуют ортонормированный базис $\mathfrak{F}$. В самом деле, ввиду (2)

$$(f_a, f_{a'}) = \frac{1}{p}\sum_x \zeta^{(a'-a)x} = \begin{cases} 1 & \text{при } a \equiv a' \pmod p, \\ 0 & \text{при } a \not\equiv a' \pmod p. \end{cases}$$

Функции (17), обладающие свойством

$$f_a(x+y) = f_a(x) f_a(y),$$

называются *аддитивными характерами* по модулю p. Найдем координаты мультипликативного характера χ в базисе (17). Пусть

$$\chi = \sum_a \alpha_a f_a. \tag{18}$$

Тогда

$$\alpha_a = (\chi, f_a) = \frac{1}{p}\sum_x \chi(x)\zeta^{ax} = \frac{1}{p}\tau_a(\chi). \tag{19}$$

Мы видим, таким образом, что гауссовы суммы $\tau_a(\chi)$ (с точностью до множителя $1/p$) являются коэффициентами в разложении мультипликативного характера χ по аддитивным характерам f_a.

Чтобы получить одно важное соотношение между координатами α_a (и, значит, между гауссовыми суммами $\tau_a(\chi)$), умножим равенство

$$\chi(x) = \sum_a \alpha_a f_a(x) \tag{20}$$

на $\chi(c)$, где $c \not\equiv 0 \pmod p$, и заменим индекс суммирования a на ac:

$$\chi(cx) = \sum_a \chi(c)\alpha_{ac} f_{ac}(x) = \sum_a \chi(c)\alpha_{ac} f_a(cx).$$

Сравнивая это с (20), мы получаем, что

$$\alpha_a = \chi(c)\alpha_{ac}. \tag{21}$$

Полагая здесь $a = 1$ и замечая, что $|\chi(c)| = 1$, мы находим

$$|\alpha_c| = |\alpha_1| \quad \text{при} \quad c \not\equiv 0 \pmod p. \tag{22}$$

Предположим теперь, что характер χ отличен от единичного характера χ_0. Тогда число c (взаимно простое с p) можно выбрать так, чтобы $\chi(c) \neq 1$, и равенство (21) при $a = 0$ дает нам, что

$$\alpha_0 = 0. \tag{23}$$

Докажем теперь нужный нам результат о модуле гауссовой суммы.

Теорема 4. *Если χ — мультипликативный характер по модулю p, отличный от единичного характера χ_0, и a — целое число, взаимно простое с p, то $|\tau_a(\chi)| = \sqrt{p}$.*

Доказательство. Рассмотрим в пространстве $\mathfrak{F}$ скалярное произведение (χ, χ). Так как $|\chi(x)| = 1$ при $x \not\equiv 0 \pmod p$, то

$$(\chi, \chi) = \frac{1}{p} \sum_x \chi(x)\overline{\chi(x)} = \frac{p-1}{p}.$$

С другой стороны, используя разложение (18) и учитывая (22) и (23), мы находим $(\chi, \chi) = \sum_a |\alpha_a|^2 = (p-1)|\alpha_c|^2$. Оба результата вместе дают нам равенство

$$|\alpha_c| = 1/\sqrt{p}, \qquad c \not\equiv 0 \pmod p,$$

откуда ввиду формулы (19) и следует утверждение теоремы.

Задачи

1. Доказать, что для многочлена $F = x^2 + y^2$ не выполняется теорема A (относительно ненулевых решений), а для $F = x^2 - y^2$ — теорема B. Эти многочлены, конечно, не являются абсолютно неприводимыми.

2. Пусть $\varphi(x)$ — функция, заданная на целых числах x, взаимно простых с p, и принимающая отличные от нуля комплексные значения. Доказать, что если $\varphi(x) = \varphi(y)$ при $x \equiv y \pmod p$ и $\varphi(xy) = \varphi(x)\varphi(y)$ при любых x и y, то эта функция совпадает с одной из функций $\chi_s(x) = \varepsilon^{ks}$, где ε — первообразный корень степени $p-1$ из 1 (число k определяется сравнением (7)).

3. Доказать, что всякая комплекснозначная функция $f(x) \not\equiv 0$ от целочисленного аргумента, зависящая только от класса вычетов по модулю p и удовлетворяющая условию $f(x+y) = f(x)f(y)$, имеет вид $f(x) = \xi^{tx}$, где t — целое число, а ξ — фиксированный корень степени p из 1.

4. Пусть $p \not\equiv 2$. Доказать, что характер $\chi = \chi_1$, определенный равенством (10) при $d = 2$ (и $s = 1$), совпадает с символом Лежандра $\chi(x) = \left(\frac{x}{p}\right)$. (Этот характер χ называется *квадратичным характером* по модулю p.)

5. Пусть $ab \not\equiv 0 \pmod p$ и χ — квадратичный характер по модулю $p \not\equiv 2$. Для гауссовых сумм $\tau_a(\chi)$ и $\tau_b(\chi)$ доказать соотношение $\tau_a(\chi)\tau_b(\chi) = \left(\frac{-ab}{p}\right) p$.

6. При тех же обозначениях доказать, что $\sum_x{}' \tau_x(\chi) = 0$.

7. Решить задачи 10, 11 и 12 предшествующего параграфа, воспользовавшись теоремой 2 и результатами задач 5 и 6.

8. Пусть χ — произвольный мультипликативный характер по простому модулю p, отличный от χ_0, и $a \not\equiv 0 \pmod p$. Показать, что $|\tau_a(\chi)|^2 = \tau_a(\chi)\overline{\tau_a(\chi)} = p$, и этим получить новое доказательство теоремы 4.

9. Пусть $f(x)$ — целочисленный многочлен и ζ — первообразный корень степени m из 1. Положим $S_a = \sum_{x \pmod m} \zeta^{af(x)}$. Доказать, что

$$\sum_{a \pmod m} |S_a|^2 = m \sum_{c \pmod m} N(c)^2,$$

где $N(c)$ обозначает число решений сравнения $f(x) \equiv c \pmod m$.

10. Обозначим через ζ первообразный корень простой степени p из 1 и положим $T_a = \sum_x \zeta^{ax^r}$. Доказать, что

$$\sum_a{}' |T_a|^2 = p(p-1)(d-1),$$

где $d = (r, p-1)$.

11. В тех же обозначениях показать, что суммы T_a, $a \not\equiv 0 \pmod p$, разбиваются на d групп по $(p-1)/d$ равных между собой сумм. Пользуясь этим и результатом задачи 10, показать, далее, что

$$|T_a| < d\sqrt{p}, \qquad a \not\equiv 0 \pmod p.$$

12. Принимая во внимание тот факт, что $\sum_a{}' T_a = 0$, получить для T_a более точную оценку:

$$|T_a| \leqslant (d-1)\sqrt{p}, \qquad a \not\equiv 0 \pmod p.$$

(Ввиду формулы (5) эта оценка дает нам другое доказательство теоремы 3.)

13. Доказать, что сравнение

$$3x^3 + 4y^3 + 5z^3 \equiv 0 \pmod p$$

имеет ненулевое решение при любом простом p.

14. Доказать, что сравнение

$$2x^2 + y^4 - 17z^4 \equiv 0 \pmod p$$

имеет нетривиальное решение по любому простому модулю p.

§ 3. *p*-адические числа

1. Целые *p*-адические числа. Теперь мы перейдем к сравнениям, модуль которых есть степень простого числа. Начнем с примера. Рассмотрим сравнение $x^2 \equiv 2 \pmod{7^n}$ по степеням простого числа 7. При $n = 1$ сравнение имеет два решения:

$$x_0 \equiv \pm 3 \pmod 7. \tag{1}$$

Положим теперь $n = 2$. Из

$$x^2 \equiv 2 \pmod{7^2} \tag{2}$$

следует $x^2 \equiv 2 \pmod 7$, так что решения сравнения (2) надо искать в виде $x_0 + 7t_1$, где x_0 — одно из чисел, определяемых сравнением (1). Займемся разысканием решений вида $x_1 = 3 + 7t_1$. (Решения вида $-3 + 7t_1$ рассматриваются совершенно так же.) Подставляя это выражение для x_1 в (2), получаем:

$$(3 + 7t_1)^2 \equiv 2 \pmod{7^2}, \qquad 9 + 6 \cdot 7t_1 + 7^2 t_1^2 \equiv 2 \pmod{7^2},$$
$$1 + 6t_1 \equiv 0 \pmod 7, \qquad t_1 \equiv 1 \pmod 7.$$

Таким образом, получается решение $x_1 \equiv 3 + 7 \cdot 1 \pmod{7^2}$. Аналогично при $n = 3$ получаем $x_2 = x_1 + 7^2 t_2$ и из сравнения

$$(3 + 7 + 7^2 t_2)^2 \equiv 2 \pmod{7^3}$$

находим $t_2 \equiv 2 \pmod 7$, т. е.

$$x_2 \equiv 3 + 7 \cdot 1 + 7^2 \cdot 2 \pmod{7^3}.$$

Нетрудно видеть, что этот процесс мы можем продолжить до бесконечности. Мы получим последовательность

$$x_0, x_1, \ldots, x_n, \ldots, \tag{3}$$

обладающую свойствами:

$$x_0 \equiv 3 \pmod 7, \quad x_n \equiv x_{n-1} \pmod{7^n}, \quad x_n^2 \equiv 2 \pmod{7^{n+1}}.$$

Процесс построения последовательности (3) напоминает процесс извлечения квадратного корня из 2. Действительно, вычисление $\sqrt{2}$ состоит в построении последовательности рациональных чисел $r_0, r_1, \ldots, r_n, \ldots$, квадраты которых становятся сколь угодно близкими к 2, например: $|r_n^2 - 2| < 1/10^n$. В нашем же случае строится последовательность целых чисел $x_0, x_1, \ldots, x_n, \ldots$, для которых $x_n^2 - 2$ делится на 7^{n+1}. Эта аналогия становится более отчетливой, если мы условимся два целых числа называть близкими (точнее, p-близкими, где p — некоторое простое число), когда их разность делится на достаточно большую степень p. При таком понимании близости можно сказать, что квадраты чисел последовательности (3) при возрастании n становятся сколь угодно 7-близкими к 2.

Задание последовательности $\{r_n\}$ определяет вещественное число $\sqrt{2}$. Можно предположить, что последовательность (3) также определяет число α некоторой новой природы, причем такое, что $\alpha^2 = 2$.

Обратим внимание на следующее обстоятельство. Если последовательность рациональных чисел $\{r'_n\}$ такова, что $|r_n - r'_n| < 1/10^n$ при всех n, то ее пределом также будет $\sqrt{2}$. Естественно предположить, что последовательность $\{x'_n\}$, для которой $x_n \equiv x'_n \pmod{7^{n+1}}$, определяет то же самое новое число α (для новой последовательности $\{x'_n\}$, очевидно, также имеем $x'^2_n \equiv 2 \pmod{7^{n+1}}$ и $x'_n \equiv x'_{n-1} \pmod{7^n}$).

Эти замечания приводят нас к следующему определению.

Определение. *Пусть p — некоторое простое число. Последовательность целых чисел*

$$\{x_n\} = \{x_0, x_1, \ldots, x_n, \ldots\},$$

обладающих тем свойством, что

$$x_n \equiv x_{n-1} \pmod{p^n} \tag{4}$$

для всех $n \geqslant 1$, определяет новый объект, называемый целым p-адическим числом. Две последовательности $\{x_n\}$ и $\{x'_n\}$ тогда

и только тогда определяют одно и то же целое p-адическое число, когда $x_n \equiv x'_n \pmod{p^{n+1}}$ *для всех* $n \geqslant 0$.

То, что последовательность $\{x_n\}$ определяет целое p-адическое число α, будет записываться так: $\{x_n\} \to \alpha$.

Множество всех целых p-адических чисел мы будем обозначать через $\mathbb{Z}_p$. В отличие от целых p-адических чисел обычные *целые числа будут называться целыми рациональными.*

Каждому целому рациональному числу x сопоставим целое p-адическое число, определяемое последовательностью $\{x, x, \ldots, x, \ldots\}$. Это целое p-адическое число, соответствующее рациональному x, мы будем обозначать той же буквой x. Два различных целых рациональных числа x и y определяют разные целые p-адические числа. Действительно, из их равенства как целых p-адических чисел следовали бы при всех n сравнения $x \equiv y \pmod{p^n}$, что возможно только при $x = y$. Ввиду этого мы можем и будем рассматривать множество $\mathbb{Z}$ целых рациональных чисел как часть множества $\mathbb{Z}_p$ целых p-адических чисел.

Для того чтобы яснее представить себе множество $\mathbb{Z}_p$ укажем способ, при помощи которого можно из множества всех последовательностей, определяющих данное целое p-адическое число, выбрать одну стандартную.

Пусть целое p-адическое число задается последовательностью $\{x_n\}$. Обозначим наименьшее неотрицательное число, сравнимое с x_n по модулю p^{n+1}, через $\bar{x}_n$:

$$x_n \equiv \bar{x}_n \pmod{p^{n+1}}, \tag{5}$$

$$0 \leqslant \bar{x}_n < p^{n+1}. \tag{6}$$

Сравнение (5) показывает, что

$$\bar{x}_n \equiv x_n \equiv x_{n-1} \equiv \bar{x}_{n-1} \pmod{p^n},$$

так что последовательность $\{\bar{x}_n\}$ определяет некоторое целое p-адическое число, и притом в силу (5) то же самое, что и последовательность $\{x_n\}$. Последовательность, все члены которой удовлетворяют условиям (4) и (6), будем называть канонической. Мы доказали, следовательно, что каждое целое p-адическое число определяется некоторой канонической последовательностью.

Легко видеть, что две разные канонические последовательности определяют разные целые p-адические числа. Действительно, если канонические последовательности $\{\bar{x}_n\}$ и $\{\bar{y}_n\}$ определяют одно и то же целое p-адическое число, то в силу сравнений

$$\bar{x}_n \equiv \bar{y}_n \pmod{p^{n+1}}$$

и условий $0 \leqslant \bar{x}_n < p^{n+1}$, $0 \leqslant \bar{y}_n < p^{n+1}$ получаем, что $\bar{x}_n = \bar{y}_n$ при всех $n \geqslant 0$. Таким образом, целые p-адические числа находятся во взаимно однозначном соответствии с каноническими последовательностями. Из условия (4) следует, что $\bar{x}_{n+1} = \bar{x}_n + a_{n+1}p^{n+1}$,

а так как $0 \leqslant \bar{x}_{n+1} < p^{n+2}$ и $0 \leqslant \bar{x}_n < p^{n+1}$, то $0 \leqslant a_{n+1} < p$. Следовательно, всякая каноническая последовательность имеет вид

$$\{a_0,\ a_0 + a_1 p,\ a_0 + a_1 p + a_2 p^2 \ldots\},$$

где $0 \leqslant a_i < p$. Очевидно, что и, наоборот, каждая последовательность такого вида является канонической последовательностью, определяющей некоторое целое p-адическое число. Исходя из этого, легко доказать, что множество канонических последовательностей, а следовательно, и множество всех целых p-адических чисел имеют мощность континуума.

2. Кольцо целых p-адических чисел.

Определение. *Суммой и произведением целых p-адических чисел α и β, определяемых последовательностями $\{x_n\}$ и $\{y_n\}$, называются целые p-адические числа, определяемые соответственно последовательностями $\{x_n + y_n\}$ и $\{x_n y_n\}$.*

Чтобы быть уверенным в корректности этого определения, мы должны доказать, что последовательности $\{x_n + y_n\}$ и $\{x_n y_n\}$ определяют некоторые целые p-адические числа и что эти числа зависят только от α и β, а не от выбора определяющих их последовательностей. Оба эти свойства доказываются путем очевидной проверки, которую мы пропустим.

Столь же очевидно, что при данном нами определении действий над целыми p-адическими числами они образуют коммутативное кольцо, содержащее кольцо целых рациональных чисел в качестве подкольца.

Делимость целых p-адических чисел определяется так же, как в любом кольце (см. Дополнение, § 4, п. 1): α делится на β, если существует такое целое p-адическое число γ, что $\alpha = \beta\gamma$. Для исследования свойств деления важно знать, каковы те целые p-адические числа, для которых существуют обратные целые p-адические числа. Такие числа, согласно п. 1 § 4 Дополнения, называются делителями единицы или единицами. Мы их будем называть также *p-адическими единицами.*

Теорема 1. *Целое p-адическое число α, определяемое последовательностью $\{x_0, x_1, \ldots, x_n, \ldots\}$, тогда и только тогда является единицей, когда $x_0 \not\equiv 0 \pmod p$.*

Доказательство. Пусть α является единицей. Тогда существует такое целое p-адическое число β, что $\alpha\beta = 1$. Если β определяется последовательностью $\{y_n\}$, то условие $\alpha\beta = 1$ означает, что

$$x_n y_n \equiv 1 \pmod{p^{n+1}}. \tag{7}$$

В частности, $x_0 y_0 \equiv 1 \pmod p$, а значит, $x_0 \not\equiv 0 \pmod p$. Обратно, пусть $x_0 \not\equiv 0 \pmod p$. Из условия (4) легко следует, что

$$x_n \equiv x_{n-1} \equiv \ldots \equiv x_0 \pmod p,$$

так что $x_n \not\equiv 0 \pmod p$. Следовательно, для любого n можно

найти такое y_n, что будет справедливо сравнение (7). Так как $x_n \equiv x_{n-1} \pmod{p^n}$ и $x_n y_n \equiv x_{n-1} y_{n-1} \pmod{p^n}$, то $y_n \equiv y_{n-1} \pmod{p^n}$. Это значит, что последовательность $\{y_n\}$ определяет некоторое целое p-адическое число β. Сравнения (7) показывают, что $\alpha\beta = 1$, т. е. что α является единицей.

Из доказанной теоремы следует, что целое рациональное число a, будучи рассмотрено как элемент кольца $\mathbb{Z}_p$, тогда и только тогда является единицей, когда $a \not\equiv 0 \pmod{p}$. Если это условие выполнено, то a^{-1} содержится в $\mathbb{Z}_p$. Отсюда следует, что любое целое рациональное b делится на такое a в $\mathbb{Z}_p$, т. е. что любое рациональное число вида b/a, где a и b целые и $a \not\equiv 0 \pmod{p}$, содержится в $\mathbb{Z}_p$. Рациональные числа такого вида называются *p-целыми*. Они образуют очевидным образом кольцо. Полученный нами результат можно теперь сформулировать так:

Следствие. *Кольцо $\mathbb{Z}_p$ целых p-адических чисел содержит подкольцо, изоморфное кольцу p-целых рациональных чисел.*

Теорема 2. *Всякое отличное от нуля целое p-адическое число α однозначно представляется в виде*

$$\alpha = p^m \varepsilon, \tag{8}$$

где ε — единица кольца $\mathbb{Z}_p$.

Доказательство. Если α — единица, то равенство (8) справедливо при $m = 0$. Пусть $\{x_n\} \to \alpha$ и α не является единицей, так что согласно теореме 1 $x_n \equiv 0 \pmod{p}$. Так как $\alpha \neq 0$, то сравнения $x_n \equiv 0 \pmod{p^{n+1}}$ невозможны при всех n. Пусть m — наименьший индекс, для которого

$$x_m \not\equiv 0 \pmod{p^{m+1}}. \tag{9}$$

Для любого $s \geqslant 0$

$$x_{m+s} \equiv x_{m-1} \equiv 0 \pmod{p^m},$$

поэтому число $y_s = x_{m+s}/p^m$ целое. Из сравнения

$$p^m y_s - p^m y_{s-1} = x_{m+s} - x_{m+s-1} \equiv 0 \pmod{p^{m+s}}$$

следует, что $y_s \equiv y_{s-1} \pmod{p^s}$ при всех $s \geqslant 0$. Последовательность $\{y_s\}$ определяет, таким образом, некоторое $\varepsilon \in \mathbb{Z}_p$. Так как $y_0 = x_m/p^m \not\equiv 0 \pmod{p}$, то по теореме 1 ε является единицей. Наконец, из сравнения

$$p^m y_s = x_{m+s} \equiv x_s \pmod{p^{s+1}}$$

вытекает, что $p^m \varepsilon = \alpha$, т. е. имеет место представление (8).

Предположим теперь, что α имеет другое представление: $\alpha = p^k \eta$, где $k \geqslant 0$, η — единица. Если $\{z_s\} \to \eta$, то

$$p^m y_s \equiv p^k z_s \pmod{p^{s+1}} \tag{10}$$

при всех $s \geqslant 0$, причем согласно теореме 1 все y_s и z_s не делятся на p, так как ε и η — единицы. Положив в сравнении (10) $s = m$, получаем, что $p^m y_m \equiv p^k z_m \not\equiv 0 \pmod{p^{m+1}}$, откуда вытекает нера-

венство $k \leqslant m$. В силу симметрии мы получаем, что и $m \leqslant k$, т. е. $k = m$. Заменим теперь в сравнении (10) s на $s+m$ и сократим его на p^m. Мы получим, что

$$y_{m+s} \equiv z_{m+s} \pmod{p^{s+1}},$$

а так как $y_{m+s} \equiv y_s \pmod{p^{s+1}}$ и $z_{m+s} \equiv z_s \pmod{p^{s+1}}$ ввиду условия (4), то $y_s \equiv z_s \pmod{p^{s+1}}$. Так как это сравнение справедливо для всех $s \geqslant 0$, то $\varepsilon = \eta$. Теорема 2 доказана.

Следствие 1. *Целое p-адическое число α, определяемое последовательностью $\{x_n\}$, тогда и только тогда делится на p^k, когда $x_n \equiv 0 \pmod{p^{n+1}}$ при всех $n = 0, 1, \ldots, k-1$.*

Действительно, мы определили показатель m в разложении (8) как наименьший индекс m, для которого имеет место (9).

Следствие 2. *Кольцо $\mathbb{Z}_p$ не имеет делителей нуля.*

Действительно, если $\alpha \neq 0$ и $\beta \neq 0$, то для них имеются представления $\alpha = p^m\varepsilon$, $\beta = p^k\eta$, в которых ε и η — единицы. (Для ε и η в кольце $\mathbb{Z}_p$ существуют, следовательно, обратные элементы ε^{-1} и η^{-1}.) Если бы $\alpha\beta = 0$, то, умножив равенство $p^{m+k}\varepsilon\eta = 0$ на $\varepsilon^{-1}\eta^{-1}$, мы получили бы $p^{m+k} = 0$, а это невозможно.

Определение. *Число m в представлении (8) отличного от нуля целого p-адического числа α называется p-показателем α и обозначается через $\nu_p(\alpha)$.*

В случае, если будет ясно, какое простое число p имеется в виду, мы будем говорить просто о показателе и обозначать его через $\nu(\alpha)$. Чтобы функция $\nu(\alpha)$ была определена на всех целых p-адических числах, мы доопределим ее, полагая $\nu(0) = \infty$. (Целесообразность этого формального равенства обусловлена тем, что 0 делится на сколь угодно большую степень p.)

Непосредственная проверка дает следующие свойства показателя:

$$\nu(\alpha\beta) = \nu(\alpha) + \nu(\beta), \tag{11}$$

$$\nu(\alpha+\beta) \geqslant \min(\nu(\alpha), \nu(\beta)), \tag{12}$$

$$\nu(\alpha+\beta) = \min(\nu(\alpha), \nu(\beta)), \text{ если } \nu(\alpha) \neq \nu(\beta). \tag{13}$$

В терминах показателя особенно просто выражаются свойства делимости целых p-адических чисел. В частности, из теоремы 2 сразу же вытекает

Следствие 3. *Целое p-адическое число α тогда и только тогда делится на β, когда $\nu(\alpha) \geqslant \nu(\beta)$.*

Таким образом, арифметика кольца $\mathbb{Z}_p$ очень проста: в нем имеется один-единственный (с точностью до ассоциированности) простой элемент, это число p. Через его степени и единицы выражаются все отличные от нуля элементы из $\mathbb{Z}_p$.

В заключение остановимся на сравнениях в кольце $\mathbb{Z}_p$. Сравнимость элементов определяется здесь так же, как для целых

чисел и вообще для элементов любого кольца (см. Дополнение, § 4, п. 1): $\alpha \equiv \beta \pmod{\gamma}$ означает, что $\alpha - \beta$ делится на γ. Если $\gamma = p^n\varepsilon$, где ε — единица, то всякое сравнение по модулю γ равносильно тому же сравнению по модулю p^n. Можно ограничиться поэтому рассмотрением сравнений только по модулю p^n.

Теорема 3. *Всякое целое p-адическое число сравнимо с целым рациональным числом по модулю p^n. Два целых рациональных числа тогда и только тогда сравнимы по модулю p^n в кольце $\mathbb{Z}_p$, когда они сравнимы по этому модулю в кольце $\mathbb{Z}$.*

Доказательство. Чтобы доказать первое утверждение, покажем, что если α — целое p-адическое число и $\{x_n\}$ — определяющая его последовательность целых рациональных чисел, то

$$\alpha \equiv x_{n-1} \pmod{p^n}. \tag{14}$$

Так как x_{n-1} определяется последовательностью $\{x_{n-1}, x_{n-1}, \ldots\}$, то последовательность, определяющая $\alpha - x_{n-1}$, есть $\{x_0 - x_{n-1}, x_1 - x_{n-1}, \ldots\}$. Применим к целому p-адическому числу $\alpha - x_{n-1}$ следствие 1 теоремы 2. Мы видим, что сравнение (14) равносильно сравнениям

$$x_k - x_{n-1} \equiv 0 \pmod{p^{k+1}}, \quad k = 0, 1, \ldots, n-1,$$

справедливость которых в свою очередь вытекает из условия (4) в определении целых p-адических чисел.

Докажем теперь, что для двух целых рациональных чисел x и y сравнимость по модулю p^n в кольце $\mathbb{Z}^p$ равносильна сравнимости по тому же модулю в кольце $\mathbb{Z}$. Для этого положим

$$x - y = p^m a, \quad a \not\equiv 0 \pmod{p} \tag{15}$$

(мы считаем $x \neq y$). Сравнение

$$x \equiv y \pmod{p^n} \tag{16}$$

в кольце $\mathbb{Z}$ равносильно условию $n \leqslant m$. С другой стороны, (15) есть представление (8) для числа $x - y$, так как a является p-адической единицей. Следовательно, $\nu_p(x - y) = m$ и условие $n \leqslant m$ можно переписать в виде $\nu_p(x - y) \geqslant n$, а это равносильно сравнению (16) в $\mathbb{Z}_p$, так как $\nu(p^n) = n$ (см. следствие 3 теоремы 2).

Следствие. *Число классов вычетов по модулю p^n в $\mathbb{Z}_p$ равно p^n.*

3. Дробные p-адические числа. Так как кольцо $\mathbb{Z}_p$ не имеет делителей нуля (следствие 2 теоремы 2), то его можно включить в поле, используя конструкцию поля отношений области целостности. В применении к нашему случаю эта конструкция сводится к рассмотрению дробей вида α/p^k, где α — некоторое целое p-адическое число, $k \geqslant 0$. Дробь рассматривается здесь просто как удобная запись пары (α, p^k).

Определение. *Дробь вида α/p^k, $\alpha \in \mathbb{Z}_p$, $k \geqslant 0$, определяет дробное p-адическое число или просто p-адическое число. Две*

дроби, α/p^k и β/p^m, определяют одно и то же p-адическое число, если $\alpha p^m = \beta p^k$ в $\mathbb{Z}_p$.

Совокупность всех p-адических чисел будет обозначаться через $\mathbb{Q}_p$.

Целое p-адическое число определяет элемент $\alpha/1 = \alpha/p^0$ из $\mathbb{Q}_p$. Очевидно, что различные целые p-адические числа определяют различные элементы из $\mathbb{Q}_p$. Ввиду этого мы будем считать $\mathbb{Z}_p$ подмножеством множества $\mathbb{Q}_p$.

Действия в $\mathbb{Q}_p$ определяются правилами:

$$\frac{\alpha}{p^k} + \frac{\beta}{p^m} = \frac{\alpha p^m + \beta p^k}{p^{k+m}}, \qquad \frac{\alpha}{p^k} \cdot \frac{\beta}{p^m} = \frac{\alpha\beta}{p^{k+m}}.$$

Очевидная проверка показывает, что результат действий не зависит от выбора тех дробей, которые определяют элементы из $\mathbb{Q}_p$, и что относительно этих действий $\mathbb{Q}_p$ образует поле — *поле всех p-адических чисел*. Очевидно, что поле $\mathbb{Q}_p$ имеет характеристику нуль и, следовательно, содержит поле рациональных чисел.

Теорема 4. *Всякое p-адическое число $\xi \neq 0$ единственным образом представляется в виде*

$$\xi = p^m \varepsilon, \tag{17}$$

где m — целое число, а ε — единица из $\mathbb{Z}_p$.

Доказательство. Пусть $\xi = \alpha/p^k$, $\alpha \in \mathbb{Z}_p$. По теореме 2 α представляется в виде $\alpha = p^l\varepsilon$, $l \geqslant 0$, где ε — единица кольца $\mathbb{Z}_p$. Мы получаем, что $\xi = p^m\varepsilon$, где $m = l - k$. Единственность представления (17) вытекает из соответствующего утверждения для целых p-адических чисел, доказанного в теореме 2.

Введенное в п. 2 понятие показателя легко обобщается на любые p-адические числа. Мы полагаем $\nu_p(\xi) = m$, где m — показатель в представлении (17). Легко видеть, что свойства (11), (12) и (13) показателя автоматически переносятся на поле $\mathbb{Q}_p$. Очевидно, что p-адическое число ξ тогда и только тогда является целым p-адическим числом, когда $\nu_p(\xi) \geqslant 0$.

4. Сходимость в поле p-адических чисел. В п. 1 мы обратили внимание на аналогию между целыми p-адическими и вещественными числами: и те и другие определяются некоторыми последовательностями рациональных чисел.

Так как каждое вещественное число является, как известно, пределом той последовательности рациональных чисел, которая его определяет, то естественно предположить, что аналогичный факт должен иметь место и для p-адических чисел, если только правильно определить для них понятие сходимости. При определении предела вещественных чисел мы опираемся, по существу, на понятие близости: два вещественных или рациональных числа считаются близкими, если абсолютная величина их разности достаточно мала. Для определения сходимости в поле p-адических

чисел нам надо, следовательно, уяснить себе, при каком условии два p-адических числа должны рассматриваться как близкие.

При рассмотрении примера, приведенного в начале параграфа, мы уже упоминали о p-близости двух целых рациональных чисел x и y, понимая под этим делимость разности $x-y$ на достаточно большую степень p. Именно при таком новом понимании близости, как мы видели, и проявляется аналогия в определении вещественных и целых p-адических чисел. Если воспользоваться понятием p-показателя ν_p, то p-близость x и y будет характеризоваться, очевидно, значением $\nu_p(x-y)$. Это подсказывает нам, что два произвольных p-адических числа ξ и η (не обязательно целых) надо считать близкими в том случае, если значение $\nu_p(\xi-\eta)$ достаточно велико. Другими словами, «малые» p-адические числа должны характеризоваться большим значением их p-показателя.

После этих предварительных замечаний перейдем к точному определению.

Определение. *Последовательность*

$$\{\xi_n\}=\{\xi_0, \xi_1, \ldots, \xi_n, \ldots\}$$

p-адических чисел называется сходящейся к p-адическому числу ξ (*в обозначении* $\lim\limits_{n\to\infty}\xi_n=\xi$ *или* $\{\xi_n\}\to\xi$), *если*

$$\lim_{n\to\infty}\nu_p(\xi_n-\xi)=\infty.$$

Существенной особенностью этого определения (отличающей его от обычного определения сходимости для вещественных чисел) является то, что в нем сходимость $\{\xi_n\}\to\xi$ связывается с последовательностью целых рациональных чисел $\nu_p(\xi_n-\xi)$, которая должна стремиться к бесконечности. Можно придать этому определению более привычный вид, если вместо показателя ν_p на поле $\mathbb{Q}_p$ рассмотреть другую функцию с вещественными неотрицательными значениями, которая стремится к нулю, когда показатель стремится к бесконечности. Именно, выбрав некоторое вещественное число ρ, удовлетворяющее условию $0<\rho<1$, положим

$$\varphi_p(\xi)=\begin{cases}\rho^{\nu_p(\xi)} & \text{при } \xi\neq 0,\\ 0 & \text{при } \xi=0.\end{cases} \tag{18}$$

Определение. *Функция* $\varphi_p(\xi)$, $\xi\in\mathbb{Q}_p$, *определенная условиями* (18), *называется p-адической метрикой. Значение* $\varphi_p(\xi)$ *называется величиной p-адического числа* ξ *в этой метрике.*

Как и в случае показателя, мы будем иногда функцию φ_p называть просто метрикой и обозначать через φ.

Из свойств (11) и (12) показателя очевидным образом вытекают следующие свойства метрики:

$$\varphi(\xi\eta) = \varphi(\xi)\varphi(\eta), \tag{19}$$

$$\varphi(\xi + \eta) \leqslant \max(\varphi(\xi), \varphi(\eta)). \tag{20}$$

Из последнего перавенства получаем также, что

$$\varphi(\xi + \eta) \leqslant \varphi(\xi) + \varphi(\eta). \tag{21}$$

Свойства (19) и (21) (а также свойство: $\varphi(\xi) > 0$ при $\xi \neq 0$) указывают на то, что введенное понятие метрики для p-адических чисел является аналогом понятия абсолютной величины в поле вещественных чисел (или модуля в поле всех комплексных чисел).

В терминах метрики φ_p определение сходимости в поле $\mathbb{Q}_p$ принимает следующий вид: последовательность $\{\xi_n\}$, $\xi_n \in \mathbb{Q}_p$, сходится к p-адическому числу ξ, если

$$\lim_{n\to\infty} \varphi_p(\xi_n - \xi) = 0.$$

Для поля $\mathbb{Q}_p$ легко могут быть сформулированы и доказаны обычные теоремы о пределах последовательностей, хорошо известные из математического анализа. Покажем, например, что если $\{\xi_n\} \to \xi$ и $\xi \neq 0$, то $\{1/\xi_n\} \to 1/\xi$. Прежде всего, начиная с некоторого места, т. е. при $n \geqslant n_0$, имеем $\nu(\xi_n - \xi) > \nu(\xi)$, откуда, согласно свойству (13) для показателей, получаем: $\nu(\xi_n) = \min(\nu(\xi_n - \xi), \nu(\xi)) = \nu(\xi)$; в частности, $\nu(\xi_n) \neq \infty$, т. е. $\xi_n \neq 0$, а значит, $1/\xi_n$ при тех же $n \geqslant n_0$ имеет смысл. Далее,

$$\nu\left(\frac{1}{\xi_n} - \frac{1}{\xi}\right) = \nu(\xi - \xi_n) - \nu(\xi_n) - \nu(\xi) = \nu(\xi_n - \xi) - 2\nu(\xi) \to \infty$$

при $n \to \infty$, и наше утверждение доказано.

Теорема 5. *Если целое p-адическое число α определяется последовательностью целых чисел $\{x_n\}$, то эта последовательность сходится к α. Произвольное p-адическое число ξ является пределом последовательности рациональных чисел.*

Доказательство. Из сравнения (14) следует, что $\nu_p(x_n - \alpha) \geqslant n + 1$. Следовательно, $\nu(x_n - \alpha) \to \infty$ при $n \to \infty$, а это и означает, что $\{x_n\}$ стремится к α. Рассмотрим теперь дробное p-адическое число $\xi = \alpha/p^k$. Так как

$$\nu\left(\frac{x_n}{p^k} - \xi\right) = \nu\left(\frac{x_n - \alpha}{p^k}\right) = \nu(x_n - \alpha) - k \to \infty$$

при $n \to \infty$, то ξ является пределом рациональной последовательности $\{x_n/p^k\}$. Теорема доказана.

Из всякой ограниченной последовательности вещественных чисел всегда можно выделить, как известно, сходящуюся подпо-

следовательность. Аналогичное свойство имеет место и для p-адических чисел.

Определение. *Последовательность p-адических чисел $\{\xi_n\}$ называется ограниченной, если все значения $\varphi_p(\xi_n)$ ограничены сверху или, что то же самое, все числа $v_p(\xi_n)$ ограничены снизу.*

Теорема 6. *Из всякой ограниченной последовательности p-адических чисел (в частности, из всякой последовательности целых p-адических чисел) можно выделить сходящуюся подпоследовательность.*

Доказательство. Докажем сначала теорему для последовательности $\{\alpha_n\}$ целых p-адических чисел. Так как в кольце $\mathbb{Z}_p$ число классов вычетов по модулю p конечно (следствие теоремы 3), то в последовательности $\{\alpha_n\}$ содержится бесконечно много членов, сравнимых по модулю p с одним и тем же целым рациональным числом x_0. Выделяя все эти члены, мы получаем подпоследовательность $\{\alpha_n^{(1)}\}$, все члены которой удовлетворяют сравнению $\alpha_n^{(1)} \equiv x_0 \pmod p$. Аналогичным образом, применяя следствие теоремы 3 при $n=2$, мы из $\{\alpha_n^{(1)}\}$ выделим подпоследовательность $\{\alpha_n^{(2)}\}$ с условием $\alpha_n^{(2)} \equiv x_1 \pmod{p^2}$, где x_1 — некоторое целое рациональное число; при этом, очевидно, $x_1 \equiv x_0 \pmod p$. Продолжая этот процесс до бесконечности, мы для каждого k получим последовательность $\{\alpha_n^{(k)}\}$, которая является подпоследовательностью предыдущей последовательности $\{\alpha_n^{(k-1)}\}$ и для членов которой справедливы сравнения

$$\alpha_n^{(k)} \equiv x_{k-1} \pmod{p^k}$$

при некотором целом рациональном x_{k-1}. Так как все $\alpha_n^{(k+1)}$ находятся среди $\alpha_n^{(k)}$ и $x_k \equiv \alpha_n^{(k+1)} \pmod{p^{(k+1)}}$, то

$$x_k \equiv x_{k-1} \pmod{p^k}$$

при всех $k \geqslant 1$. Последовательность $\{x_n\}$ определяет, следовательно, некоторое целое p-адическое число α. Составим теперь «диагональную» последовательность $\{\alpha_n^{(n)}\}$. Ясно, что она является подпоследовательностью исходной последовательности $\{\alpha_n\}$. Утверждаем, что $\{\alpha_n^{(n)}\} \to \alpha$. В самом деле, в силу (14) имеем: $\alpha \equiv x_{n-1} \pmod{p^n}$; с другой стороны, $\alpha_n^{(n)} \equiv x_{n-1} \pmod{p^n}$, следовательно, $\alpha_n^{(n)} \equiv \alpha \pmod{p^n}$, т. е. $v(\alpha_n^{(n)} - \alpha) \geqslant n$. Отсюда следует, что $v(\alpha_n^{(n)} - \alpha) \to \infty$ при $n \to \infty$, а значит $\{\alpha_n^{(n)}\}$ сходится к α.

Перейдем к доказательству теоремы в общем случае. Если для последовательности p-адических чисел $\{\xi_n\}$ имеем $v(\xi_n) \geqslant -k$ (k — некоторое целое рациональное число), то для $\alpha_n = \xi_n p^k$ будем иметь $v(\alpha_n) \geqslant 0$. По доказанному из последовательности $\{\alpha_n\}$ целых p-адических чисел можно извлечь сходящуюся подпоследовательность $\{\alpha_{n_i}\}$. Но тогда последовательность $\{\xi_{n_i}\} = \{\alpha_{n_i} p^{-k}\}$

будет сходящейся подпоследовательностью для $\{\xi_n\}$. Теорема 6 доказана полностью.

Для p-адических чисел справедлив также признак сходимости Коши: последовательность

$$\{\xi^n\},\ \xi_n \in \mathbb{Q}_p, \tag{22}$$

сходится тогда и только тогда, когда

$$\lim_{m,n\to\infty} \nu(\xi_m - \xi_n) = \infty. \tag{23}$$

Необходимость этого условия очевидна. Для доказательства достаточности заметим прежде всего, что из (23) вытекает ограниченность (22). В самом деле, из условия (23) следует существование такого n_0, что $\nu(\xi_m - \xi_{n_0}) \geqslant 0$ при всех $m \geqslant n_0$. Но тогда в силу свойства (12) для тех же $m \geqslant n_0$ справедливо неравенство

$$\nu(\xi_m) = \nu((\xi_m - \xi_{n_0}) + \xi_{n_0}) \geqslant \min(0, \nu(\xi_{n_0})),$$

откуда и следует ограниченность (22). По теореме 6 из (22) можно извлечь сходящуюся подпоследовательность $\{\xi_{n_i}\}$ с пределом, скажем, ξ. Покажем, что тогда сама последовательность (22) сходится к элементу ξ. Пусть M — произвольное сколь угодно большое число. В силу (23) и определения сходимости мы можем найти такое натуральное число N, что, во-первых, $\nu(\xi_m - \xi_n) \geqslant M$ при $m,\ n \geqslant N$ и, во-вторых, $\nu(\xi_{n_i} - \xi) \geqslant M$ при $n_i \geqslant N$. Тогда

$$\nu(\xi_m - \xi) \geqslant \min(\nu(\xi_m - \xi_{n_i}), \nu(\xi_{n_i} - \xi)) \geqslant M$$

для всех $m \geqslant N$. Таким образом, $\lim\limits_{m\to\infty} \nu(\xi_m - \xi) = \infty$, т. е. последовательность (22) сходящаяся.

Доказанному признаку сходимости в поле p-адических чисел можно дать другую, более сильную форму. Если для последовательности (22) выполнено условие (23), то, очевидно, имеем также

$$\lim_{n\to\infty} \nu(\xi_{n+1} - \xi_n) = \infty. \tag{24}$$

Оказывается, что и, обратно, из условия (24) следует (23). Действительно, если $\nu(\xi_{n+1} - \xi_n) \geqslant M$ при всех $n \geqslant N$, то в силу (12) из равенства

$$\xi_m - \xi_n = \sum_{i=n}^{m-1} (\xi_{i+1} - \xi_i),\ m > n \geqslant N,$$

вытекает

$$\nu(\xi_m - \xi_n) \geqslant \min_{i=n,\ldots,m-1} \nu(\xi_{i+1} - \xi_i) \geqslant M,$$

т. е. $\nu(\xi_m - \xi_n) \to \infty$ при $m,\ n \to \infty$. Таким образом, имеет место

Теорема 7. *Для сходимости последовательности p-адических чисел $\{\xi_n\}$ необходимо и достаточно, чтобы* $\lim\limits_{n\to\infty} \nu(\xi_{n+1} - \xi_n) = \infty$.

Наличие понятия сходимости в поле $\mathbb{Q}_p$ дает возможность говорить о непрерывных p-адических функциях от p-адического аргумента. Их определение, по существу, ничем не отличается от обычного. Именно, функция $F(\xi)$ называется непрерывной при $\xi = \xi_0$, если для всякой последовательности $\{\xi_n\}$, сходящейся к ξ_0, последовательность значений $\{F(\xi_n)\}$ сходится к $F(\xi_0)$. Аналогично будет для функций от нескольких переменных. Так же, как и в вещественном анализе, легко могут быть доказаны обычные теоремы об арифметических операциях над непрерывными p-адическими функциями. В частности, легко убедиться, что многочлен от любого числа переменных с p-адическими коэффициентами есть непрерывная p-адическая функция. Этим простым фактом мы в дальнейшем (§ 5, п. 1) воспользуемся.

В заключение этого пункта сделаем несколько замечаний о рядах с p-адическими членами.

Определение. *Если последовательность частных сумм* $s_n = \sum_{i=0}^{n} \alpha_i$ *ряда*

$$\sum_{i=0}^{\infty} \alpha_i = \alpha_0 + \alpha_1 + \ldots + \alpha_n + \ldots \tag{25}$$

с p-адическими членами сходится к p-адическому числу α, то говорим, что этот ряд сходится и что его сумма равна α.

Из теоремы 7 непосредственно вытекает следующий признак сходимости для рядов.

Теорема 8. *Для сходимости ряда* (25) *необходимо и достаточно, чтобы его общий член α_n стремился к нулю, т. е. чтобы $\nu(\alpha_n) \to \infty$ при $n \to \infty$.*

Сходящиеся p-адические ряды можно, очевидно, почленно складывать, вычитать и умножать на постоянные p-адические числа. Для них имеет место также сочетательное свойство рядов.

Теорема 9. *При любой перестановке членов сходящегося p-адического ряда его сходимость не нарушается и сумма не меняется.*

Доказательство этой теоремы совсем просто, и мы предоставляем его читателю.

В курсе математического анализа доказывается, что свойство, указанное в теореме 9, в применении к рядам с вещественными членами характеризует абсолютно сходящиеся ряды. Все сходящиеся p-адические ряды являются, таким образом, и «абсолютно сходящимися». Отсюда следует, что в поле p-адических чисел сходящиеся ряды можно перемножать по обычным правилам анализа.

Если целое p-адическое число α определяется канонической последовательностью $\{a_0,\ a_0 + a_1 p,\ a_0 + a_1 p + a_2 p^2,\ \ldots\}$ (см. п. 1), то, согласно первому утверждению теоремы 5, оно будет равно

сумме сходящегося ряда

$$a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^n + \ldots, \qquad 0 \leqslant a_n \leqslant p-1, \quad n = 0, 1, \ldots \tag{26}$$

Так как различные канонические последовательности определяют различные целые p-адические числа, то представление α в виде ряда (26) однозначно. Очевидно, что и, обратно, всякий ряд вида (26) сходится к некоторому целому p-адическому числу.

Представление целых p-адических чисел рядами (26) напоминает запись вещественных чисел в виде бесконечных десятичных дробей.

Если рассмотреть ряд

$$b_0 + b_1 p + \ldots + b_n p^n + \ldots, \tag{27}$$

в котором коэффициенты — произвольные целые рациональные числа, то он, очевидно, будет сходящимся (так как $\nu(b_n p^n) \geqslant n$) и его сумма будет равна некоторому целому p-адическому числу α. Чтобы для этого α получить представление (26), надо, как легко видеть, последовательно заменить все коэффициенты в (27) их остатками от деления на p, относя неполное частное на каждом шаге к следующему члену. Это замечание имеет значение для выполнения действий в кольце $\mathbb{Z}_p$. Именно, при сложении, вычитании или умножении рядов вида (26) по правилам действий над степенными рядами мы получим ряд вида (27), в котором коэффициенты, вообще говоря, не будут наименьшими неотрицательными вычетами по модулю p. Для преобразования его в ряд вида (26) надо применить только что отмеченный прием. Этот способ выполнения действий над целыми p-адическими числами аналогичен, как видим, обычному способу производства действий над вещественными числами, записанными в виде бесконечных десятичных дробей.

Из теоремы 1 легко следует, что целое p-адическое число, представленное в виде ряда (26), является единицей кольца $\mathbb{Z}_p$ тогда и только тогда, когда $a_0 \neq 0$. Вместе с теоремой 4 это дает нам следующий результат.

Теорема 10. *Каждое отличное от нуля p-адическое число ξ однозначно записывается в виде*

$$\xi = p^m (a_0 + a_1 p + \ldots + a_n p^n + \ldots), \tag{28}$$

где $m = \nu_p(\xi)$, $1 \leqslant a_0 \leqslant p-1$, $0 \leqslant a_n \leqslant p-1$ $(n = 1, 2, \ldots)$.

Замечание. Приведенное нами построение кольца целых p-адических чисел является частным случаем одной общей конструкции, применяющейся в топологии и алгебре,— конструкции проективного предела обратного спектра топологических пространств, групп, колец и т. п. (с этим понятием можно ознакомиться, например, по книге [4], гл. III). Именно, кольцо $\mathbb{Z}_p$ можно

интерпретировать также как проективный предел обратного спектра колец вычетов $\Omega_i = \mathbb{Z}/p^i\mathbb{Z}$ относительно естественных гомоморфизмов $\Omega_j \to \Omega_i$ $(j > i)$. При этом топология на $\mathbb{Z}_p$, вносимая понятием сходимости (см. п. 4) будет совпадать с топологией, возникающей на проективном пределе конечных колец Ω_i, если последние рассматривать как топологические пространства с дискретной топологией.

Задачи

1. Положим $x_n = 1 + p + \ldots + p^{n-1}$. Показать, что в поле p-адических чисел последовательность $\{x_n\}$ сходится к $1/(1-p)$.

2. Пусть $p \neq 2$ и c — квадратичный вычет по модулю p. Доказать, что существуют два (различных) p-адических числа, квадраты которых равны c.

3. Пусть c — целое рациональное число, не делящееся на p. Показать, что в поле $\mathbb{Q}_p$ последовательность $\{c^{p^n}\}$ сходится. Доказать, далее, что для предела γ этой последовательности имеем: $\gamma \equiv c \pmod p$ и $\gamma^{p-1} = 1$.

4. Используя предыдущую задачу, показать, что в поле $\mathbb{Q}_p$ многочлен $t^{p-1} - 1$ раскладывается целиком на линейные множители.

5. Представить число -1 в поле p-адических чисел в виде ряда (26).

6. Представить число $-2/3$ в виде ряда (26) в поле 5-адических чисел.

7. Доказать, что при $p \neq 2$ в поле p-адических чисел не существует корней p-й степени из 1, отличных от 1.

8. Доказать, что представление рационального числа $\neq 0$ в поле $\mathbb{Q}_p$ в виде ряда (28) имеет периодические коэффициенты (начиная с некоторого места). Обратно, всякий ряд вида (28), для коэффициентов которого имеем $a_{m+k} = a_k$ при всех $k \geqslant k_0$ $(m > 0)$, представляет рациональное число.

9. Доказать для многочленов над полем p-адических чисел признак неприводимости Эйзенштейна: многочлен $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ с целыми p-адическими коэффициентами неприводим над полем $\mathbb{Q}_p$, если a_0 не делится на p, все остальные коэффициенты $a_1, \ldots, a_n$ делятся на p и свободный член a_n, делясь на p, не делится на p^2.

10. Показать, что над полем p-адических чисел существуют конечные расширения произвольной степени.

11. Доказать, что для различных простых p и q поля $\mathbb{Q}_p$ и $\mathbb{Q}_q$ не изоморфны. Доказать также, что всякое поле $\mathbb{Q}_p$ не изоморфно полю вещественных чисел.

12. Доказать, что поле p-адических чисел не имеет никаких автоморфизмов, кроме тождественного. (Аналогичное утверждение справедливо и для поля вещественных чисел.)

13. Пусть α — *главная* p-адическая единица, т. е. $\alpha \in \mathbb{Z}_p$ и $\alpha \equiv 1 \pmod p$. Положим $\nu(\alpha - 1) = m$. Доказать, что если $\alpha \neq 1$ и $p \neq 2$, то $\nu(\alpha^p - 1) = m + 1$. Доказать, далее, что последняя формула справедлива и при $p = 2$, если только $m \geqslant 2$.

14. Для главной p-адической единицы α и целого p-адического x положим $\alpha^x = \lim\limits_{n\to\infty} \alpha^{x_n}$, где $\{x_n\}$ — произвольная последовательность натуральных чисел, сходящаяся к x. Доказать, что этим однозначно определена функция α^x, непрерывно и гомоморфно отображающая аддитивную группу целых p-адических чисел в мультипликативную группу главных p-адических единиц.

15. Для α и x из задачи 14 доказать формулу

$$\nu(\alpha^x - 1) = \nu(\alpha - 1) + \nu(x)$$

(при $p = 2$ предполагается, что $\nu_2(\alpha - 1) \geqslant 2$; задача 13).

16. Доказать, что при $p \neq 2$ любая p-адическая единица ε однозначно представляется в виде

$$\varepsilon = \gamma(1+p)^a, \qquad \gamma^{p-1} = 1, \qquad a \in \mathbb{Z}_p$$

(см. задачи 3 и 14). Доказать также, что всякая 2-адическая единица ε однозначно представляется в виде $\varepsilon = \pm 5^a$, $a \in \mathbb{Z}_2$.

17. Доказать, что $v_p(n!) < n$.

18. Пусть Z_m — кольцо классов вычетов $\mathbb{Z}/m\mathbb{Z}$ по натуральному модулю m. Если n делится на m, то мы имеем естественный кольцевой эпиморфизм $f_m^n\colon Z_n \to Z_m$. Обозначим через $\widetilde{Z}$ проективный предел обратного спектра колец $\{Z_m, f_m^n\}$ (частично упорядоченного отношением делимости). Доказать, что кольцо $\widetilde{Z}$ изоморфно декартову произведению $\prod_p \mathbb{Z}_p$ колец целых p-адических чисел для всех простых чисел p. (Если на $\widetilde{Z}$ ввести топологию посредством дискретной топологии на Z_m, то кольца $\widetilde{Z}$ и $\prod_p \mathbb{Z}_p$ будут топологически изоморфны.)

§ 4. Аксиоматическая характеристика поля p-адических чисел

Поля p-адических чисел принадлежат к числу основных инструментов теории чисел. Следующие параграфы этой главы будут посвящены их приложениям к некоторым теоретико-числовым задачам. Сейчас, однако, мы несколько отвлечемся от основной темы главы, чтобы уяснить себе место полей p-адических чисел в общей теории полей.

1. Метризованные поля. Мы же несколько раз указывали на аналогию между p-адическими и вещественными числами. В настоящем параграфе мы придадим этой аналогии более точный смысл. Именно, мы здесь опишем один общий метод построения полей, охватывающий в качестве частных случаев построение как вещественных, так и p-адических чисел. Этот метод для случая поля вещественных чисел совпадает с методом Кантора построения вещественных чисел при помощи фундаментальных последовательностей рациональных чисел.

Перенесение метода Кантора на другие поля основывается на следующем соображении. Все понятия и конструкции, необходимые для проведения этого метода, определяются через понятие сходимости последовательности рациональных чисел. Само это понятие в свою очередь опирается на понятие абсолютной величины. (Мы говорим, что последовательность рациональных чисел $\{r_n\}$ сходится к рациональному числу r, если абсолютная величина разности $|r_n - r|$ стремится к нулю.) При этом можно заметить, что всюду используется только несколько простых свойств абсолютной величины. Естественно поэтому предположить, что если в произвольном поле k определена функция φ от элементов этого поля, принимающая вещественные значения и обладающая

теми же основными свойствами, что и абсолютная величина, то в k можно определить понятие сходимости и, применяя метод Кантора, построить из k некоторое новое поле.

Определение. *Пусть k — произвольное поле. Функция φ, определенная на элементах α поля k и принимающая вещественные значения $\varphi(\alpha)$, называется метрикой поля k, если она обладает следующими свойствами:*

1° $\varphi(\alpha) > 0$ *при* $\alpha \neq 0$; $\varphi(0) = 0$;

2° $\varphi(\alpha + \beta) \leqslant \varphi(\alpha) + \varphi(\beta)$;

3° $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$.

Поле k вместе с заданной в нем метрикой φ называется метризованным полем (и обозначается иногда через (k, φ)). Из определения легко вытекают следующие свойства метрик:

$$\varphi(\pm 1) = 1; \quad \varphi(-\alpha) = \varphi(\alpha); \quad \varphi(\alpha - \beta) \leqslant \varphi(\alpha) + \varphi(\beta);$$

$$\varphi(\alpha \pm \beta) \geqslant |\varphi(\alpha) - \varphi(\beta)|; \quad \varphi\left(\frac{\alpha}{\beta}\right) = \frac{\varphi(\alpha)}{\varphi(\beta)}, \quad \beta \neq 0.$$

Примерами метрик являются:

1) абсолютная величина в поле рациональных чисел;

2) абсолютная величина в поле вещественных чисел;

3) модуль в поле комплексных чисел;

4) определенная в п. 4 § 3 p-адическая метрика φ_p в поле p-адических чисел $\mathbb{Q}_p$;

5) функция $\varphi(\alpha)$, определенная в произвольном поле k условиями: $\varphi(0) = 0$, $\varphi(\alpha) = 1$ при $\alpha \neq 0$. Такая метрика называется тривиальной.

Если метрику φ_p поля $\mathbb{Q}_p$ мы рассмотрим лишь на рациональных числах, то получим некоторую новую метрику поля рациональных чисел $\mathbb{Q}$. Эта метрика, обозначаемая также через φ_p, называется p-адической метрикой поля $\mathbb{Q}$. Ее значение для отличного от нуля рационального числа $x = p^{v_p(x)}a/b$ (a и b — целые, не делящиеся на p) задается, очевидно, формулой

$$\varphi_p(x) = \rho^{v_p(x)}, \tag{1}$$

где ρ — фиксированное вещественное число, удовлетворяющее условию $0 < \rho < 1$. Ниже мы увидим, что применение конструкции Кантора к полю рациональных чисел с p-адической метрикой на нем (вместо абсолютной величины) и приводит нас к полю p-адических чисел $\mathbb{Q}_p$.

В каждом метризованном поле (k, φ) может быть определено понятие сходимости: последовательность $\{\alpha_n\}$ элементов из k называется сходящейся к элементу $\alpha \in k$, если $\varphi(\alpha_n - \alpha) \to 0$ при $n \to \infty$. В этом случае говорят также, что α является пределом последовательности $\{\alpha_n\}$, и пишут $\{\alpha_n\} \to \alpha$ или $\alpha = \lim\limits_{n\to\infty} \alpha_n$.

Определение. *Последовательность* $\{\alpha_n\}$ *элементов метризованного поля* k *с метрикой* φ *называется фундаментальной, если* $\varphi(\alpha_n - \alpha_m) \to 0$ *при* $n, m \to \infty$.

Очевидно, что всякая сходящаяся последовательность фундаментальна. Действительно, если $\{\alpha_n\} \to \alpha$, то, в силу неравенства

$$\varphi(\alpha_n - \alpha_m) = \varphi(\alpha_n - \alpha + \alpha - \alpha_m) \leqslant \varphi(\alpha_n - \alpha) + \varphi(\alpha_m - \alpha),$$

$\varphi(\alpha_n - \alpha_m) \to 0$ (так как $\varphi(\alpha_n - \alpha) \to 0$ и $\varphi(\alpha_m - \alpha) \to 0$).

Обратное утверждение справедливо для некоторых, но не для всех метризованных полей. Оно верно для поля вещественных и для поля p-адических чисел в силу критерия сходимости Коши (см. § 3, п. 4). В то же время оно неверно для поля рациональных чисел $\mathbb{Q}$, какой бы из известных нам метрик мы его ни снабжали — абсолютной величиной или p-адической метрикой.

Определение. *Метризованное поле называется полным, если в нем любая фундаментальная последовательность сходится.*

Метод Кантора состоит во вложении неполного поля рациональных чисел (с абсолютной величиной в качестве метрики) в полное поле вещественных чисел. Оказывается, что такое вложение возможно и для любого метризованного поля, причем доказательство этого утверждения почти дословно повторяет то, которое приводится в методе Кантора.

Условимся в следующей терминологии. Если мы говорим, что метризованное поле (k, φ) является подполем метризованного поля (k_1, φ_1), то, помимо включения $k \subset k_1$, подразумеваем также, что метрика φ_1 на подполе k совпадает с φ. Далее, подмножество метризованного поля k будем называть всюду плотным в k, если всякий элемент из k является пределом некоторой сходящейся последовательности элементов из этого подмножества.

Имеет место

Теорема 1. *Для любого метризованного поля* k *существует полное метризованное поле* $\bar{k}$, *содержащее* k *в качестве всюду плотного подполя.*

Для формулировки следующей теоремы нам необходимо еще одно определение.

Определение. *Пусть* (k_1, φ_1) *и* (k_2, φ_2) *— два изоморфных между собой метризованных поля. Изоморфизм* $\sigma\colon k_1 \to k_2$ *называется непрерывным в обе стороны или топологическим, если для всякой последовательности* $\{\alpha_n\}$ *элементов из* k_1, *сходящейся к элементу* α *по метрике* φ_1, *последовательность* $\{\sigma(\alpha_n)\}$ *сходится к* $\sigma(\alpha)$ *по метрике* φ_2, *и обратно.*

Теорема 2. *Поле* $\bar{k}$, *о котором говорится в теореме* 1, *определено однозначно с точностью до топологического изоморфизма, оставляющего на месте элементы поля* k.

Определение. *Поле* $\bar{k}$, *существование и единственность которого устанавливается теоремами* 1 *и* 2, *называется пополнением метризованного поля* k.

Ясно, что поле вещественных чисел является пополнением поля рациональных чисел $\mathbb{Q}$, снабженного абсолютной величиной в качестве метрики. Если же снабдить поле рациональных чисел p-адической метрикой (1), то пополнением этого метризованного поля будет поле p-адических чисел $\mathbb{Q}_p$. Действительно, второе утверждение теоремы 5 § 3 показывает, что $\mathbb{Q}$ всюду плотно в $\mathbb{Q}_p$, а признак сходимости Коши (теорема 7 § 3) утверждает полноту $\mathbb{Q}_p$. Мы получили, таким образом, новое аксиоматическое определение поля p-адических чисел:

Поле p-адических чисел — это пополнение поля рациональных чисел по p-адической метрике (1).

Перейдем к доказательствам теорем 1 и 2. Мы приведем только схему этих доказательств, пропуская те места, которые дословно повторяют соответствующие рассуждения вещественного анализа.

Доказательство теоремы 1. Назовем две фундаментальные последовательности $\{x_n\}$ и $\{y_n\}$ элементов метризованного поля (k, φ) эквивалентными, если $\{x_n - y_n\} \to 0$. Совокупность всех эквивалентных друг другу фундаментальных последовательностей назовем классом, а совокупность всех классов обозначим через $\bar{k}$. В множестве $\bar{k}$ определяем следующим образом действия сложения и умножения: если α и β — два класса и $\{x_n\} \in \alpha$ и $\{y_n\} \in \beta$ — любые содержащиеся в них фундаментальные последовательности, то суммой (соответственно произведением) классов α и β назовем класс, содержащий последовательность $\{x_n + y_n\}$ (соответственно $\{x_n y_n\}$). Легко видеть, что $\{x_n + y_n\}$ и $\{x_n y_n\}$ действительно являются фундаментальными последовательностями и что классы, которым они принадлежат, не зависят от выбора последовательностей $\{x_n\}$ и $\{y_n\}$ в классах α и β.

Очевидная проверка показывает, что $\bar{k}$ является кольцом с единицей; нулем и единицей являются классы, содержащие последовательности $\{0, 0, \ldots\}$ и $\{1, 1, \ldots\}$.

Докажем, что $\bar{k}$ является полем. Если α — класс, отличный от нуля, и $\{x_n\}$ — содержащаяся в нем фундаментальная последовательность, то, как легко видеть, все x_n, начиная с некоторого места (например, при $n \geqslant n_0$), отличны от нуля.

Рассмотрим последовательность $\{y_n\}$, определенную условиями:

$$y_n = \begin{cases} 1 & \text{при } n < n_0, \\ 1/x_n & \text{при } n \geqslant n_0. \end{cases}$$

Простая проверка показывает, что последовательность $\{y_n\}$ фундаментальна и что класс, в котором она содержится, является обратным к классу α.

Введем теперь в поле $\bar{k}$ метрику. Для этого заметим, что, как легко доказать, если $\{x_n\}$ — фундаментальная последовательность элементов поля k, то $\{\varphi(x_n)\}$ является фундаментальной последо-

вательностью вещественных чисел. Ввиду полноты поля вещественных чисел эта последовательность сходится к некоторому вещественному числу, которое не изменится, если заменить последовательность $\{x_n\}$ эквивалентной. Положим $\varphi(\alpha) = \lim_{n\to\infty} \varphi(x_n)$, если α — класс, содержащий последовательность $\{x_n\}$. Нетрудно доказать, что определенная таким образом функция $\varphi(\alpha)$ удовлетворяет всем условиям, входящим в определение метрики, и, следовательно, превращает $\bar{k}$ в метризованное поле.

Сопоставим любому элементу a поля k класс, содержащий последовательность $\{a, a, \ldots\}$. Мы получим отображение поля k в $\bar{k}$, устанавливающее, как легко видеть, изоморфизм метризованного поля k с подполем поля $\bar{k}$, сохраняющим значение метрики. Мы не будем дальше отличать элемент поля k от соответствующего ему элемента поля $\bar{k}$ и будем считать, что k содержится в $\bar{k}$. Очевидно, что k всюду плотно в $\bar{k}$; действительно, если α — класс, содержащий фундаментальную последовательность $\{x_n\}$, то $\{x_n\} \to \alpha$.

Нам остается доказать последнее свойство поля $\bar{k}$ — его полноту. Пусть $\{\alpha_n\}$ — фундаментальная последовательность элементов поля $\bar{k}$. Так как α_n является пределом последовательности элементов поля k, то существует элемент $x_n \in k$, для которого $\varphi(\alpha_n - x_n) < 1/n$.

Из фундаментальности последовательности $\{\alpha_n\}$ немедленно следует, что и последовательность $\{x_n\}$, состоящая уже из элементов поля k, является фундаментальной. Обозначим через α класс, содержащий последовательность $\{x_n\}$. Простая проверка показывает, что $\{\alpha_n\} \to \alpha$, что и завершает доказательство теоремы 1.

Доказательство теоремы 2. Пусть $\bar{k}$ и $\bar{k}_1$ — два полных поля, содержащих k в качестве всюду плотного подполя. Мы укажем только, как устанавливается соответствие между элементами полей $\bar{k}$ и $\bar{k}_1$. Проверку того, что это соответствие является топологическим изоморфизмом, переводящим элементы k в себя, мы предоставим читателю.

Пусть α — элемент поля $\bar{k}$. По условию существует такая последовательность $\{x_n\}$ элементов поля k, что $\{x_n\} \to \alpha$. Так как последовательность $\{x_n\}$ сходится в $\bar{k}$, то она является фундаментальной. Это свойство сохранится и тогда, когда мы рассмотрим ее как последовательность элементов поля k. Ввиду полноты поля $\bar{k}_1$ последовательность $\{x_n\}$ сходится в нем к некоторому пределу, который мы обозначим α_1. Легко доказать, что если $\{y_n\}$ — другая последовательность элементов поля k, сходящаяся в $\bar{k}$ к α, то предел $\{y_n\}$ в поле $\bar{k}_1$ будет тем же элементом α_1. Таким образом, элемент α_1 поля $\bar{k}_1$ однозначно определяется элементом α поля $\bar{k}$. Соответствие, сопоставляющее элементу α элемент α_1, и является нужным нам изоморфизмом.

2. Метрики поля рациональных чисел. В связи с результатами предыдущего пункта естественно возникает вопрос, существуют ли, помимо поля вещественных чисел и полей p-адических чисел (для всех простых p), другие пополнения поля рациональных чисел $\mathbb{Q}$. Ответ оказывается отрицательным: перечисленные поля исчерпывают собой все возможные пополнения поля $\mathbb{Q}$. Доказательство этого факта и является нашей ближайшей целью.

Ясно, что поднятый нами вопрос сводится к перечислению всех метрик поля $\mathbb{Q}$.

В определении p-адической метрики φ_p на поле $\mathbb{Q}$ участвует некоторое вещественное число ρ, от которого требуется лишь, чтобы оно удовлетворяло условию $0<\rho<1$ (см. равенство (1), а также (18) § 3). Таким образом, мы имеем бесконечно много метрик, связанных с данным простым числом p. Однако все они определяют, очевидно, одну и ту же сходимость на $\mathbb{Q}$ и, следовательно, приводят к одному и тому же пополнению — к полю p-адических чисел $\mathbb{Q}_p$.

Покажем, что наряду с абсолютной величиной $|x|$ функция

$$\varphi(x)=|x|^\alpha \tag{2}$$

при любом вещественном α, удовлетворяющем условию $0<\alpha\leqslant 1$, также является метрикой поля $\mathbb{Q}$. Действительно, выполнение условий 1° и 3° из определения метрики очевидно. Пусть $|x|\geqslant |y|$, $x\neq 0$. Тогда

$$|x+y|^\alpha=|x|^\alpha\left|1+\frac{y}{x}\right|^\alpha\leqslant |x|^\alpha\left(1+\left|\frac{y}{x}\right|\right)^\alpha\leqslant$$

$$\leqslant |x|^\alpha\left(1+\left|\frac{y}{x}\right|^\alpha\right)\leqslant |x|^\alpha\left(1+\left|\frac{y}{x}\right|^\alpha\right)=|x|^\alpha+|y|^\alpha,$$

т. е. условие 2° также выполнено.

Сходимость в $\mathbb{Q}$ по любой из метрик вида (2) совпадает, очевидно, со сходимостью по абсолютной величине, а значит, процесс пополнения по всем этим метрикам приводит всякий раз к полю вещественных чисел.

Теорема 3 (теорема Островского). *Метрики вида* (2) *и* p-*адические метрики* (1) *для всех простых* p *исчерпывают все нетривиальные метрики поля рациональных чисел* $\mathbb{Q}$.

Доказательство. Пусть φ — произвольная нетривиальная метрика поля рациональных чисел. Возможны два случая: либо существует хоть одно натуральное $a>1$, для которого $\varphi(a)>1$, либо $\varphi(n)\leqslant 1$ при всех натуральных n. Рассмотрим сначала первый случай. Так как

$$\varphi(n)=\varphi(1+\ldots+1)\leqslant\varphi(1)+\ldots+\varphi(1)=n, \tag{3}$$

то можно положить

$$\varphi(a)=a^\alpha, \tag{4}$$

где вещественное α удовлетворяет условию $0<\alpha\leqslant 1$.

Взяв произвольное натуральное N, разложим его по степеням a:

$$N = x_0 + x_1 a + \ldots + x_{k-1} a^{k-1},$$

где $0 \leqslant x_i \leqslant a-1$ $(0 \leqslant i \leqslant k-1)$, $x_{k-1} \geqslant 1$. Для N имеет место, следовательно, неравенство $a^{k-1} \leqslant N < a^k$. В силу свойств метрики и формул (3) и (4), получаем

$$\varphi(N) \leqslant \varphi(x_0) + \varphi(x_1)\varphi(a) + \ldots + \varphi(x_{k-1})\varphi(a)^{k-1} \leqslant$$

$$\leqslant (a-1)(1 + a^\alpha + \ldots + a^{(k-1)\alpha}) = (a-1)\frac{a^{k\alpha}-1}{a^\alpha - 1} <$$

$$< (a-1)\frac{a^{k\alpha}}{a^\alpha - 1} = \frac{(a-1)a^\alpha}{a^\alpha - 1} a^{(k-1)\alpha} \leqslant \frac{(a-1)a^\alpha}{a^\alpha - 1} N^\alpha = CN^\alpha,$$

т. е. $\varphi(N) < CN^\alpha$, где константа C не зависит от N. В полученном неравенстве заменим N на N^m с натуральным m. Мы получим $\varphi(N)^m = \varphi(N^m) < CN^{m\alpha}$, откуда $\varphi(N) < \sqrt[m]{C}N^\alpha$. Устремляя здесь m к бесконечности, приходим к неравенству

$$\varphi(N) \leqslant N^\alpha. \tag{5}$$

Положим теперь $N = a^k - b$, где $0 < b \leqslant a^k - a^{k-1}$. В силу 2° имеем

$$\varphi(N) \geqslant \varphi(a^k) - \varphi(b) = a^{\alpha k} - \varphi(b).$$

По только что доказанному

$$\varphi(b) \leqslant b^\alpha \leqslant (a^k - a^{k-1})^\alpha,$$

поэтому

$$\varphi(N) \geqslant a^{\alpha k} - (a^k - a^{k-1})^\alpha = \left(1 - \left(1 - \frac{1}{a}\right)^\alpha\right) a^{\alpha k} = C_1 a^{\alpha k} > C_1 N^\alpha,$$

где константа C_1 не зависит от N. Пусть снова m — произвольное натуральное число. Заменяя в последнем неравенстве N на N^m, получаем $\varphi(N)^m = \varphi(N^m) > C_1 N^{\alpha m}$, откуда $\varphi(N) > \sqrt[m]{C_1}N^\alpha$, а это при $m \to \infty$ дает нам

$$\varphi(N) \geqslant N^\alpha. \tag{6}$$

Сопоставляя (5) и (6), видим, что $\varphi(N) = N^\alpha$ для любого натурального N. Пусть теперь $x = \pm N_1/N_2$ — произвольное рациональное число, отличное от нуля (N_1 и N_2 натуральные). Тогда

$$\varphi(x) = \varphi(N_1/N_2) = \varphi(N_1)/\varphi(N_2) = N_1^\alpha / N_2^\alpha = |x|^\alpha.$$

Мы доказали, таким образом, что если $\varphi(a) > 1$ хоть при одном натуральном a, то метрика φ имеет вид (2).

Перейдем теперь к рассмотрению случая, когда

$$\varphi(n) \leqslant 1 \tag{7}$$

при всех натуральных n. Если бы для всех простых чисел p мы имели $\varphi(p) = 1$, то в силу свойства 3° мы имели бы также $\varphi(n) = 1$ при всех натуральных n и, следовательно, $\varphi(x) = 1$ при всех рациональных $x \neq 0$. Это противоречит, однако, нетривиальности метрики φ. Таким образом, для некоторого простого p имеем $\varphi(p) < 1$. Допустим, что для некоторого другого простого числа $q \neq p$ также имеем $\varphi(q) < 1$. Выберем показатели k и l так, чтобы выполнялись неравенства

$$\varphi(p)^k < 1/2, \quad \varphi(q)^l < 1/2.$$

Так как p^k и q^l взаимно просты, то $up^k + vq^l = 1$ при некоторых целых рациональных u и v. В силу (7) имеем $\varphi(u) \leqslant 1$ и $\varphi(v) \leqslant 1$, поэтому

$$1 = \varphi(1) = \varphi(up^k + vq^l) \leqslant \varphi(u)\,\varphi(p)^k + \varphi(v)\,\varphi(q)^l < \frac{1}{2} + \frac{1}{2}.$$

Полученное противоречие показывает, что существует только одно простое число p, для которого

$$\varphi(p) = \rho < 1.$$

Так как $\varphi(q) = 1$ для всех других простых чисел, то, очевидно, $\varphi(a) = 1$ для всех целых a, взаимно простых с p. Пусть $x = p^m a/b$ — отличное от нуля рациональное число (a и b целые, взаимно простые с p). Тогда

$$\varphi(x) = \varphi(p^m)\frac{\varphi(a)}{\varphi(b)} = \varphi(p)^m = \rho^m.$$

Таким образом, в этом случае метрика φ совпадает с p-адической метрикой (1).

Доказательство теоремы 3 окончено.

Задачи

1. Показать, что на конечном поле существует только одна метрика — тривиальная.

2. Две метрики φ и ψ, заданные на одном и том же поле k, называются эквивалентными, если они определяют на k одинаковые сходимости, т. е. если условия $\varphi(x_n - x) \to 0$ и $\psi(x_n - x) \to 0$ равносильны. Доказать, что для эквивалентности φ и ψ необходимо и достаточно, чтобы условия $\varphi(x) < 1$ и $\psi(x) < 1$ ($x \in k$) были равносильны.

3. Доказать, что если φ и ψ — эквивалентные метрики поля k, то $\varphi(x) = (\psi(x))^\delta$ при всех $x \in k$ (δ — некоторое вещественное число).

4. Метрика φ, заданная на некотором поле k, называется *неархимедовой*, если она удовлетворяет не только условию 2°, но и более сильному условию

$$2^{\circ\circ} \qquad \varphi(\alpha + \beta) \leqslant \max(\varphi(\alpha), \varphi(\beta)).$$

(Если же это более сильное условие не выполняется, то метрика φ называется *архимедовой*.) Доказать, что метрика φ неархимедова тогда и только тогда, когда $\varphi(n) \leqslant 1$ для любого натурального n (точнее, для любого натурального кратного единичного элемента поля k).

5. Показать, что всякая метрика поля характеристики p неархимедова.

6. Пусть k_0 — произвольное поле и $k = k_0(t)$ — поле рациональных функций над k_0. Каждую отличную от нуля рациональную функцию $u \in k$ можно представить в виде

$$u = t^m \frac{f(t)}{g(t)}, \qquad f(0) \neq 0, \quad g(0) \neq 0,$$

где f и g — многочлены. Показать, что функция

$$\varphi(u) = \rho^m \quad (0 < \rho < 1), \qquad \varphi(0) = 0, \tag{8}$$

является метрикой поля k.

7. Доказать, что пополнение поля $k = k_0(t)$ по метрике (8) изоморфно полю $k_0\{t\}$ формальных степенных рядов, состоящему из всех рядов вида $\sum_{n=m}^{\infty} a_n t^n$, $a_n \in k_0$, с обычными правилами действий над степенными рядами (число m может быть положительным, отрицательным или равным нулю).

§ 5. Сравнения и целые p-адические числа

1. Сравнения и уравнения в кольце $\mathbb{Z}_p$. В начале § 3 мы рассмотрели вопрос о разрешимости сравнений $x^2 \equiv 2 \pmod{7^n}$ при $n = 1, 2, \ldots$, и это привело нас к понятию целого p-адического числа. Уже само определение целых p-адических чисел (§ 3, п. 1) указывает на их глубокую связь со сравнениями. Более полно эта связь вскрывается следующей теоремой.

Теорема 1. *Пусть $F(x_1, \ldots, x_n)$ — многочлен с целыми рациональными коэффициентами. Сравнения*

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p^k} \tag{1}$$

тогда и только тогда разрешимы при любом $k \geqslant 1$, когда уравнение

$$F(x_1, \ldots, x_n) = 0 \tag{2}$$

разрешимо в целых p-адических числах.

Доказательство. Пусть уравнение (2) имеет решение $(\alpha_1, \ldots, \alpha_n)$ в целых p-адических числах. Для любого k существуют тогда такие целые рациональные числа $x_1^{(k)}, \ldots, x_n^{(k)}$, что

$$\alpha_1 \equiv x_1^{(k)} \pmod{p^k}, \ldots, \alpha_n \equiv x_n^{(k)} \pmod{p^k}. \tag{3}$$

Отсюда следует, что

$$F\left(x_1^{(k)}, \ldots, x_n^{(k)}\right) \equiv F(\alpha_1, \ldots, \alpha_n) \equiv 0 \pmod{p^k},$$

т. е. $\left(x_1^{(k)}, \ldots, x_n^{(k)}\right)$ есть решение сравнения (1).

Предположим теперь, что сравнение (1) для любого k имеет решение $\left(x_1^{(k)}, \ldots, x_n^{(k)}\right)$. Выберем из последовательности целых рациональных чисел $\{x_1^{(k)}\}$ p-адически сходящуюся подпоследовательность $\{x_1^{(k_i)}\}$ (теорема 6 § 3). Из последовательности $\{x_2^{(k_i)}\}$

выберем опять сходящуюся подпоследовательность. Повторяя этот процесс n раз, мы придем к такой подпоследовательности натурального ряда $\{l_1, l_2, \ldots\}$, что каждая из последовательностей $\{x_i^{(l_1)}, x_i^{(l_2)}, \ldots\}$ p-адически сходится. Пусть

$$\lim_{m\to\infty} x_i^{(l_m)} = \alpha_i.$$

Докажем, что $(\alpha_1, \ldots, \alpha_n)$ — решение уравнения (2). Так как многочлен $F(x_1, \ldots, x_n)$ — непрерывная функция, то

$$F(\alpha_1, \ldots, \alpha_n) = \lim_{m\to\infty} F\left(x_1^{(l_m)}, \ldots, x_n^{(l_m)}\right).$$

С другой стороны, по выбору последовательности $\left(x_1^{(k)}, \ldots, x_n^{(k)}\right)$

$$F\left(x_1^{(l_m)}, \ldots, x_n^{(l_m)}\right) \equiv 0 \pmod{p^{l_m}},$$

так что $\lim_{m\to\infty} F\left(x_1^{(l_m)}, \ldots, x_n^{(l_m)}\right) = 0$. Таким образом, $F(\alpha_1, \ldots, \alpha_n) = 0$, и теорема 1 доказана.

Рассмотрим теперь случай, когда $F(x_1, \ldots, x_n)$ — форма с целыми рациональными коэффициентами. Допустим, что уравнение $F(x_1, \ldots, x_n) = 0$ имеет ненулевое решение $(\bar{\alpha}_1, \ldots, \bar{\alpha}_n)$ в целых p-адических числах. Пусть $m = \min(\nu_p(\bar{\alpha}_1), \ldots, \nu_p(\bar{\alpha}_n))$. Тогда все $\bar{\alpha}_i$ представляются в виде

$$\bar{\alpha}_i = p^m \alpha_i, \quad i = 1, \ldots, n,$$

причем все α_i целые и хотя бы одно из них не делится на p. Ясно, что $(\alpha_1, \ldots, \alpha_n)$ — также решение уравнения $F(x_1, \ldots, x_n) = 0$. Числа $\left(x_1^{(k)}, \ldots, x_n^{(k)}\right)$, удовлетворяющие условиям (3), дают, как мы видели, решение сравнения (1), причем хотя бы одно из них не делится на p.

Допустим, что, наоборот, сравнение (1) при однородном F имеет при любом k решение $\left(x_1^{(k)}, \ldots, x_n^{(k)}\right)$, в котором хотя бы одно из чисел $x_i^{(k)}$ не делится на p. Ясно, что для некоторого индекса $i = i_0$ будет существовать бесконечно много значений m, при которых $x_{i_0}^{(m)}$ не делится на p. Поэтому последовательность $\{l_1, l_2, \ldots\}$ мы можем выбрать так, чтобы все $x_{i_0}^{(l_m)}$ не делились на p. Но тогда из равенства $\alpha_{i_0} = \lim x_{i_0}^{(l_m)}$ следует, что α_{i_0} не делится на p, а значит, и подавно $\alpha_{i_0} \neq 0$. Этим доказана следующая теорема.

Теорема 2. *Пусть $F(x_1, \ldots, x_n)$ — форма с целыми рациональными коэффициентами. Тогда, для того чтобы уравнение $F(x_1, \ldots, x_n) = 0$ имело в кольце $\mathbb{Z}_p$ нетривиальное решение, не-*

обходимо и достаточно, чтобы при любом натуральном m для сравнения $F(x_1, \ldots, x_n) \equiv 0 \pmod{p^m}$ существовало решение, в котором не все значения неизвестных делятся на p.

Очевидно, что в теоремах 1 и 2 под F можно также понимать многочлены с целыми p-адическими коэффициентами.

2. О разрешимости некоторых сравнений. Доказанная в предыдущем пункте теорема 1 сводит вопрос о разрешимости уравнения (2) в целых p-адических числах к проверке разрешимости бесконечной серии сравнений (1). Вопрос о том, как ограничиться рассмотрением только конечного числа из этих сравнений, в общем случае довольно сложен. Мы ограничимся здесь рассмотрением одного частного случая.

Теорема 3. *Пусть для многочлена $F(x_1, \ldots, x_n)$ с целыми p-адическими коэффициентами и целых p-адических чисел $\gamma_1, \ldots, \gamma_n$ при некотором i $(1 \leqslant i \leqslant n)$ имеем:*

$$F(\gamma_1, \ldots, \gamma_n) \equiv 0 \pmod{p^{2\delta+1}},$$

$$\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \equiv 0 \pmod{p^{\delta}},$$

$$\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \pmod{p^{\delta+1}}$$

(δ — неотрицательное целое рациональное число). Тогда существуют такие целые p-адические $\theta_1, \ldots, \theta_n$, что

$$F(\theta_1, \ldots, \theta_n) = 0$$

и

$$\theta_1 \equiv \gamma_1 \pmod{p^{\delta+1}}, \ldots, \theta_n \equiv \gamma_n \pmod{p^{\delta+1}}.$$

Доказательство. Положим $\gamma_i = \gamma$ и

$$f(x) = F(\gamma_1, \ldots, \gamma_{i-1}, x, \gamma_{i+1}, \ldots, \gamma_n).$$

Для доказательства теоремы нам достаточно показать, что для многочлена $f(x)$, для которого

$$f(\gamma) \equiv 0 \pmod{p^{2\delta+1}} \quad \text{и} \quad f'(\gamma) = up^{\delta}$$

(где u — p-адическая единица), существует такое целое p-адическое число α, что

$$f(\alpha) = 0 \text{ и } \alpha \equiv \gamma \pmod{p^{\delta+1}}$$

(если такое α будет найдено, то можно положить $\theta_j = \gamma_j$ при $j \neq i$ и $\theta_i = \alpha$).

Существование α мы докажем способом, совпадающим по существу с известным методом Ньютона приближенного вычисления вещественных корней (некоторое видоизменение вызвано специфическими отличиями поля p-адических чисел от поля вещественных чисел).

Отправляясь от $\alpha_0 = \gamma$, построим индуктивно последовательность $\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots$, полагая

$$\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}, \tag{4}$$

и докажем, что все α_n — целые p-адические числа и для них

$$f(\alpha_n) \equiv 0 \pmod{p^{2\delta+1+n}}, \quad n \geqslant 0, \tag{4'}$$

$$\alpha_n \equiv \alpha_{n-1} \pmod{p^{\delta+n}}, \quad n \geqslant 1. \tag{4''}$$

Доказательство сравнений (4′) и (4″) мы проведем индукцией по n. Пусть эти сравнения справедливы для некоторого $n \geqslant 0$ (при $n = 0$ речь идет только о (4′)). Так как

$$\alpha_n \equiv \alpha_0 \pmod{p^{\delta+1}},$$

то $f'(\alpha_n) \equiv f'(\alpha_0) = up^{\delta}$, а значит, $f'(\alpha_n) = u_n p^{\delta}$, где u_n — p-адическая единица. Следовательно, ввиду (4′) α_{n+1} целое и $\alpha_{n+1} \equiv \alpha_n \pmod{p^{\delta+n+1}}$.

Далее, разложим многочлен $f(x)$ по степеням $x - \alpha_n$, объединив вместе все члены степени выше первой:

$$f(x) = f(\alpha_n) + f'(\alpha_n)(x - \alpha_n) + (x - \alpha_n)^2 G(x),$$

где $G(x)$ — многочлен с целыми p-адическими коэффициентами. Полагая здесь $x = \alpha_{n+1}$ и учитывая (4), мы получим

$$f(\alpha_{n+1}) = \left(\frac{f(\alpha_n)}{f'(\alpha_n)}\right)^2 G(\alpha_{n+1}),$$

откуда $f(\alpha_{n+1}) \equiv 0 \pmod{p^{2\delta+2+2n}}$. Сравнения (4′) и (4″) справедливы, таким образом, для всех n.

Из (4″) следует, что последовательность $\{\alpha_n\}_{n=0}^{\infty}$ сходится. Обозначим ее предел через α. Ясно, что $\alpha \equiv \alpha_0 = \gamma \pmod{p^{\delta+1}}$. Далее из (4′) следует, что $\lim\limits_{n\to\infty} f(\alpha_n) = 0$; с другой стороны, по непрерывности многочлена $\lim\limits_{n\to\infty} f(\alpha_n) = f(\alpha)$. Таким образом, $f(\alpha) = 0$, и теорема 3 доказана.

Замечание. Другое доказательство теоремы 3 (при $n = 1$) содержится в задачах 16 и 17.

Следствие. *Если для многочлена $F(x_1, \ldots, x_n)$ с целыми p-адическими коэффициентами и целых p-адических $\gamma_1, \ldots, \gamma_n$ при некотором i $(1 \leqslant i \leqslant n)$ имеем:*

$$F(\gamma_1, \ldots, \gamma_n) \equiv 0 \pmod{p}, \qquad F'_{x_i}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \pmod{p},$$

то существуют такие целые p-адические $\theta_1, \ldots, \theta_n$, что

$$F(\theta_1, \ldots, \theta_n) = 0$$

и $\theta_1 \equiv \gamma_1 \pmod{p}, \ldots, \theta_n \equiv \gamma_n \pmod{p}$.

$L_1 p^{n-1}$. Таким образом, число всех решений сравнения (7) не превосходит $lp^{n-1} + L_1 p^{n-1} \leqslant Lp^{n-1}$, что и требовалось доказать.

Доказательство теоремы С. Мы можем, конечно, считать, что многочлен F действительно зависит от переменной x_n. Рассмотрим F как многочлен от x_n с коэффициентами, являющимися многочленами от $x_1, \ldots, x_{n-1}$. Из абсолютной неприводимости F тогда следует, что дискриминант $D_{x_n}(x_1, \ldots, x_{n-1})$ многочлена F, как многочлена от x_n, является не равным тождественно нулю многочленом от $x_1, \ldots, x_{n-1}$, в противном случае F делился бы на квадрат некоторого многочлена. Рассмотрим простые числа p, не делящие всех коэффициентов $D_{x_n}(x_1, \ldots, x_{n-1})$, и оценим для них число $N_1(p)$ решений системы сравнений (6). Если $(c_1, \ldots, c_n)$ — решение системы (6), то c_n является общим корнем многочленов $F(c_1, \ldots, c_{n-1}, x_n)$ и $F'_{x_n}(c_1, \ldots, c_{n-1}, x_n)$ по модулю p и поэтому $D_{x_n}(c_1, \ldots, c_{n-1}) \equiv 0 \pmod p$.

На основании леммы число систем $(c_1, \ldots, c_{n-1})$, удовлетворяющих этому сравнению, не превосходит $K_1 p^{n-2}$, где K_1 — некоторая константа, зависящая только от многочлена F. Для заданных же $c_1, \ldots, c_{n-1}$ значение c_n определяется из сравнения

$$F(c_1, \ldots, c_{n-1}, x_n) \equiv 0 \pmod p,$$

и поэтому число значений c_n не превосходит степени m многочлена F по переменной x_n. Таким образом, число $N_1(p)$ решений системы (6) не превосходит Kp^{n-2}, где $K = mK_1$. Докажем теперь, что число $N(p)$ решений сравнения (7) при достаточно большом p больше числа $N_1(p)$ решений системы (6). Действительно, из теоремы B следует, что

$$N(p) > p^{n-1} - Cp^{n-1-1/2},$$

а мы только что доказали, что $N_1(p) < Kp^{n-2}$. Отсюда следует, что

$$N(p) - N_1(p) > p^{n-1} - Cp^{n-1-1/2} - Kp^{n-2} = p^{n-2}(p - Cp^{1/2} - K),$$

а значит, $N(p) > N_1(p)$ при достаточно большом p. Таким образом, при достаточно большом p сравнение $F \equiv 0 \pmod p$ имеет решение $(\gamma_1, \ldots, \gamma_n)$, для которого

$$\frac{\partial F}{\partial x_n}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \pmod p.$$

Ввиду следствия к теореме 3 отсюда и следует разрешимость уравнения $F = 0$ в кольце $\mathbb{Z}_p$ для всех p, начиная с некоторой границы.

Замечание 1. В работе [64] показано, что для каждого многочлена $f = f(x_1, \ldots, x_n)$ с целыми p-адическими коэффициентами можно эффективно указать такое натуральное число $d = d(f)$, что каждое решение сравнения $f \equiv 0 \pmod{p^{d+1}}$ может быть «поднято» до решения уравнения $f = 0$. Точнее это означает, что

если целые p-адические $a_1, \ldots, a_n$ удовлетворяют сравнению

$$f(a_1, \ldots, a_n) \equiv 0 \pmod{p^{d+1}}, \tag{10}$$

то в $\mathbb{Z}_p$ существуют $\alpha_1, \ldots, \alpha_n$ такие, что $f(\alpha_1, \ldots, \alpha_n) = 0$ и $\alpha_i \equiv a_i \pmod{p^{d+1}}$. Так как вопрос о разрешимости сравнения (10) решается эффективно, то тем самым мы имеем эффективный метод для решения вопроса о разрешимости p-адического уравнения $f(x_1, \ldots, x_n) = 0$.

Замечание 2. Пусть $F(x_1, \ldots, x_n)$ — произвольный многочлен с целыми p-адическими коэффициентами. Обозначим через c_m $(m \geqslant 0)$ число решений сравнения

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p^m}. \tag{11}$$

Все решения сравнения (11) являются, очевидно, «поднятиями» некоторых решений того же сравнения, но по модулю p^{m-1}. С учетом предыдущего замечания это наводит на мысль, что числа c_m $(m \geqslant 0)$ связаны между собой какими-то жесткими закономерностями (возможно, начиная с некоторого места). Если предположить, что эти зависимости линейны, т. е. что каждое c_m (при $m \geqslant m_0$) выражается через k предшествующих значений при помощи формулы

$$c_m = A_1 c_{m-1} + \ldots + A_k c_{m-k}$$

с коэффициентами $A_1, \ldots, A_k$, не зависящими от m, то это означало бы, что ряд

$$\varphi(t) = \sum_{m=0}^{\infty} c_m t^m \tag{12}$$

является рациональной функцией от t (такое заключение следует из известных формул для решения линейного уравнения в конечных разностях с постоянными коэффициентами). Основываясь на этих соображениях, в предшествующих изданиях книги [2] авторами была высказана гипотеза, что для произвольного многочлена F ряд (12), который (по аналогии с аналогичными рядами, встречающимися в топологии) был назван *рядом Пуанкаре* многочлена F, представляет рациональную функцию от t. Рациональность ряда (12) является, как видим, своеобразным выражением факта существования рекуррентных соотношений между числами c_m. Справедливость приведенной гипотезы доказал Игуса в 1975 г. Его доказательство основывается на рассмотрении функции

$$\int \ldots \int_{\Omega} \left(\left(\frac{1}{p} \right)^{v_p(F(x_1, \ldots, x_n))} \right)^s dx_1 \ldots dx_n \tag{13}$$

от комплексного аргумента s в правой полуплоскости. Выражение (13) является p-адическим интегралом, который берется по мно-

$L_1 p^{n-1}$. Таким образом, число всех решений сравнения (7) не превосходит $lp^{n-1} + L_1 p^{n-1} \leqslant Lp^{n-1}$, что и требовалось доказать.

Доказательство теоремы С. Мы можем, конечно, считать, что многочлен F действительно зависит от переменной x_n. Рассмотрим F как многочлен от x_n с коэффициентами, являющимися многочленами от $x_1, \ldots, x_{n-1}$. Из абсолютной неприводимости F тогда следует, что дискриминант $D_{x_n}(x_1, \ldots, x_{n-1})$ многочлена F, как многочлена от x_n, является не равным тождественно нулю многочленом от $x_1, \ldots, x_{n-1}$, в противном случае F делился бы на квадрат некоторого многочлена. Рассмотрим простые числа p, не делящие всех коэффициентов $D_{x_n}(x_1, \ldots, x_{n-1})$, и оценим для них число $N_1(p)$ решений системы сравнений (6). Если $(c_1, \ldots, c_n)$ — решение системы (6), то c_n является общим корнем многочленов $F(c_1, \ldots, c_{n-1}, x_n)$ и $F'_{x_n}(c_1, \ldots, c_{n-1}, x_n)$ по модулю p и поэтому $D_{x_n}(c_1, \ldots, c_{n-1}) \equiv 0 \pmod p$.

На основании леммы число систем $(c_1, \ldots, c_{n-1})$, удовлетворяющих этому сравнению, не превосходит $K_1 p^{n-2}$, где K_1 — некоторая константа, зависящая только от многочлена F. Для заданных же $c_1, \ldots, c_{n-1}$ значение c_n определяется из сравнения

$$F(c_1, \ldots, c_{n-1}, x_n) \equiv 0 \pmod p,$$

и поэтому число значений c_n не превосходит степени m многочлена F по переменной x_n. Таким образом, число $N_1(p)$ решений системы (6) не превосходит Kp^{n-2}, где $K = mK_1$. Докажем теперь, что число $N(p)$ решений сравнения (7) при достаточно большом p больше числа $N_1(p)$ решений системы (6). Действительно, из теоремы В следует, что

$$N(p) > p^{n-1} - Cp^{n-1-1/2},$$

а мы только что доказали, что $N_1(p) < Kp^{n-2}$. Отсюда следует, что

$$N(p) - N_1(p) > p^{n-1} - Cp^{n-1-1/2} - Kp^{n-2} = p^{n-2}(p - Cp^{1/2} - K),$$

а значит, $N(p) > N_1(p)$ при достаточно большом p. Таким образом, при достаточно большом p сравнение $F \equiv 0 \pmod p$ имеет решение $(\gamma_1, \ldots, \gamma_n)$, для которого

$$\frac{\partial F}{\partial x_n}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \pmod p.$$

Ввиду следствия к теореме 3 отсюда и следует разрешимость уравнения $F = 0$ в кольце $\mathbb{Z}_p$ для всех p, начиная с некоторой границы.

Замечание 1. В работе [64] показано, что для каждого многочлена $f = f(x_1, \ldots, x_n)$ с целыми p-адическими коэффициентами можно эффективно указать такое натуральное число $d = d(f)$, что каждое решение сравнения $f \equiv 0 \pmod{p^{d+1}}$ может быть «поднято» до решения уравнения $f = 0$. Точнее это означает, что

если целые p-адические $a_1, \ldots, a_n$ удовлетворяют сравнению

$$f(a_1, \ldots, a_n) \equiv 0 \pmod{p^{d+1}}, \tag{10}$$

то в $\mathbb{Z}_p$ существуют $\alpha_1, \ldots, \alpha_n$ такие, что $f(\alpha_1, \ldots, \alpha_n) = 0$ и $\alpha_i \equiv a_i \pmod{p^{d+1}}$. Так как вопрос о разрешимости сравнения (10) решается эффективно, то тем самым мы имеем эффективный метод для решения вопроса о разрешимости p-адического уравнения $f(x_1, \ldots, x_n) = 0$.

Замечание 2. Пусть $F(x_1, \ldots, x_n)$ — произвольный многочлен с целыми p-адическими коэффициентами. Обозначим через c_m $(m \geqslant 0)$ число решений сравнения

$$F(x_1, \ldots, x_n) \equiv 0 \pmod{p^m}. \tag{11}$$

Все решения сравнения (11) являются, очевидно, «поднятиями» некоторых решений того же сравнения, но по модулю p^{m-1}. С учетом предыдущего замечания это наводит на мысль, что числа c_m $(m \geqslant 0)$ связаны между собой какими-то жесткими закономерностями (возможно, начиная с некоторого места). Если предположить, что эти зависимости линейны, т. е. что каждое c_m (при $m \geqslant m_0$) выражается через k предшествующих значений при помощи формулы

$$c_m = A_1 c_{m-1} + \ldots + A_k c_{m-k}$$

с коэффициентами $A_1, \ldots, A_k$, не зависящими от m, то это означало бы, что ряд

$$\varphi(t) = \sum_{m=0}^{\infty} c_m t^m \tag{12}$$

является рациональной функцией от t (такое заключение следует из известных формул для решения линейного уравнения в конечных разностях с постоянными коэффициентами). Основываясь на этих соображениях, в предшествующих изданиях книги [2] авторами была высказана гипотеза, что для произвольного многочлена F ряд (12), который (по аналогии с аналогичными рядами, встречающимися в топологии) был назван *рядом Пуанкаре* многочлена F, представляет рациональную функцию от t. Рациональность ряда (12) является, как видим, своеобразным выражением факта существования рекуррентных соотношений между числами c_m. Справедливость приведенной гипотезы доказал Игуса в 1975 г. Его доказательство основывается на рассмотрении функции

$$\int_{\Omega} \ldots \int \left(\left(\frac{1}{p} \right)^{v_p(F(x_1, \ldots, x_n))} \right)^s dx_1 \ldots dx_n \tag{13}$$

от комплексного аргумента s в правой полуплоскости. Выражение (13) является p-адическим интегралом, который берется по мно-

жеству Ω всех точек $(x_1, \ldots, x_n)$ с целыми p-адическими координатами, относительно некоторой естественной меры, определенной на этом множестве Ω. Поведение функции (13) зависит от характера особых точек алгебраического многообразия, определяемого уравнением $F(x_1, \ldots, x_n) = 0$. Доказательство использует поэтому также теорему Хиронака о разрешении особенностей алгебраического многообразия. Позднее в работе [82] было приведено более простое доказательство, основанное на тех же идеях. (Заметим, что Игуса рассматривал более общий случай сравнений по степеням максимального идеала в кольце целых элементов произвольного конечного расширения поля p-адических чисел.) В дальнейшем результат Игуса о рациональности ряда $\varphi(t)$ его же методом был обобщен на случай систем сравнений [109]. Наконец, в последнее время в работе [72] предложено доказательство рациональности ряда $\varphi(t)$ для случая систем сравнений над кольцом целых p-адических чисел, не использующее метода разрешения особенностей, но с привлечением средств математической логики (элиминация кванторов для поля p-адических чисел).

Задачи

1. Доказать, что если m и p взаимно просты, то всякая p-адическая единица ε, удовлетворяющая сравнению $\varepsilon \equiv 1 \pmod p$ является m-й степенью в $\mathbb{Q}_p$.

2. Пусть $m = p^\delta m_0$, $(m_0, p) = 1$, пусть $\varepsilon \equiv 1 \pmod{p^{2\delta+1}}$. Доказать, что тогда p-адическая единица ε является m-й степенью в $\mathbb{Q}_p$.

3. Доказать, что при $p \neq 2$ разрешимость сравнения $\alpha x^p \equiv \beta \pmod{p^2}$ с целыми p-адическими α и β, не делящимися на p, достаточна для разрешимости уравнения $\alpha x^p = \beta$ в поле $\mathbb{Q}_p$. Доказать, далее, что уравнение

$$x^7 + y^7 = z^7$$

разрешимо в целых 7-адических числах x, y, z, одновременно не делящихся на 7 (учесть, что $1^7 + 2^7 \equiv 3^7 \pmod{7^2}$).

4. Предположим, что коэффициенты ε_i формы $G = \varepsilon_1 x_1^p + \ldots + \varepsilon_n x_n^p$ являются p-адическими единицами ($p \neq 2$). Доказать, что если сравнение $G \equiv 0 \pmod{p^2}$ имеет решение, в котором значение хоть одной неизвестной не делится на p, то в поле $\mathbb{Q}_p$ уравнение $G = 0$ имеет ненулевое решение.

5. Пусть все коэффициенты формы $G = \alpha_1 x_1^p + \ldots + \alpha_n x_n^p$ — целые p-адические числа, делящиеся на p самое большее в степени $p - 1$. Доказать, что уравнение $G = 0$ имеет в поле $\mathbb{Q}_p$ ненулевое решение, если сравнение $G \equiv 0 \pmod{p^{p+2}}$ имеет решение, в котором не все значения неизвестных делятся на p. (В случае $p \neq 2$ достаточно потребовать разрешимости сравнения $G \equiv 0 \pmod{p^{p+1}}$.)

6. Предположим, что квадратичная форма $F = \alpha_1 x_1^2 + \ldots + \alpha_n x_n^2$ имеет целые p-адические коэффициенты ($p \neq 2$), делящиеся на p не выше чем в первой степени. Доказать, что если сравнение $F \equiv 0 \pmod{p^2}$ имеет решение, в котором не все значения неизвестных делятся на p, то уравнение $F = 0$ имеет в $\mathbb{Q}_p$ ненулевое решение.

7. Для формы $F = \alpha_1 x_1^m + \ldots + \alpha_n x_n^m$, где α_i — отличные от нуля целые p-адические числа, положим $r = \nu_p(m)$, $s = \max(\nu_p(\alpha_1), \ldots, \nu_p(\alpha_n))$

и $N = 2(r+s)+1$. Доказать, что уравнение $F = 0$ имеет в поле $\mathbb{Q}_p$ ненулевое решение тогда и только тогда, когда сравнение $F \equiv 0 \pmod{p^N}$ имеет решение, в котором значение хоть одной неизвестной не делится на p.

8. Доказать, что форма $3x^3 + 4y^3 + 5z^3$ представляет нуль в поле $\mathbb{Q}_p$ при любом p (см. задачу 13 § 2).

9. Найти ряд Пуанкаре $\varphi(t)$ для многочлена $F = \varepsilon_1 x_1^2 + \ldots + \varepsilon_n x_n^2$, где ε_i — p-адические единицы, и убедиться, что функция $\varphi(t)$ рациональна.

10. Найти ряд Пуанкаре для многочлена $F(x_1, \ldots, x_n)$ с целыми p-адическими коэффициентами, обладающего тем свойством, что для всякого решения сравнения $F \equiv 0 \pmod{p}$ при некотором $i = 1, \ldots, n$ имеем $\frac{\partial F}{\partial x_i} \not\equiv 0 \pmod{p}$.

11. Вычислить ряд Пуанкаре для многочлена $F(x, y) = x^2 - y^3$.

12. Доказать рациональность ряда Пуанкаре для случая $n = 1$, т. е. для многочленов одной переменной (с целыми p-адическими коэффициентами).

13. Пусть $f(x_1, \ldots, x_n)$ — форма степени d над кольцом целых p-адических чисел, $p \neq 2$, $m \geqslant 0$. Доказать, что если $n > d\,(1 + p + \ldots + p^m)$, то сравнение

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{p^{m+1}}$$

имеет решение, у которого значение хоть одной неизвестной не делится на p.

14. Доказать, что при любом p в поле p-адических чисел $\mathbb{Q}_p$ уравнение $2x^2 + y^4 - 17z^4 = 0$ имеет решение с ненулевыми значениями неизвестных (см. задачу 14 § 2).

15. Пусть $f(x)$ — многочлен с целыми p-адическими коэффициентами и γ — целое p-адическое число такое, что $f(\gamma) \equiv 0 \pmod{p^{2\delta+1}}$, $f'(\gamma) = p^\delta u$, u — p-адическая единица, $\delta \geqslant 1$. Доказать, что в кольце целых p-адических чисел уравнение $f(x) = 0$ имеет только одно решение $x = \alpha$, удовлетворяющее сравнению $\alpha \equiv \gamma \pmod{p^{\delta+1}}$ (см. доказательство теоремы 3).

16. Пусть $\varphi(x) = \sum_{n=0}^{\infty} a_n x^n$ — формальный степенной ряд с коэффициентами из некоторого коммутативного кольца $\mathfrak{O}$ с единицей. Доказать, что если a_1 — обратимый элемент кольца, то существует формальный степенной ряд $\psi(x) = \sum_{n=1}^{\infty} b_n x^n$ без свободного члена ($b_n \in \mathfrak{O}$, $n \geqslant 1$) такой, что

$$\varphi(\psi(x)) = \sum_{n=0}^{\infty} a_n \psi(x)^n = a_0 + x$$

(относительно операции формальной подстановки ряда в ряд см. п. 1 § 5 гл. IV).

17. Пусть выполнены условия задачи 15. Положим $f(\gamma) = p^{2\delta} a_0$, где $a_0 \equiv 0 \pmod{p}$. Для $x = \gamma + p^\delta y$ имеем

$$f(\gamma + p^\delta y) = f(\gamma) + f'(\gamma) p^\delta y + a_2 p^{2\delta} y^2 + \ldots = p^{2\delta} \varphi(y),$$

где $\varphi(y) = a_0 + uy + a_2 y^2 + \ldots$ — многочлен с целыми p-адическими коэффициентами, удовлетворяющий условию задачи 16. Пусть $\psi(y) = \sum_{n=1}^{\infty} b_n y^n$ — формальный степенной ряд с целыми p-адическими коэффициентами, для которого $\varphi(\psi(y)) = a_0 + y$. Доказать, что целое p-адическое число $\alpha = \gamma + p^\delta \psi(-a_0)$ удовлетворяет условиям

$$f(\alpha) = 0, \qquad \alpha \equiv \gamma \pmod{p^{\delta+1}}.$$

§ 6. Квадратичные формы с p-адическими коэффициентами

В этом и следующем параграфе мы применим развитую нами теорию p-адических чисел к исследованию простейших неопределенных уравнений. Именно, мы рассмотрим вопрос о представлениях p-адических и рациональных чисел квадратичными формами. Необходимые нам алгебраические сведения о квадратичных формах в произвольном поле изложены в § 1 Дополнения.

1. Квадраты в поле p-адических чисел. При изучении квадратичных форм в том или ином поле важно знать, какие элементы поля являются квадратами. Займемся поэтому сначала изучением квадратов в поле p-адических чисел $\mathbb{Q}_p$.

Мы знаем (§ 3, теорема 4), что каждое отличное от нуля p-адическое число α однозначно представляется в виде $\alpha = p^m\varepsilon$, где ε — p-адическая единица (т. е. единица в кольце целых p-адических чисел $\mathbb{Z}_p$). Если α является квадратом p-адического числа $\gamma = p^k\varepsilon_0$, то $m = 2k$ и $\varepsilon = \varepsilon_0^2$. Для описания всех квадратов поля $\mathbb{Q}_p$ нам достаточно знать, следовательно, какие единицы из $\mathbb{Z}_p$ являются квадратами.

Теорема 1. *Пусть $p \neq 2$. Для того чтобы p-адическая единица*

$$\varepsilon = c_0 + c_1 p + c_2 p^2 + \ldots, \quad 0 \leqslant c_i < p, \quad c_0 \neq 0 \tag{1}$$

была квадратом, необходимо и достаточно, чтобы число c_0 было квадратичным вычетом по модулю p.

Доказательство. Если $\varepsilon = \eta^2$ и $\eta \equiv b \pmod p$ (b целое рациональное), то $c_0 \equiv b^2 \pmod p$. Обратно, если $c_0 \equiv b^2 \pmod p$, то, рассматривая многочлен $F(x) = x^2 - \varepsilon$, имеем: $F(b) \equiv 0 \pmod p$ и $F'(b) = 2b \not\equiv 0 \pmod p$. По следствию к теореме 3 § 5 существует такое $\eta \in \mathbb{Z}_p$, что $F(\eta) = 0$ и $\eta \equiv b \pmod p$. Таким образом, $\varepsilon = \eta^2$, и теорема доказана.

Следствие 1. *При $p \neq 2$ всякая p-адическая единица, сравнимая с 1 по модулю p, является квадратом в $\mathbb{Q}_p$.*

Следствие 2. *При $p \neq 2$ индекс $(\mathbb{Q}_p^* : \mathbb{Q}_p^{*2})$ подгруппы квадратов $\mathbb{Q}_p^{*2}$ в мультипликативной группе поля p-адических чисел равен 4.*

Действительно, если единица ε не является квадратом, то отношение любых двух из чисел $1, \varepsilon, p, p\varepsilon$ не является квадратом в поле $\mathbb{Q}_p$. В то же время всякое отличное от нуля p-адическое число представляется в виде произведения одного из чисел $1, \varepsilon, p, p\varepsilon$ на некоторый квадрат.

При $p \neq 2$ для единицы (1) положим:

$$\left(\frac{\varepsilon}{p}\right) = \begin{cases} +1, \text{ если } \varepsilon \text{ является квадратом в } \mathbb{Q}_p, \\ -1, \text{ в противном случае.} \end{cases}$$

В силу теоремы 1 имеем $\left(\frac{\varepsilon}{p}\right)=\left(\frac{c_0}{p}\right)$, где $\left(\frac{c_0}{p}\right)$ — символ Лежандра. Если ε — целое рациональное число, взаимно простое с p, то введенный символ $\left(\frac{\varepsilon}{p}\right)$ совпадает, очевидно, с символом Лежандра. Легко видеть, что для p-адических единиц ε и η имеем $\left(\frac{\varepsilon\eta}{p}\right)=\left(\frac{\varepsilon}{p}\right)\left(\frac{\eta}{p}\right)$.

Обратимся к случаю $p=2$.

Теорема 2. *Для того чтобы 2-адическая единица ε была квадратом (в поле $\mathbb{Q}_2$), необходимо и достаточно, чтобы* $\varepsilon\equiv 1 \pmod 8$.

Доказательство. Необходимость следует из того, что квадрат нечетного числа всегда сравним с 1 по модулю 8. Для доказательства достаточности условия рассмотрим многочлен $F(x)=x^2-\varepsilon$ и применим к нему теорему 3 § 5, взяв $\delta=1$ и $\gamma=1$. Так как $F(1)\equiv 0 \pmod 8$, $F'(1)=2\not\equiv 0 \pmod 4$, то согласно этой теореме существует такое $\eta\equiv 1 \pmod 4$, что $F(\eta)=0$, т. е. $\varepsilon=\eta^2$.

Следствие. *Индекс $(\mathbb{Q}_2^*:\mathbb{Q}_2^{*2})$ подгруппы квадратов в мультипликативной группе поля 2-адических чисел равен* 8.

Действительно, согласно теореме приведенная система вычетов 1, 3, 5, 7 по модулю 8 является в то же время системой представителей из классов смежности группы 2-адических единиц по подгруппе ее квадратов. Присоединяя к ним произведения $2\cdot 1$, $2\cdot 3$, $2\cdot 5$, $2\cdot 7$, мы получаем полную систему представителей из классов смежности группы $\mathbb{Q}_2^*$ по подгруппе $\mathbb{Q}_2^{*2}$.

2. Представление нуля p-адическими квадратичными формами. Как и во всяком поле, неособенная квадратичная форма над полем $\mathbb{Q}_p$ при помощи линейного преобразования переменных может быть приведена к виду

$$\alpha_1x_1^2+\ldots+\alpha_nx_n^2,\quad \alpha_i\neq 0$$

(см. Дополнение, § 1, п. 1). Если $\alpha_i=p^{2k_i}\varepsilon_i$ или $\alpha_i=p^{2k_i+1}\varepsilon_i$ (ε_i — единицы в $\mathbb{Z}_p$), то после преобразования $p^{k_i}x_i=y_i$ мы придем к форме, у которой все коэффициенты — целые p-адические числа, делящиеся на p не выше чем в первой степени. Таким образом, всякая неособенная квадратичная форма над полем $\mathbb{Q}_p$ эквивалентна форме вида

$$F=F_0+pF_1=\varepsilon_1x_1^2+\ldots+\varepsilon_rx_r^2+p\left(\varepsilon_{r+1}x_{r+1}^2+\ldots+\varepsilon_nx_n^2\right), \quad (2)$$

где ε_i — p-адические единицы.

Рассматривая вопрос о существовании представлений нуля, мы можем считать, что $r\geqslant n-r$. Действительно, форма pF, очевидно, эквивалентна форме F_1+pF_0. Так как F и pF лишь

одновременно представляют нуль, то вместо $F_0 + pF_1$ мы можем взять форму $F_1 + pF_0$.

Рассмотрим сначала случай $p \neq 2$.

Теорема 3. *Пусть* $p \neq 2$ *и* $0 < r < n$. *Форма* (2) *представляет нуль в поле* $\mathbb{Q}_p$ *тогда и только тогда, когда представляет нуль хоть одна из форм* F_0 *или* F_1.

Доказательство. Пусть форма (2) представляет нуль:

$$\varepsilon_1\xi_1^2 + \ldots + \varepsilon_r\xi_r^2 + p\left(\varepsilon_{r+1}\xi_{r+1}^2 + \ldots + \varepsilon_n\xi_n^2\right) = 0. \qquad (3)$$

Мы можем, очевидно, считать, что все ξ_i целые и хоть одно из них не делится на p. Если не все $\xi_1, \ldots, \xi_r$ делятся на p, скажем $\xi_1 \not\equiv 0 \pmod p$, то, рассматривая равенство (3) по модулю p, мы получим

$$F_0(\xi_1, \ldots, \xi_r) \equiv 0 \pmod p;$$

$$\frac{\partial F_0}{\partial x_1}(\xi_1, \ldots, \xi_r) = 2\varepsilon_1\xi_1 \not\equiv 0 \pmod p.$$

По следствию к теореме 3 § 5 форма F_0 представляет нуль. Пусть теперь все значения $\xi_1, \ldots, \xi_r$ делятся на p, так что $\varepsilon_1\xi_1^2 + \ldots + \varepsilon_r\xi_r^2 \equiv 0 \pmod{p^2}$. Перейдем в равенстве (3) к сравнению по модулю p^2. Сокращая это сравнение на p, мы получим

$$F_1(\xi_{r+1}, \ldots, \xi_n) \equiv 0 \pmod p,$$

причем хоть одно из $\xi_{r+1}, \ldots, \xi_n$ не делится на p. Применяя опять следствие к теореме 3 § 5, заключаем, что в этом случае форма F_1 представляет нуль. Поскольку достаточность условия очевидна, то этим доказательство теоремы 3 закончено. Попутно нами получено следующее утверждение.

Следствие 1. *Если* $\varepsilon_1, \ldots, \varepsilon_r$ — *p-адические единицы, то при* $p \neq 2$ *форма* $f = \varepsilon_1 x_1^2 + \ldots + \varepsilon_r x_r^2$ *представляет нуль в* $\mathbb{Q}_p$ *тогда и только тогда, когда сравнение* $f(x_1, \ldots, x_r) \equiv 0 \pmod p$ *имеет в* $\mathbb{Z}_p$ *нетривиальное решение.*

Следствие 2. *Если при тех же предположениях* $r \geqslant 3$, *то форма* $f(x_1, \ldots, x_r)$ *всегда представляет нуль в* $\mathbb{Q}_p$.

Действительно, по теореме 5 § 1 сравнение $f(x_1, \ldots, x_r) \equiv 0 \pmod p$ имеет нетривиальное решение.

При доказательстве теоремы 3 равенство (3) фактически не было использовано: мы имели дело лишь со сравнениями $F \equiv 0 \pmod p$ и $F \equiv 0 \pmod{p^2}$. Таким образом, уже из разрешимости второго из этих сравнений вытекает, что одна из форм F_0 или F_1, а значит и F, представляет нуль. Мы имеем, таким образом,

Следствие 3. *При* $p \neq 2$ *форма* (2) *представляет нуль тогда и только тогда, когда сравнение* $F \equiv 0 \pmod{p^2}$ *имеет решение, в котором значение хоть одной неизвестной не делится на* p.

Перейдем теперь к рассмотрению квадратичных форм в поле 2-адических чисел. В этом случае теорема 3 и все следствия к ней уже не имеют места. Например, для формы $f = x_1^2 + x_2^2 + x_3^2 + x_4^2$ уравнение $f = 0$ не имеет нетривиальных решений в $\mathbb{Q}_2$ (так как уже сравнение $f \equiv 0 \pmod 8$ не имеет решений с нечетным значением хотя бы одной неизвестной). В то же время форма $f + 2x_5^2$ представляет нуль в $\mathbb{Q}_2$ (теорема 5).

Теорема 4. *В поле 2-адических чисел форма* (2) (*с* $p = 2$) *представляет нуль тогда и только тогда, когда разрешимо сравнение* $F \equiv 0 \pmod{16}$ *с нечетным значением хоть одной неизвестной.*

Доказательство. Пусть $F(\xi_1, \ldots, \xi_n) \equiv 0 \pmod{16}$, где не все целые 2-адические числа ξ_i делятся на 2. Предположим сначала, что $\xi_i \not\equiv 0 \pmod 2$ хоть для одного $i \leqslant r$, скажем $\xi_1 \not\equiv 0 \pmod 2$. Так как $F(\xi_1, \ldots, \xi_n) \equiv 0 \pmod 8$ и $\frac{\partial F}{\partial x_1}(\xi_1, \ldots, \xi_n) = 2\varepsilon_1\xi_1 \not\equiv 0 \pmod 4$, то по теореме 3 § 5 (при $\delta = 1$) форма F представляет нуль. Пусть теперь $\xi_1, \ldots, \xi_r$ все делятся на 2, т. е. $\xi_i = 2\eta_i$ $(1 \leqslant i \leqslant r)$ с целыми 2-адическими η_i. Сокращая сравнение

$$4\sum_{i=1}^{r} \varepsilon_i\eta_i^2 + 2\sum_{i=r+1}^{n} \varepsilon_i\xi_i^2 \equiv 0 \pmod{16}$$

на 2, мы получим $\sum_{i=r+1}^{n} \varepsilon_i\xi_i^2 + 2\sum_{i=1}^{r} \varepsilon_i\eta_i^2 \equiv 0 \pmod 8$, причем здесь одно из $\xi_{r+1}, \ldots, \xi_n$ не делится на 2. Как и выше, из полученного сравнения следует, что форма $F_1 + 2F_0$ представляет нуль. Но тогда эквивалентная ей форма $2F$ также представляет нуль, и достаточность условия доказана. Что касается обратного утверждения, то оно очевидно.

При доказательстве теоремы 4 нами получен также следующий результат.

Следствие. *Если для формы* (2) (*с* $p = 2$) *сравнение* $F \equiv 0 \pmod 8$ *имеет решение с нечетным значением хоть одной из неизвестных* $x_1, \ldots, x_r$, *то эта форма представляет нуль в поле* $\mathbb{Q}_2$.

Теорема 5. *В поле* p*-адических чисел* $\mathbb{Q}_p$ *всякая неособенная квадратичная форма от пяти и более переменных всегда представляет нуль.*

Доказательство. Можно считать, что заданная форма имеет вид (2), причем $r \geqslant n - r$. Так как $n \geqslant 5$, то $r \geqslant 3$. Пусть $p \neq 2$; в этом случае по следствию 2 к теореме 3 форма F_0 представляет нуль. Вместе с F_0 форма F также представляет нуль. Этим для $p \neq 2$ теорема доказана.

Пусть теперь $p = 2$. Если $n - r > 0$, то мы рассмотрим «частичную» форму $f = \varepsilon_1x_1^2 + \varepsilon_2x_2^2 + \varepsilon_3x_3^2 + 2\varepsilon_nx_n^2$. Такая форма

всегда представляет нуль в $\mathbb{Q}_2$. Действительно, так как $\varepsilon_1+\varepsilon_2 \equiv 2\alpha$ (α целое 2-адическое), то $\varepsilon_1+\varepsilon_2+2\varepsilon_n\alpha^2 \equiv 2\alpha+2\alpha^2 = 2\alpha(1+\alpha) \equiv 0 \pmod 4$, т. е. $\varepsilon_1+\varepsilon_2+2\varepsilon_n\alpha^2 = 4\beta$ с целым 2-адическим β. Полагая $x_1=x_2=1$, $x_3=2\beta$, $x_n=\alpha$, имеем $\varepsilon_1\cdot 1^2+\varepsilon_2\cdot 1^2+\varepsilon_3\cdot(2\beta)^2+2\varepsilon_n\alpha^2 \equiv 4\beta+4\beta^2 \equiv 0 \pmod 8$. По следствию к теореме 4 форма f представляет нуль. Но тогда F также представляет нуль. В случае $n=r$ в качестве «частичной» формы мы возьмем $f=\varepsilon_1x_1^2+\varepsilon_2x_2^2+\varepsilon_3x_3^2+\varepsilon_4x_4^2+\varepsilon_5x_5^2$. Если $\varepsilon_1+\varepsilon_2 \equiv \varepsilon_3+\varepsilon_4 \equiv 2 \pmod 4$, то положим $x_1=x_2=x_3=x_4=1$, а если, например, $\varepsilon_1+\varepsilon_2 \equiv 0 \pmod 4$, то $x_1=x_2=1$, $x_3=x_4=0$. В обоих случаях $\varepsilon_1x_1^2+\varepsilon_2x_2^2+\varepsilon_3x_3^2+\varepsilon_4x_4^2=4\gamma$ с целым 2-адическим γ. Полагая $x_5=2\gamma$, получим

$$f \equiv 4\gamma+4\gamma^2 \equiv 0 \pmod 8.$$

Применение следствия к теореме 4 завершает доказательство и в этом случае. Теорема 5 доказана полностью.

Согласно теореме 6 § 1 Дополнения из доказанной теоремы 5 вытекает следующее:

Следствие 1. *В поле $\mathbb{Q}_p$ всякая неособенная квадратичная форма от четырех и более переменных представляет все p-адические числа.*

Следствие 2. *Пусть $F(x_1, \ldots, x_n)$ — неособенная квадратичная форма с целыми рациональными коэффициентами. Если $n \geqslant 5$, то для любого модуля m сравнение $F(x_1, \ldots, x_n) \equiv 0 \pmod m$ имеет нетривиальное решение.*

Действительно, так как форма F представляет нуль в $\mathbb{Q}_p$, то при любом натуральном $s \geqslant 1$ сравнение $F \equiv 0 \pmod{p^s}$ имеет решение, в котором хоть одна неизвестная не делится на p.

3. Бинарные формы. Важным примером общей теории служит случай бинарных квадратичных форм. В этом пункте мы рассмотрим вопрос о представлении чисел поля $\mathbb{Q}_p$ бинарной квадратичной формой вида

$$x^2-\alpha y^2, \quad \alpha \neq 0, \quad \alpha \in \mathbb{Q}_p. \tag{4}$$

(Очевидно, что общий случай бинарной неособенной формы сводится к этому путем преобразования переменных и умножения формы на некоторое p-адическое число.)

Совокупность всех отличных от нуля p-адических чисел, представимых формой (4), мы обозначим через H_α. Эта совокупность замечательна тем, что она всегда является группой по умножению. Действительно, если $\beta=x^2-\alpha y^2$, $\beta_1=x_1^2-\alpha y_1^2$, то, как показывает простая выкладка,

$$\beta\beta_1=(xx_1+\alpha yy_1)^2-\alpha(xy_1+yx_1)^2, \quad \beta^{-1}=\left(\frac{x}{\beta}\right)^2-\alpha\left(\frac{y}{\beta}\right)^2.$$

Приведем другое доказательство этого же факта, основанное на

рассмотрении квадратичного расширения $\mathbb{Q}_p(\sqrt{\alpha})$ поля $\mathbb{Q}_p$ (при условии, что α не является квадратом в $\mathbb{Q}_p$). Равенство $\beta = x^2 - \alpha y^2$ эквивалентно тому, что β является нормой числа $\xi = x + y\sqrt{\alpha}$ из $\mathbb{Q}_p(\sqrt{\alpha})$. Но если $\beta = N(\xi)$ и $\beta_1 = N(\xi_1)$, то $\beta\beta_1 = N(\xi\xi_1)$ и $\beta^{-1} = N(\xi^{-1})$.

Если α является квадратом в $\mathbb{Q}_p$, то форма (4) представляет нуль, а значит, и все числа из $\mathbb{Q}_p$. Следовательно, в этом случае H_α совпадает со всей мультипликативной группой $\mathbb{Q}_p^*$ поля $\mathbb{Q}_p$.

Так как форма (4) заведомо представляет все квадраты поля $\mathbb{Q}_p$ (при $y = 0$), то $\mathbb{Q}_p^{*2} \subset H_\alpha$. Но согласно следствиям к теоремам 1 и 2 индекс $(\mathbb{Q}_p^* : \mathbb{Q}_p^{*2})$ конечен, поэтому тем более и группа H_α имеет конечный индекс в $\mathbb{Q}_p^*$.

Теорема 6. *Если число $\alpha \in \mathbb{Q}_p^*$ не является квадратом, то* $(\mathbb{Q}_p^* : H_\alpha) = 2$.

Доказательство. Заметим прежде всего, что форма (4) представляет p-адическое число β тогда и только тогда, когда форма

$$\alpha x^2 + \beta y^2 - z^2 \tag{5}$$

представляет нуль (теорема 6 § 1 Дополнения). Далее, условие представимости нуля формой (5), очевидно, не меняется при умножении α и β на квадраты. Мы можем поэтому считать, что α и β берутся из некоторой фиксированной системы представителей группы $\mathbb{Q}_p^*$ по подгруппе квадратов $\mathbb{Q}_p^{*2}$.

Рассмотрим сначала случай $p \neq 2$. Покажем, что $H_\alpha \neq \mathbb{Q}_p^{*2}$. Это очевидно, если $-\alpha$ не есть квадрат (так как $-\alpha \in H_\alpha$). Если же $-\alpha$ является квадратом, то форма $x^2 - \alpha y^2$ эквивалентна форме $x^2 + y^2$, которая представляет все p-адические единицы (следствие 2 теоремы 3); значит, H_α и в этом случае не совпадает с $\mathbb{Q}_p^{*2}$. Далее, H_α не совпадает с $\mathbb{Q}_p^*$ (если, конечно, $\alpha \notin \mathbb{Q}_p^{*2}$). Действительно, выбрав p-адическую единицу ε, не являющуюся квадратом, мы можем ограничиться для α значениями ε, p и $p\varepsilon$. Но по теореме 3 (и теореме 10 § 1 Дополнения) форма (5) не представляет нуля при $\alpha = \varepsilon$, $\beta = p$ и при $\alpha = p$, $p\varepsilon$, $\beta = \varepsilon$. Таким образом, действительно $H_\alpha \neq \mathbb{Q}_p^*$. Применим теперь следствие 2 теоремы 1. Так как $\mathbb{Q}_p^* \supset H_\alpha \supset \mathbb{Q}_p^{*2}$, то индекс $(\mathbb{Q}_p^* : H_\alpha)$ должен быть делителем индекса $(\mathbb{Q}_p^* : \mathbb{Q}_p^{*2}) = 4$. Но по доказанному он не может равняться ни 4, ни 1. Следовательно, $(\mathbb{Q}_p^* : H_\alpha) = 2$, и теорема 6 для случая $p \neq 2$ доказана.

Пусть теперь $p = 2$. В этом случае мы имеем 8 классов смежности $\mathbb{Q}_2^*$ по $\mathbb{Q}_2^{*2}$, в качестве представителей которых можно взять числа 1, 3, 5, 7, $2 \cdot 1$, $2 \cdot 3$, $2 \cdot 5$, $2 \cdot 7$. Будем считать поэтому, что α и β в форме (5) совпадают с этими числами, и выясним, в каких случаях эта форма представляет нуль в $\mathbb{Q}_2$. Ответ

сведен в нижеследующей таблице, в которой знак + означает, что для α и β, стоящих на соответствующих горизонтали и вертикали, форма (5) представляет нуль в $\mathbb{Q}_2$, а пустые клетки соответствуют формам, не представляющим нуля. (В силу симметрии между α и β в форме (5) знаки в таблице расположены симметрично относительно диагонали, идущей из левого верхнего угла в правый нижний.)

α \ β	1	3	5	7	2·1	2·3	2·5	2·7
1	+	+	+	+	+	+	+	+
3	+		+			+		+
5	+	+	+	+				
7	+		+		+		+	
2·1	+			+	+			+
2·3	+	+					+	+
2·5	+			+		+	+	
2·7	+	+			+	+		

Мы видим, что в каждой строчке кроме первой, знак + стоит ровно в четырех клетках. Это означает, что для любого $\alpha \in \mathbb{Q}_2^*$, не являющегося квадратом, имеется ровно четыре класса смежности по подгруппе $\mathbb{Q}_2^{*2}$, представляемых формой (4). Таким образом, $(H_\alpha : \mathbb{Q}_2^{*2}) = 4$, а так как $(\mathbb{Q}_2^* : \mathbb{Q}_2^{*2}) = 8$ (следствие теоремы 2), то $(\mathbb{Q}_2^* : H_\alpha) = 2$.

Проверка таблицы производится на основе результатов п. 2. Пусть $\alpha = 2\varepsilon$, $\beta = 2\eta$, где ε и η — 2-адические единицы, и пусть

$$2\varepsilon x^2 + 2\eta y^2 - z^2 = 0. \tag{6}$$

Значения x, y и z мы можем, конечно, считать здесь целыми и не делящимися на 2 одновременно. Ясно, что $z \equiv 0 \pmod 2$ и, далее, что x и y вместе не делятся на 2 (в противном случае левая часть (6) делилась бы на 4). Полагая $z = 2t$, мы приводим равенство (6) к виду $\varepsilon x^2 + \eta y^2 - 2t^2 = 0$; это равенство, согласно следствию теоремы 4, равносильно сравнению по модулю 8 (с нечетными x и y). Так как $x^2 \equiv y^2 \equiv 1 \pmod 8$ и $2t^2 \equiv 2 \pmod 8$ или $2t^2 \equiv 0 \pmod 8$, то мы получаем, следовательно, что разрешимость уравнения (6) равносильна выполнению хотя бы одного из сравнений

$$\varepsilon + \eta \equiv 2 \pmod 8, \qquad \varepsilon + \eta \equiv 0 \pmod 8.$$

Пусть теперь $\alpha = 2\varepsilon$, $\beta = \eta$. В равенстве $2\varepsilon x^2 + \eta y^2 - z^2 = 0$ (с целыми 2-адическими x, y и z, не делящимися на 2 одновременно) по тем же соображениям мы имеем: $y \not\equiv 0 \pmod 2$ и $z \not\equiv 0 \pmod 2$. Следовательно, выполнение этого равенства (по тому же следствию теоремы 4) равносильно выполнению хотя бы

одного из сравнений

$$2\varepsilon + \eta \equiv 1 \pmod 8, \quad \eta \equiv 1 \pmod 8, \tag{7}$$

соответствующих случаям $2 \nmid x$ и $2 \mid x$.

Остается рассмотреть еще случай $\alpha = \varepsilon$, $\beta = \eta$. Если в равенстве $\varepsilon x^2 + \eta y^2 - z^2 = 0$ целые 2-адические x, y и z не все делятся на 2, то ровно одно из них делится на 2, а два других — нет. Если $z \equiv 0 \pmod 2$, то $\varepsilon x^2 + \eta y^2 \equiv \varepsilon + \eta \equiv 0 \pmod 4$, откуда следует, что либо $\varepsilon \equiv 1 \pmod 4$, либо $\eta \equiv 1 \pmod 4$. Если же $z \not\equiv 0 \pmod 2$, то $\varepsilon x^2 + \eta y^2 \equiv 1 \pmod 4$, и так как одно из чисел x или y должно делится на 2, а другое — нет, то опять получаем, что выполняется хоть одно из сравнений

$$\varepsilon \equiv 1 \pmod 4, \quad \eta \equiv 1 \pmod 4. \tag{8}$$

Обратно, предположим, например, что $\varepsilon \equiv 1 \pmod 4$. Тогда сравнение $\varepsilon x^2 + \eta y^2 - z^2 \equiv 0 \pmod 8$ выполняется при $x = 1$, $y = 0$, $z = 1$, если $\varepsilon \equiv 1 \pmod 8$, и при $x = 1$, $y = 2$, $z = 1$, если $\varepsilon \equiv 5 \pmod 8$, а значит, форма $\varepsilon x^2 + \eta y^2 - z^2$ представляет нуль.

Закончив проверку таблицы, мы тем самым завершили доказательство теоремы 6.

Из теоремы 6 следует, что для p-адического числа $\alpha \neq 0$, не являющегося квадратом, фактор-группа $\mathbb{Q}_p^*/H_\alpha$ есть циклическая группа второго порядка. Мы можем поэтому установить изоморфизм этой фактор-группы с группой $\{1, -1\}$ корней второй степени из 1. Единственный изоморфизм между $\mathbb{Q}_p^*/H_\alpha$ и $\{1, -1\}$ сопоставляет подгруппе H_α число $+1$, а классу смежности βH_α, отличному от H_α,— число -1. Удобнее, однако, рассматривать гомоморфизм группы $\mathbb{Q}_p^*$ на группу $\{1, -1\}$ с ядром H_α, так как тогда мы будем иметь дело с функцией на $\mathbb{Q}_p^*$ (а не на фактор-группе $\mathbb{Q}_p^*/H_\alpha$).

Определение. *Для p-адических чисел $\alpha \neq 0$ и $\beta \neq 0$ мы определяем символ (α, β), который равен $+1$ или -1 в зависимости от того, представляет форма $\alpha x^2 + \beta y^2 - z^2$ нуль в поле $\mathbb{Q}$ или нет. Символ (α, β) называется символом Гильберта.*

Из определения непосредственно следует, что если α является квадратом, то $(\alpha, \beta) = 1$ при всех β. Если же $\alpha \notin \mathbb{Q}_p^{*2}$, то $(\alpha, \beta) = 1$ тогда и только тогда, когда $\beta \in H_\alpha$. Отсюда легко получаем, что при любом $\alpha \neq 0$ отображение $\beta \to (\alpha, \beta)$ является гомоморфизмом группы $\mathbb{Q}_p^*$ в группу $\{1, -1\}$ с ядром H_α. Другими словами, имеет место формула

$$(\alpha, \beta_1\beta_2) = (\alpha, \beta_1)(\alpha, \beta_2). \tag{9}$$

Далее, значение символа (α, β) зависит только от разрешимости уравнения $\alpha x^2 + \beta y^2 - z^2 = 0$, которое симметрично относительно

α и β, поэтому

$$(\beta, \alpha) = (\alpha, \beta), \tag{10}$$

откуда ввиду (9) следует, что

$$(\alpha_1\alpha_2, \beta) = (\alpha_1, \beta)(\alpha_2, \beta). \tag{11}$$

Заметим еще, что

$$(\alpha, -\alpha) = 1 \tag{12}$$

для любого $\alpha \in \mathbb{Q}_p^*$ (так как уравнение $\alpha x^2 - \alpha y^2 - z^2 = 0$ имеет решение $x = y = 1$, $z = 0$), а значит, в силу (9)

$$(\alpha, \alpha) = (\alpha, -1). \tag{13}$$

На основании формул (9)—(13) вычисление символа (α, β) в общем случае сводится к вычислению значений (p, ε) и (ε, η), где ε и η — p-адические единицы. Действительно, если $\alpha = p^k\varepsilon$, $\beta = p^l\eta$, то ввиду этих формул мы имеем

$$(p^k\varepsilon, p^l\eta) = (p, p)^{kl}(\varepsilon, p)^l(p, \eta)^k(\varepsilon, \eta) = (p, \varepsilon^l\eta^k(-1)^{kl})(\varepsilon, \eta).$$

Займемся вычислением значений символов (p, ε) и (ε, η). Если $p \neq 2$, то по теореме 3 форма $px^2 + \varepsilon y^2 - z^2$ представляет нуль тогда и только тогда, когда $\varepsilon y^2 - z^2$ представляет нуль, т. е. когда единица ε является квадратом. Таким образом, $(p, \varepsilon) = \left(\frac{\varepsilon}{p}\right)$ при $p \neq 2$ (см. п. 1). Далее, по следствию 2 теоремы 3 форма $\varepsilon x^2 + \eta y^2 - z^2$ всегда представляет нуль, а значит, $(\varepsilon, \eta) = +1$ для любых p-адических единиц ε и η ($p \neq 2$).

В случае $p = 2$ значения символов $(2, \eta)$ и (ε, η) для 2-адических единиц ε и η нами, по существу, уже найдены при доказательстве теоремы 6. Действительно, согласно (7) (при $\varepsilon = 1$) форма $2x^2 + \eta y^2 - z^2$ представляет нуль тогда и только тогда, когда $\eta \equiv \pm 1 \pmod 8$. Следовательно, $(2, \eta) = (-1)^{\frac{\eta^2-1}{8}}$. Далее, мы видели, что форма $\varepsilon x^2 + \eta y^2 - z^2$ представляет нуль тогда и только тогда, когда выполнено хоть одно из сравнений (8). Следовательно,

$$(\varepsilon, \eta) = (-1)^{\frac{\varepsilon-1}{2}\cdot\frac{\eta-1}{2}}.$$

Сформулируем полученный результат.

Теорема 7. *Значения символов Гильберта (p, ε) и (ε, η) для p-адических единиц ε и η определяются формулами:*

$$(p, \varepsilon) = \left(\frac{\varepsilon}{p}\right), \quad (\varepsilon, \eta) = 1 \quad \textit{при } p \neq 2;$$

$$(2, \varepsilon) = (-1)^{\frac{\varepsilon^2-1}{8}}, \quad (\varepsilon, \eta) = (-1)^{\frac{\varepsilon-1}{2}\cdot\frac{\eta-1}{2}} \quad \textit{при } p = 2.$$

4. Эквивалентность бинарных форм. Символ Гильберта дает возможность записать в явном виде условие эквивалентности

двух неособенных бинарных квадратичных форм в поле $\mathbf{Q}_p$. Пусть $f(x, y)$ и $g(x, y)$ — две бинарные неособенные квадратичные формы с коэффициентами из $\mathbf{Q}_p$ и $\delta(f)$, $\delta(g)$ — их определители. Для эквивалентности форм f и g необходимо, чтобы $\delta(f)$ и $\delta(g)$ отличались на множитель, принадлежащий $\mathbf{Q}_p^{*2}$ (теорема 1 § 1 Дополнения). Чтобы сформулировать еще одно необходимое условие эквивалентности, которое вместе с отмеченным будет уже и достаточным, докажем следующий факт.

Теорема 8. *Для всех p-адических чисел $\alpha \neq 0$, представимых бинарной формой f определителя $\delta \neq 0$, значение символа Гильберта $(\alpha, -\delta)$ имеет одно и то же значение.*

Доказательство. Пусть α и α' — два отличных от нуля p-адических числа, представимых формой f. Согласно теореме 2 § 1 Дополнения форма f эквивалентна форме f_1 вида $\alpha x^2 + \beta y^2$. Так как α' представляется также и формой f_1, то $\alpha' = \alpha x_0^2 + \beta y_0^2$, откуда $\alpha\alpha' - \alpha\beta y_0^2 - (\alpha x_0)^2 = 0$. Последнее означает, что форма $\alpha\alpha' x^2 - \alpha\beta y^2 - z^2$ представляет нуль, следовательно, $(\alpha\alpha', -\alpha\beta) = 1$. Но $\alpha\beta$ отличается от δ на квадрат, поэтому имеем также $(\alpha\alpha', -\delta) = 1$, а значит, по свойству (11) $(\alpha, -\delta) = (\alpha', -\delta)$, что и доказывает теорему.

Согласно теореме 8 мы можем ввести для бинарной формы f новый инвариант, положив

$$e(f) = (\alpha, -\delta(f)),$$

где α — любое отличное от нуля p-адическое число, представимое формой f.

Теорема 9. *Для эквивалентности неособенных бинарных квадратичных форм f и g в поле $\mathbf{Q}_p$ необходимо и достаточно, чтобы выполнялись условия*:

1) $$\delta(f) = \delta(g)\gamma^2, \quad \gamma \in \mathbf{Q}_p^*;$$

2) $$e(f) = e(g).$$

Доказательство. Необходимость обоих условий очевидна. Для доказательства достаточности покажем, что при выполнении условий теоремы формы f и g представляют одни и те же p-адические числа. Пусть число $\gamma \in \mathbf{Q}_p^*$ представляется формой g. Предполагая, что форма f приведена к виду $\alpha x^2 + \beta y^2$, мы будем иметь

$$(\alpha, -\alpha\beta) = e(f) = e(g) = (\gamma, -\delta(g)) = (\gamma, -\alpha\beta),$$

откуда

$$(\gamma\alpha^{-1}, -\alpha\beta) = 1.$$

По определению символа Гильберта это значит, что разрешимо уравнение

$$\gamma\alpha^{-1}x^2 - \alpha\beta y^2 - z^2 = 0$$

в отличных от нуля x, y и z. Но тогда

$$\gamma = \alpha\left(\frac{z}{x}\right)^2 + \beta\left(\frac{\alpha y}{x}\right)^2,$$

т. е. γ представляется и формой f. Эквивалентность f и g следует теперь из теоремы 11 § 1 Дополнения.

5. Замечания о формах высших степеней. Доказанная нами теорема 5 о квадратичных формах в поле $\mathbb{Q}_p$ принадлежит к числу часто встречающихся в теории чисел фактов такого типа: «все обстоит хорошо, если число переменных достаточно велико». В нашем случае «хорошо» означает, что квадратичная форма представляет нуль в поле p-адических чисел, а «достаточно большое» число переменных равно пяти. Очень интересно было бы проследить это явление и дальше — для форм любых степеней над полем p-адических чисел.

Точная постановка вопроса заключается в следующем. Фиксируем простое число p. Для любого натурального числа r найти минимальное число $N_p(r)$, обладающее тем свойством, что любая форма степени r с p-адическими коэффициентами, у которой число переменных больше $N_p(r)$, представляет нуль в поле p-адических чисел $\mathbb{Q}_p$. Далеко не очевидный a priori факт существования такого конечного числа $N_p(r)$ был доказан Брауэром [66]. Однако оценка, получающаяся из его доказательства, чрезмерно велика.

Легко устанавливается, что

$$N_p(r) \geqslant r^2. \tag{14}$$

Для доказательства неравенства (14) надо показать, что для любого r существуют формы степени r от r^2 переменных, не представляющие нуля в поле p-адических чисел. Построим пример такой формы. Для этого вспомним, что в п. 2 § 1 этой главы была построена такая форма $F(x_1, \ldots, x_n)$ степени n и от n переменных, что сравнение

$$F(x_1, \ldots, x_n) \equiv 0 \pmod p$$

имеет только одно решение:

$$x_1 \equiv 0 \pmod p, \quad \ldots, \quad x_n \equiv 0 \pmod p. \tag{15}$$

Положим

$$\Phi(x_1, \ldots, x_{n^2}) = F(x_1, \ldots, x_n) + pF(x_{n+1}, \ldots, x_{2n}) + \ldots$$
$$\ldots + p^{n-1}F(x_{n^2-n+1}, \ldots, x_{n^2})$$

и докажем, что форма Φ не представляет нуля в поле p-адических чисел. Допустим противное, т. е. допустим, что уравнение

$$\Phi(x_1, \ldots, x_{n^2}) = 0 \tag{16}$$

имеет ненулевое решение. В силу однородности Φ мы можем счи-

тать, что все неизвестные целые и хоть одна из них не делится на p. Рассматривая (16) как сравнение по модулю p, мы получаем $F(x_1, \ldots, x_n) \equiv 0 \pmod{p}$, откуда ввиду (15) следует, что $x_1 = px_1', \ldots, x_n = px_n'$. Равенство (16) принимает теперь вид

$$p^n F(x_1', \ldots, x_n') + pF(x_{n+1}, \ldots, x_{2n}) + \ldots$$
$$\ldots + p^{n-1} F(x_{n^2-n+1}, \ldots, x_{n^2}) = 0$$

или, после сокращения на p,

$$F(x_{n+1}, \ldots, x_{2n}) + \ldots + p^{n-2} F(x_{n^2-n+1}, \ldots, x_{n^2}) +$$
$$+ p^{n-1} F(x_1', \ldots, x_n') = 0.$$

В качестве следующего шага доказательства мы получим, что $x_{n+1}, \ldots, x_{2n}$ делятся на p. Повторив это рассуждение n раз, мы докажем, что все $x_1, \ldots, x_{n^2}$ делятся на p, в противоречии с тем, что предположили.

Таким образом, для $N_p(r)$ мы имеем оценку снизу (14). Но согласно теореме 5 при $r = 2$ имеет место равенство $N_p(2) = 4$ (при $r = 1$ также имеем очевидное равенство $N_p(1) = 1$). Естественно возникает вопрос, не будет ли равенство $N_p(r) = r^2$ выполняться для любого r? Ряд результатов, казалось, подтверждал такое предположение. Так, В. Б. Демьянов [45] и Левис [101] доказали, что любая кубическая форма над полем p-адических чисел, число переменных которой больше 9, представляет нуль; другими словами, $N_p(3) = 9$. Далее, Экс и Кочен [57], применив очень оригинальный метод, заимствованный из математической логики, установили, что для фиксированного r почти для всех p, т. е. для всех, за исключением конечного числа, имеет место равенство $N_p(r) = r^2$. Кроме того, «диагональные» формы $\sum_{i=1}^{n} a_i x_i^r$ в поле p-адических чисел всегда допускают нетривиальное представление нуля, если только число переменных n удовлетворяет неравенству $n > r^2$ (см. [71]).

В связи с вопросом о представлении нуля формами над заданным полем было введено следующее определение. Говорят, что поле K *обладает свойством* C_i, если любая форма степени d от n переменных с коэффициентами из K при $n > d^i$ допускает нетривиальное представление нуля. Свойством C_0 обладают алгебраически замкнутые поля и только они. Теорема Шевалле (теорема 3 § 1) означает, что поле вычетов $\mathbb{F}_p$ обладает свойством C_1 (это верно для любого конечного поля). Свойством C_2 обладает поле формальных степенных рядов $\mathbb{F}_p\{t\}$, очень похожее на поле p-адических чисел (задача 23). Вопрос о равенстве $N_p(r) = r^2$ равносилен вопросу: обладает ли поле p-адических чисел свойством C_2?

Эти предположения были перенесены и на системы форм. По аналогии с теоремой 4 § 1 предполагалось, что система уравнений

$$F_1(x_1, \ldots, x_n) = 0,$$
$$\ldots\ldots\ldots$$
$$F_k(x_1, \ldots, x_n) = 0,$$

где $F_1, \ldots, F_k$ — формы с p-адическими коэффициентами степеней $r_1, \ldots, r_k$, имеет ненулевое решение, если $n > r_1^2 + \ldots + r_k^2$. В. Б. Демьянов доказал это утверждение для случая пары квадратичных форм ($k = 2$; $r_1 = r_2 = 2$). Простое доказательство результата Демьянова содержится в работе [63].

Всей этой системе красивых и взаимосвязанных гипотез был нанесен удар, когда в 1966 г. Г. Тержанян [137] построил пример формы 4-й степени от 18 переменных, не представляющей нуля в поле 2-адических чисел (задачи 15—16). В дальнейшем аналогичные примеры были построены и для $p \neq 2$ (задачи 17—18). Стоит заметить при этом, что во всех известных примерах неравенства $N_p(r) > r^2$ формы имеют четную степень. Аналогичные примеры форм нечетной степени не найдены.

После этого можно было еще надеяться, что функция $N_p(r)$ растет все же не слишком быстро, например, что поле p-адических чисел обладает свойством C_3. Эти надежды, однако, не оправдались. Г. И. Архипов и А. А. Карацуба [41] показали, что для любого p функция $N_p(r)$ растет быстрее любой степени r, почти как показательная функция. Ниже приведены их рассуждения для случая $p \neq 2$ (случай $p = 2$ рассматривается аналогично). Напомним, что p-адическая единица u называется *главной*, если $u \equiv 1 \pmod p$.

Лемма. *Пусть* $a \leqslant r_1 < \ldots < r_m \leqslant b$ — *натуральные числа*, N — *натуральное число*, $N + a - b \geqslant 1$, $p \neq 2$. *Если для главных* p-*адических единиц* $u_1, \ldots, u_n$ *выполнены сравнения*

$$\sum_{i=1}^{n} u_i^{r_j} \equiv 0 \pmod{p^N}, \qquad 1 \leqslant j \leqslant m,$$

то $n \geqslant p^h$, *где* $h = \min(m, N + a - b)$.

Доказательство. Согласно задаче 16 § 3 при некоторых натуральных c_i справедливы сравнения

$$u_i \equiv (1 + p)^{c_i} \pmod{p^N}, \quad 1 \leqslant i \leqslant n.$$

Введем в рассмотрение многочлен

$$f(t) = t^{c_1} + \ldots + t^{c_n}.$$

Так как $f(1) = n$, то для доказательства леммы достаточно убедиться, что $\nu(f(1)) \geqslant h$. Положим

$$\varphi(t) = (t - x_1) \ldots (t - x_m), \qquad x_j = (1 + p)^{r_j}, \quad 1 \leqslant j \leqslant m,$$

и разделим $f(t)$ на $\varphi(t)$ с остатком:

$$f(t) = \varphi(t)q(t) + g(t),$$

так что $g(t)$ имеет степень $<m$. Так как

$$f(x_j) = \sum_{i=1}^{n} (1+p)^{c_i r_j} \equiv \sum_{i=1}^{n} u_i^{r_j} \equiv 0 \pmod{p^N},$$

то также и $g(x_j) \equiv 0 \pmod{p^N}$. Согласно задаче 15 § 3 $\nu(1-x_j) = 1+\nu(r_j)$, поэтому

$$\nu(\varphi(1)) = m + \sum \nu(r_j) \geqslant m.$$

Нам достаточно теперь убедиться лишь в том, что $\nu(g(1)) \geqslant N+a-b$.

Согласно интерполяционной формуле Лагранжа

$$g(t) = \sum_{k=1}^{m} g_k(t), \qquad g_k(t) = \frac{g(x_k)}{\varphi'(x_k)} \prod_{j \neq k} (t - x_j).$$

Дадим оценку снизу для $\nu(g_k(1))$. Имеем

$$\nu(g_k(1)) \geqslant N + \sum_{j \neq k} (1 + \nu(r_j)) - \nu(\varphi'(x_k)).$$

Воспользуемся еще раз задачей 15 § 3. Так как

$$x_k - x_j = x_j((1+p)^{r_k - r_j} - 1),$$

то $\nu(x_k - x_j) = 1 + \nu(r_k - r_j)$, а значит,

$$\nu(\varphi'(x_k)) = m - 1 + A,$$

где

$$A = \sum_{j<k} \nu(r_k - r_j) + \sum_{j>k} \nu(r_j - r_k) \leqslant$$

$$\leqslant \sum_{\rho=1}^{r_k - a} \nu(\rho) + \sum_{\rho=1}^{b - r_k} \nu(\rho) = \nu((r_k - a)!) + \nu((b - r_k)!) <$$

$$< r_k - a + b - r_k = b - a$$

(нами использована задача 17 § 3). Окончательно,

$$\nu(g_k(1)) \geqslant N + m - 1 - \nu(\varphi'(x_k)) >$$

$$> N + m - 1 - (m - 1 + b - a) = N + a - b.$$

Таким образом, $\nu(g(1)) \geqslant N + a - b$, а отсюда, как уже отмечалось, и вытекает утверждение леммы.

Следствие. Пусть $a \leqslant r_1 < \ldots < r_m = b$ — натуральные числа, $p \neq 2$, $pa - b \geqslant 1$. Если система m уравнений

$$\sum_{i=1}^{n} x_i^{(p-1)r_j} = 0, \qquad 1 \leqslant j \leqslant m, \tag{17}$$

имеет в поле p-адических чисел ненулевое решение, то

$$n \geqslant p^h, \qquad h = \min(m, pa-b).$$

В самом деле, мы можем считать, что p-адические числа x_i, удовлетворяющие системе, все целые и не делятся на p одновременно. Положим $N=(p-1)a$ и перейдем к сравнениям по модулю p^N. Если некоторое x_i делится на p, то $x_i^{(p-1)r_j} \equiv 0 \pmod{p^N}$. Выбросим из наших сравнений все такие x_i, если они имеются. В оставшихся слагаемых (число которых $n_1 \leqslant n$) все x_i — p-адические единицы, а значит, $u_i = x_i^{p-1}$ — главные p-адические единицы. Следовательно, по лемме $n_1 \geqslant p^h$.

Переход от системы форм к одной форме осуществляется теперь уже просто. Пусть r — произвольное натуральное число, делящееся на $p-1$. Положим

$$m = r^2, \qquad a = \frac{3m}{p-1}, \qquad b = a + 2m,$$

так что $pa - b = m$, $h = m$. Для $k = 1, \ldots, m$ вводим формы

$$H_k(x_1, \ldots, x_n) = \left(\sum_{i=1}^{n} x_i^{(p-1)(a+k)}\right)\left(\sum_{i=1}^{n} x_i^{(p-1)(b-k)}\right).$$

Все эти формы имеют одну и ту же степень $(p-1)(a+b) = (2p-2)(a+m)$. Обратимся теперь к форме $\Phi = \Phi(y_1, \ldots, y_{r^2})$ степени r от $m = r^2$ переменных, которую мы построили при доказательстве неравенства (14) и которая не допускает нетривиального представления нуля в поле p-адических чисел. Подставим в форму Φ вместо переменных $y_1, \ldots, y_m$ формы $H_1, \ldots, H_m$. Мы получим форму $F = F(x_1, \ldots, x_n) = \Phi(H_1, \ldots, H_m)$ степени $d = 2(p+2)r^3$. Допустим, что форма F представляет нуль. Согласно свойству формы Φ это возможно лишь при условии, что при любом k $(1 \leqslant k \leqslant m)$ хоть один из сомножителей формы H_k обращается в нуль. Но это значит, что система m уравнений вида (17) имеет ненулевое решение, а значит, $n > p^m$. Выражая здесь m через степень d формы F, получаем

$$n \geqslant p^{cd^{2/3}}, \qquad c = (2p+4)^{-2/3}.$$

Таким образом, существует константа C такая, что для сколь угодно больших r имеем оценку

$$N_p(r) > C^{\sqrt[3]{r^2}}, \qquad C > 1, \tag{18}$$

и, следовательно, поле p-адических чисел $\mathbb{Q}_p$ не обладает свойством C_i ни при каком i. Используя форму F точно так же, как нами была использована форма Φ, т. е. подставляя в нее формы H_k, можно улучшить показатель в неравенстве (18), например, до $r/(\log r)^{3/2}$.

В свете оценки (18) становится особенно интересным приведенный выше результат Акса и Кочена, согласно которому при фиксированном r равенство $N_p(r) = r^2$ имеет место для всех p, кроме конечного числа исключений. Каковы же эти исключительные значения p, неизвестно (даже для $r = 4$).

Замечание. Для рассмотренного в лемме многочлена $f(t)$ можно получить (следуя доказательству леммы) сравнение $f(\xi) \equiv 0 \pmod{p^h}$ для всех ξ, для которых $\xi \equiv 1 \pmod{p}$. Для этих значений $f(\xi)$ мы имеем, следовательно, оценку сверху относительно p-адической метрики φ_p. Возникает вопрос, не будет ли справедлив соответствующий аналог этого факта для произвольных аналитических p-адических функций (относительно определения аналитической функции см. п. 1 § 5 гл. IV)? Другими словами, если аналитическая функция принимает малые значения в подходящих точках круга $\varphi_p(x-1) < 1$, то нельзя ли оценить ее значения во всех точках этого круга?

Задачи

1. Доказать следующие свойства символа Гильберта:

1) $$(\alpha, 1-\alpha) = +1, \quad \alpha \neq 1;$$

2) $$(\alpha, \beta) = (\gamma, -\alpha\beta), \quad \gamma = \alpha\xi^2 + \beta\eta^2 \neq 0;$$

3) $$(\alpha\gamma, \beta\gamma) = (\alpha, \beta)\,(\gamma, -\alpha\beta).$$

2. Для квадратичной формы $f = \alpha_1 x_1^2 + \ldots + \alpha_n x_n^2$ $\left(\alpha_i \in \mathbb{Q}_p^*\right)$ выражение

$$c_p(f) = (-1, -1) \prod_{1 \leqslant i < j \leqslant n} (\alpha_i, \alpha_j)$$

носит название *символа Хассе*. Доказать, что

$$c_p(\alpha x^2 + f) = c_p(f)\,(\alpha, -\delta),$$

$$c_p(\alpha x^2 + \beta y^2 + f) = c_p(f)\,(\alpha\beta, -\delta)\,(\alpha, \beta)$$

(δ — определитель формы f).

3. Пусть неособенная квадратичная форма $f = \alpha_1 x_1^2 + \ldots + \alpha_n x_n^2$ с p-адическими коэффициентами представляет число $\gamma \neq 0$ из $\mathbb{Q}_p$. Доказать, что есть такое представление $\gamma = \alpha_1\xi_1^2 + \ldots + \alpha_n\xi_n^2$ $(\xi_i \in \mathbb{Q}_p)$, что все «отрезки» $\gamma_k = \alpha_1\xi_1^2 + \ldots + \alpha_k\xi_k^2$ $(1 \leqslant k \leqslant n)$ будут отличны от нуля (использовать теоремы 5 и 8 § 1 Дополнения).

4. При тех же обозначениях показать, что форма f эквивалентна диагональной форме вида $g = \gamma y_1^2 + \beta_2 y_2^2 + \ldots + \beta_n y_n^2$, для которой $c_p(g) = c_p(f)$. (Доказать предварительно, что форма $\alpha x^2 + \beta y^2$ преобразованием $x = \mu X - \nu\beta Y$, $y = \nu X + \mu\alpha Y$ $(\alpha\mu^2 + \beta\nu^2 = \gamma \neq 0)$ приводится к виду $\gamma X^2 + \alpha\beta\gamma Y^2$, причем $(\alpha, \beta) = (\gamma, \alpha\beta\gamma)$.)

5. Индукцией по числу переменных показать, что эквивалентные неособенные диагональные квадратичные формы над полем $\mathbb{Q}_p$ имеют одно и то же значение символа Хассе (использовать теорему 4 § 1 Дополнения). Символ Хассе теперь можно определить для произвольных неособенных квадратичных форм: если форма f эквивалентна диагональной форме f_0, то полагаем $c_p(f) = c_p(f_0)$.

6. Пусть f_1 и f_2 — две квадратичные формы над полем $\mathbb{Q}_p$ с определителями $\delta_1 \neq 0$ и $\delta_2 \neq 0$. Доказать, что

$$c_p(f_1 + f_2) = c_p(f_1)\, c_p(f_2)\, (-1, -1)\, (\delta_1, \delta_2).$$

7. Пусть f — неособенная квадратичная форма над полем $\mathbb{Q}_p$, δ — ее определитель и α — отличное от нуля число поля $\mathbb{Q}_p$. Доказать, что

$$c_p(\alpha f) = \begin{cases} c_p(f)\, (\alpha, (-1)^{(n+1)/2}), & \text{если } n \text{ нечетное}, \\ c_p(f)\, (\alpha, (-1)^{n/2}\delta), & \text{если } n \text{ четное}. \end{cases}$$

8. Доказать, что неособенная квадратичная форма от трех переменных над полем $\mathbb{Q}_p$ представляет нуль тогда и только тогда, когда $c_p(f) = +1$.

9. Пусть f — неособенная квадратичная форма над полем $\mathbb{Q}_p$ от четырех переменных и δ — ее определитель. Доказать, что f не представляет нуля в $\mathbb{Q}_p$ тогда и только тогда, когда δ — квадрат в $\mathbb{Q}_p$ и $c_p(f) = -1$.

10. Пусть f — неособенная квадратичная форма над $\mathbb{Q}_p$ от n переменных и δ — ее определитель. Доказать, что f представляет p-адическое число $\alpha \neq 0$ тогда и только тогда, когда выполнено одно из следующих условий:

1) $n = 1$ и $\alpha\delta$ — квадрат в $\mathbb{Q}_p$;
2) $n = 2$ и $c_p(f) = (-\alpha, -\delta)$;
3) $n = 3$, $-\alpha\delta$ — квадрат в $\mathbb{Q}_p$ и $c_p(f) = 1$;
4) $n = 3$ и $-\alpha\delta$ не является квадратом в $\mathbb{Q}_p$;
5) $n \geqslant 4$.

11. Выяснить, при каких условиях неособенная квадратичная форма над полем $\mathbb{Q}_p$ не представляет нуля (нетривиальным сбразом), но все же представляет все p-адические числа.

12. В каких полях p-адических чисел форма $2x^2 - 15y^2 + 14z^2$ не представляет нуля?

13. Какие 5-адические числа представляет форма $2x^2 + 5y^2$?

14. Пусть f и f' — неособенные квадратичные формы от n переменных над полем $\mathbb{Q}_p$; δ и δ' — их определители. Доказать, что f и f' эквивалентны тогда и только тогда, когда $c_p(f) = c_p(f')$ и $\delta = \delta'\alpha^2$ $(\alpha \in \mathbb{Q}_p)$.

15. Доказать, что в кольце целых 2-адических чисел многочлен

$$h(x, y, z) = x^4 + y^4 + z^4 - xyz(x + y + z) - (x^2y^2 + y^2z^2 + z^2x^2)$$

обладает свойством: если хоть одно из значений x, y, z не делится на 2, то $h(x, y, z) \equiv 1 \pmod 4$.

16. Пусть $h(x, y, z)$ — многочлен предыдущей задачи. Положим

$$g(x_1, \ldots, x_9) = h(x_1, x_2, x_3) + h(x_4, x_5, x_6) + h(x_7, x_8, x_9),$$

$$\Phi(x_1, \ldots, x_{18}) = g(x_1, \ldots, x_9) + 4g(x_{10}, \ldots, x_{18}).$$

Доказать, что в поле 2-адических чисел форма Φ допускает только тривиальное представление нуля.

17. Для $p \neq 2$ положим

$$h(x_1, \ldots, x_{p-1}) = \sum_{i=1}^{p-1} x_i^{p(p-1)} + \sum_{s=2}^{p-1} \frac{1}{s} (-1)^{s-1} \varphi_s(x_1, \ldots, x_{p-1}),$$

где φ_s — моногенный симметрический многочлен от переменных $x_1, \ldots, x_{p-1}$, определяемый одночленом

$$x_1^{(p-1)(p-s+1)} (x_2 \ldots x_s)^{p-1}, \quad 2 \leqslant s \leqslant p-1.$$

Для формы h доказать, что

$$h(x_1, \ldots, x_{p-1}) \equiv 1 \pmod{p^2},$$

если только $x_i \not\equiv 0 \pmod{p}$ хоть при одном i $(1 \leqslant i \leqslant p-1)$ (сравнения рассматриваются в кольце целых p-адических чисел).

18. В обозначениях задачи 17 положим

$$g(x_1, \ldots, x_m) = h(x_1, \ldots, x_{p-1}) + h(x_p, \ldots, x_{2p-2}) + \ldots + h(x_{m-p+2}, \ldots, x_m),$$

где $m = (p-1)(p^2-1)$. Доказать, что в кольце целых p-адических чисел форма

$$\Phi(x_1, \ldots, x_{ms}) = \\ = g(x_1, \ldots, x_m) + p^2 g(x_{m+1}, \ldots, x_{2m}) + \ldots + p^{2s-2} g(x_{ms-m+1}, \ldots, x_{ms})$$

степени $p(p-1)$ от $\frac{1}{2}p(p+1)(p-1)^3$ переменных $\left(s = \frac{1}{2}p(p-1)\right)$ допускает только тривиальное представление нуля.

19. Пусть $f(x_1, \ldots, x_n)$ — форма степени r с целыми p-адическими коэффициентами $(p \neq 2)$, обладающая свойством

$$f(x_1, \ldots, x_n) \equiv 1 \pmod{p^{m+1}},$$

если только значение хоть одного x_i не делится на p $(m \geqslant 0)$. Доказать, что тогда r делится на $(p-1)p^m$.

Указание. Рассмотреть значение $f(c, 0, \ldots, 0)$, где c — первообразный корень по модулю p^{m+1}.

20. Пусть $p \neq 2$. Доказать, что группа классов Витта над полем p-адических чисел $\mathbb{Q}_p$ есть прямое произведение четырех групп 2-го порядка, если $p \equiv 1 \pmod 4$, и прямое произведение двух циклических групп 4-го порядка, если $p \equiv 3 \pmod 4$.

21. Доказать, что над полем 2-адических чисел группа классов Витта есть прямое произведение трех групп: одной циклической группы 8-го порядка и двух групп 2-го порядка.

22. Пусть $F(x_1, \ldots, x_n)$ — форма степени d от n переменных с коэффициентами из кольца многочленов $\mathbb{F}_p[t]$ ($\mathbb{F}_p$ — поле вычетов по простому модулю p). Доказать, что если $n > d^2$, то уравнение $F(x_1, \ldots, x_n) = 0$ имеет ненулевое решение в $\mathbb{F}_p[t]$.

Указание. Представить x_i в виде $\sum_{j=1}^{s} \xi_{ij} t^j$, $\xi_{ij} \in \mathbb{F}_p$, разложить $F(x_1, \ldots, x_n)$ по степеням t и заметить, что при достаточно большом s применима теорема 4 § 1.

23. Доказать, что поле рациональных функций $\mathbb{F}_p(t)$ и поле формальных степенных рядов $\mathbb{F}_p\{t\}$ обладают свойством C_2.

24. Получить оценку типа (18) в случае $p = 2$.

§ 7. Рациональные квадратичные формы

1. Теорема Минковского — Хассе. В этом параграфе мы изложим доказательство одного из красивейших результатов теории чисел — так называемой теоремы Минковского — Хассе, о которой мы уже упоминали в начале главы.

Теорема 1 (Минковского — Хассе). *Квадратичная форма с рациональными коэффициентами тогда и только тогда представ-*

ляет нуль в поле рациональных чисел, когда она представляет нуль в поле вещественных чисел и во всех полях p-адических чисел (для всех простых p).

Доказательство этой теоремы существенно зависит от числа переменных n квадратичной формы. При $n=1$ утверждение теоремы тривиально. В случае $n=2$ ее доказательство проводится совсем просто. Если рациональная бинарная квадратичная форма f определителя $d\neq 0$ представляет нуль в поле вещественных чисел, то $-d>0$ (см. Дополнение, § 1, теорема 10); следовательно, $-d=p_1^{k_1}\dots p_s^{k_s}$, где p_i — попарно различные простые числа. Если теперь f представляет нуль в поле $\mathbb{Q}_{p_i}$, то, поскольку $-d$ является квадратом в $\mathbb{Q}_{p_i}$, показатель k_i должен быть четным ($i=1, \dots, s$). Но в таком случае $-d$ будет квадратом и в поле рациональных чисел $\mathbb{Q}$ и, следовательно, f представляет нуль в $\mathbb{Q}$.

Доказательство теоремы при $n\geqslant 3$ намного сложнее. Различные представляющиеся здесь случаи будут разобраны в следующих пунктах. Сейчас же мы сделаем несколько замечаний.

Будем считать, что коэффициенты рассматриваемой квадратичной формы $f(x_1, \dots, x_n)$ — целые рациональные числа (если это не так, то мы умножим форму на общий знаменатель ее коэффициентов). Ясно, что разрешимость уравнения

$$f(x_1, \dots, x_n)=0 \tag{1}$$

в поле рациональных чисел $\mathbb{Q}$ или в поле p-адических чисел $\mathbb{Q}_p$ эквивалентна, в силу однородности, его разрешимости в кольце целых рациональных чисел $\mathbb{Z}$ или соответственно в кольце целых p-адических чисел $\mathbb{Z}_p$. Что касается разрешимости (1) в вещественных числах, то она эквивалентна тому, что f — неопределенная форма. Ввиду этого и ввиду теоремы 2 § 5 теореме Минковского — Хассе можно придать следующую форму:

Для разрешимости неопределенного уравнения (1) *в целых рациональных числах необходимо и достаточно, чтобы форма f была неопределенной и чтобы при любом модуле вида p^m сравнение*

$$f(x_1, \dots, x_n)\equiv 0 \pmod{p^m}$$

имело решение, в котором значение хоть одной неизвестной не делится на p. Согласно теореме 5 § 6 в поле p-адических чисел всякая форма от пяти и более переменных всегда представляет нуль. Следовательно, для таких форм теорема Минковского — Хассе принимает вид:

Для того чтобы неособенная рациональная квадратичная форма от $n\geqslant 5$ переменных представляла нуль в поле рациональных чисел, необходимо и достаточно, чтобы она была неопределенной.

Таким образом, условия разрешимости в полях p-адических чисел фактически надо проверять лишь для $n=3$ и 4. Для этих

значений n теорема Минковского — Хассе также дает нам эффективный критерий разрешимости уравнения (1). Действительно, если форма f приведена к сумме квадратов $f = \sum a_i x_i^2$, то для нечетных простых p, не делящих ни одного из коэффициентов a_i, форма f при $n \geqslant 3$ всегда представляет нуль в $\mathbb{Q}_p$ на основании следствия 2 к теореме 3 § 6. Следовательно, фактической проверке подлежит только конечное число простых чисел p. Для каждого из этих p вопрос о представлении нуля формой f в поле $\mathbb{Q}_p$ решается теоремами предшествующего параграфа.

В силу теоремы 6 § 1 Дополнения из теоремы 1 вытекает следующее утверждение.

Следствие. *Для того чтобы неособенная квадратичная форма с рациональными коэффициентами представляла рациональное число a, необходимо и достаточно, чтобы она представляла a в поле вещественных чисел и во всех полях p-адических чисел $\mathbb{Q}_p$.*

2. Формы от трех переменных. Приступим к доказательству теоремы Минковского — Хассе. В этом пункте мы разберем случай $n = 3$. Для форм от трех переменных теорема 1 была доказана (в несколько других терминах) еще Лежандром. Формулировка Лежандра приведена в задаче 1.

Пусть форма приведена к сумме квадратов $a_1x^2 + a_2y^2 + a_3z^2$. Неопределенность формы означает, что коэффициенты a_1, a_2, a_3 не все одного знака. Умножив форму в случае надобности на -1, мы придем к случаю, когда два коэффициента положительны и один отрицательный. Кроме того, мы можем, очевидно, считать числа a_1, a_2, a_3 целыми, свободными от квадратов и взаимно простыми в совокупности (их можно сократить на общий наибольший делитель). Далее, если, например, a_1 и a_2 имеют простой общий множитель p, то, умножая форму на p и беря px и py за новые переменные, мы получим форму с коэффициентами a_1/p, a_2/p, pa_3. Повторяя этот процесс несколько раз, мы заменим нашу форму формой вида

$$ax^2 + by^2 - cz^2, \tag{2}$$

в которой целые положительные коэффициенты a, b и c попарно взаимно просты (и свободны от квадратов).

Пусть p — какой-нибудь нечетный простой делитель числа c. Так как по условию форма (2) представляет нуль в $\mathbb{Q}_p$, то в силу теоремы 3 § 6 и следствия 1 этой теоремы сравнение $ax^2 + by^2 \equiv 0 \pmod p$ имеет нетривиальное решение, скажем (x_0, y_0). Но тогда для формы $ax^2 + by^2$ по модулю p имеем разложение на линейные множители:

$$ax^2 + by^2 \equiv ay_0^{-2}(xy_0 + yx_0)(xy_0 - yx_0) \pmod p.$$

Это же, разумеется, верно и для формы (2), т. е. имеет место сравнение

$$ax^2 + by^2 - cz^2 \equiv L^{(p)}(x, y, z)M^{(p)}(x, y, z) \pmod p, \tag{3}$$

в котором $L^{(p)}$ и $M^{(p)}$ — целочисленные линейные формы. Аналогичные сравнения имеют место и для нечетных простых делителей p коэффициентов a и b, а также и для $p=2$, так как

$$ax^2+by^2-cz^2\equiv(ax+by-cz)^2 \pmod 2.$$

Найдем теперь такие линейные формы $L(x, y, z)$ и $M(x, y, z)$, чтобы

$$L(x, y, z)\equiv L^{(p)}(x, y, z) \pmod p,$$
$$M(x, y, z)\equiv M^{(p)}(x, y, z) \pmod p$$

для всех простых делителей p коэффициентов a, b и c. Сравнения (3) показывают, что тогда

$$ax^2+by^2-cz^2\equiv L(x, y, z)M(x, y, z) \pmod{abc}. \tag{4}$$

Будем придавать переменным x, y, z целые значения, удовлетворяющие условиям

$$0\leqslant x<\sqrt{bc},\quad 0\leqslant y<\sqrt{ac},\quad 0\leqslant z<\sqrt{ab}. \tag{5}$$

Если мы исключим из рассмотрения случай $a=b=c=1$ (для формы $x^2+y^2-z^2$ утверждение теоремы очевидно: она представляет нуль в любом поле), то, в силу попарной взаимной простоты a, b и c, числа $\sqrt{bc}$, $\sqrt{ac}$ и $\sqrt{ab}$ не будут все целыми. Отсюда легко следует, что число троек (x, y, z), удовлетворяющих условиям (5), будет строго больше, чем $\sqrt{ab}\cdot\sqrt{bc}\cdot\sqrt{ac}=abc$. Рассмотрим значения, принимаемые линейной формой $L(x, y, z)$ при этих значениях переменных. Так как число троек (x, y, z) с условием (5) больше числа вычетов по модулю abc, то для двух различных троек (x_1, y_1, z_1) и (x_2, y_2, z_2) будем иметь сравнение

$$L(x_1, y_1, z_1)\equiv L(x_2, y_2, z_2) \pmod{abc}.$$

В силу линейности формы L отсюда следует, что

$$L(x_0, y_0, z_0)\equiv 0 \pmod{abc}$$

при $x_0=x_1-x_2$, $y_0=y_1-y_2$, $z_0=z_1-z_2$. Из сравнения (4) получим тогда, что

$$ax_0^2+by_0^2-cz_0^2\equiv 0 \pmod{abc}. \tag{6}$$

Так как для троек (x_1, y_1, z_1) и (x_2, y_2, z_2) выполнены условия (5), то

$$|x_0|<\sqrt{bc},\quad |y_0|<\sqrt{ac},\quad |z_0|<\sqrt{ab},$$

а значит,

$$-abc<ax_0^2+by_0^2-cz_0^2<2abc. \tag{7}$$

Неравенство (7) совместимо со сравнением (6), только если или

$$ax_0^2+by_0^2-cz_0^2=0, \tag{8}$$

или

$$ax_0^2 + by_0^2 - cz_0^2 = abc. \tag{9}$$

В первом случае мы получаем нетривиальное представление нуля формой (2), что и требовалось установить. Во втором случае мы приходим к тому же результату в силу следующей леммы.

Лемма 1. *Если форма* (2) *представляет* abc, *то она представляет также и нуль.*

Пусть x_0, y_0, z_0 удовлетворяют равенству (9). Легко видеть, что тогда

$$a(x_0z_0 + by_0)^2 + b(y_0z_0 - ax_0)^2 - c(z_0^2 + ab)^2 = 0. \tag{10}$$

Если $z_0^2 + ab \neq 0$, то это равенство доказывает лемму. Если же $-ab = z_0^2$, то форма $ax^2 + by^2$ представляет нуль (см. Дополнение, § 1, теорема 10). Но тогда форма (2) также представляет нуль, так что и в этом случае лемма справедлива.

Приведенное доказательство леммы 1 очень короткое, но оно основывается на выкладке, связанной с тождеством (10). Дадим другое доказательство, использующее более общие соображения. Если bc является квадратом, то форма $by^2 - cz^2$, а вместе с ней и форма (2) представляют нуль. Будем считать, что bc не является квадратом. В этом случае, оказывается, представимость нуля формой (2) эквивалентна тому, что ac есть норма некоторого элемента поля $\mathbb{Q}(\sqrt{bc})$. Действительно, из равенства (8) (в котором можно считать $x_0 \neq 0$) следует, что

$$ac = \left(\frac{cz_0}{x_0}\right)^2 - bc\left(\frac{y_0}{x_0}\right)^2 = N\left(\frac{cz_0}{x_0} + \frac{y_0}{x_0}\sqrt{bc}\right).$$

Обратно, если $ac = N(u + v\sqrt{bc})$, то

$$ac^2 + b(cv)^2 - cu^2 = 0.$$

Предположим теперь, что имеет место равенство (9). Умножив его на c, мы придадим ему вид

$$ac(x_0^2 - bc) = (cz_0)^2 - bcy_0^2$$

или

$$acN(\alpha) = N(\beta),$$

где $\alpha = x_0 + \sqrt{bc}$, $\beta = cz_0 + y_0\sqrt{bc}$. Но тогда

$$ac = N(\gamma), \quad \gamma = \frac{\beta}{\alpha} \in \mathbb{Q}(\sqrt{bc}),$$

а это, как мы видели, и значит, что форма (2) представляет нуль в $\mathbb{Q}$.

Обратим внимание на следующее обстоятельство. В проведенном нами доказательстве теоремы 1 для случая трех переменных

мы нигде не использовали разрешимости уравнения (2) в поле 2-адических чисел. Следовательно, из разрешимости уравнения (2) в поле вещественных чисел и в полях $\mathbb{Q}_p$ для всех нечетных p следует его разрешимость и в поле $\mathbb{Q}_2$. Аналогичное обстоятельство имеет место, оказывается, и по отношению к любому другому полю $\mathbb{Q}_q$. Именно, если рациональная квадратичная форма от трех переменных представляет нуль в поле вещественных чисел и во всех полях $\mathbb{Q}_p$, за исключением, быть может, поля $\mathbb{Q}_q$, то она представляет нуль и в поле $\mathbb{Q}_q$ (а значит, по доказанному, и в поле рациональных чисел $\mathbb{Q}$).

Попробуем выяснить причину этого обстоятельства. Рассмотрим для этого условия представления нуля формой

$$ax^2 + by^2 - z^2 \tag{11}$$

во всех полях $\mathbb{Q}_p$ и в поле вещественных чисел (здесь a и b — произвольные отличные от нуля рациональные числа, ясно, что всякая неособенная рациональная квадратичная форма от трех переменных преобразованием переменных и домножением на некоторый рациональный множитель может быть приведена к виду (11)). Согласно п. 3 § 6 условие представимости нуля формой (11) в поле p-адических чисел может быть записано в виде равенства

$$\left(\frac{a,b}{p}\right) = 1, \tag{12}$$

где $\left(\frac{a,b}{p}\right)$ — символ Гильберта в поле $\mathbb{Q}_p$. Мы применили здесь для символа Гильберта (a, b) при рациональных a и b обозначение $\left(\frac{a,b}{p}\right)$ для указания того поля, в котором мы его рассматриваем. Необходимость этого изменения в обозначениях вызвана тем, что сейчас нам надо будет рассматривать символы Гильберта одновременно в различных полях $\mathbb{Q}_p$.

Что касается поля вещественных чисел, то в нем форма (11) представляет нуль, очевидно, тогда и только тогда, когда хоть одно из чисел a или b положительно. Чтобы это условие также записать в виде некоторого равенства типа (12), перенесем результаты п. 3 § 6 на поле вещественных чисел. Условимся предварительно о следующем обозначении. Все поля p-адических чисел $\mathbb{Q}_p$ и поле вещественных чисел — это все пополнения поля рациональных чисел $\mathbb{Q}$ (§ 4, п. 2). При этом поля $\mathbb{Q}_p$ взаимно однозначно соответствуют простым рациональным числам p. Желая этим соответствием охватить и поле вещественных чисел, часто вводят символ ∞, который называют бесконечно удаленным простым числом, и говорят, что поле вещественных чисел — это пополнение поля $\mathbb{Q}$, соответствующее бесконечно удаленному простому числу ∞. Обычные простые числа p, в отличие от введенного символа ∞, называют тогда конечными простыми числами. В со-

ответствии с обозначением $\mathbb{Q}_p$ для полей p-адических чисел поле вещественных чисел обозначают через $\mathbb{Q}_\infty$.

Для любого α из мультипликативной группы $\mathbb{Q}_\infty^*$ поля $\mathbb{Q}_\infty$ рассмотрим форму

$$x^2 - \alpha y^2 \tag{13}$$

и через H_α обозначим совокупность всех $\beta \in \mathbb{Q}_\infty^*$, представимых этой формой. Если $\alpha > 0$, т. е. $\alpha \in \mathbb{Q}_\infty^{*2}$, то форма (13) представляет все вещественные числа, а значит, $H_\alpha = \mathbb{Q}_\infty^*$. Если же $\alpha < 0$, т. е. α не является квадратом, то форма (13) представляет лишь положительные числа, а поэтому, как и в теореме 6 § 6, мы имеем

$$(\mathbb{Q}_\infty^* : H_\alpha) = 2. \tag{14}$$

Отсюда следует, что если для α и β из $\mathbb{Q}_\infty^*$ мы положим (α, β) равным $+1$ или -1 в зависимости от того, представляет ли форма (13) число β или нет, то для символа (α, β) будут иметь место все свойства (9)—(13) § 6. Аналогом теоремы 7 § 6, на основе которой производится вычисление символа Гильберта в p-адических полях, является здесь более простое соотношение:

$$\left.\begin{aligned} &(\alpha, \beta) = +1, \text{ если } \alpha > 0 \text{ или } \beta > 0;\\ &(\alpha, \beta) = -1, \text{ если } \alpha < 0 \text{ и } \beta < 0. \end{aligned}\right\} \tag{15}$$

В случае рациональных a и b значение (a, b) введенного символа в поле $\mathbb{Q}_\infty$ обозначается через $\left(\frac{a,b}{\infty}\right)$.

Пользуясь символом $\left(\frac{a,b}{p}\right)$, мы можем теперь переформулировать теорему 1 для форм от трех переменных следующим образом:

Форма $ax^2 + by^2 - z^2$ с отличными от нуля рациональными a и b представляет нуль в поле рациональных чисел тогда и только тогда, когда при всех p (включая $p = \infty$) выполнено равенство

$$\left(\frac{a,b}{p}\right) = 1. \tag{16}$$

Для любых отличных от нуля рациональных a и b символ $\left(\frac{a,b}{p}\right)$ отличен от $+1$ только для конечного числа значений p. Действительно, если p отлично от 2 и ∞ и если p не входит в разложения a и b в произведение степеней простых чисел (а значит, a и b являются p-адическими единицами), то, по следствию 2 к теореме 3 § 6, форма (11) представляет нуль в $\mathbb{Q}_p$ и, следовательно, для всех таких p символ $\left(\frac{a,b}{p}\right)$ равен $+1$. Помимо этого условия, значения символа $\left(\frac{a,b}{p}\right)$ при фиксированных a и b подчинены, оказывается, еще одному необходимому ограничению. Имен-

но, число тех значений p (включая $p=\infty$), для которых $\left(\frac{a,b}{p}\right)=-1$, всегда четно. В другой форме этот же факт можно выразить следующим образом:

$$\prod_p \left(\frac{a,b}{p}\right)=1, \tag{17}$$

где p пробегает все простые числа и символ ∞. В самом деле, формально бесконечное произведение слева содержит только конечное число сомножителей, отличных от $+1$, и тот факт, что само произведение равно 1, эквивалентен четности числа тех p, для которых $\left(\frac{a,b}{p}\right)=-1$.

Докажем соотношение (17). Представив a и b в виде произведения степеней простых чисел и воспользовавшись формулами (9)—(13) § 6 (справедливыми, как уже отмечалось, и при $p=\infty$), мы легко сведем доказательство формулы (17) для произвольных a и b к следующим частным случаям:

1) $a=-1$, $b=-1$;
2) $a=q$, $b=-1$ (q простое);
3) $a=q$, $b=q'$ (q и q' — простые, $q\neq q'$).

Ввиду теоремы 7 § 6 и равенств (15) настоящего параграфа мы имеем:

$$\prod_p \left(\frac{-1,-1}{p}\right)=\left(\frac{-1,-1}{2}\right)\left(\frac{-1,-1}{\infty}\right)=(-1)\cdot(-1)=1;$$

$$\prod_p \left(\frac{2,-1}{p}\right)=\left(\frac{2,-1}{2}\right)\left(\frac{2,-1}{\infty}\right)=1\cdot 1=1;$$

$$\prod_p \left(\frac{q,-1}{p}\right)=\left(\frac{q,-1}{q}\right)\left(\frac{q,-1}{2}\right)=\left(\frac{-1}{q}\right)(-1)^{\frac{q-1}{2}\cdot\frac{-1-1}{2}}=1;$$

$$\prod_p \left(\frac{2,q}{p}\right)=\left(\frac{2,q}{q}\right)\left(\frac{2,q}{2}\right)=\left(\frac{2}{q}\right)(-1)^{\frac{q^2-1}{8}}=1;$$

$$\prod_p \left(\frac{q,q'}{p}\right)=\left(\frac{q,q'}{q}\right)\left(\frac{q,q'}{q'}\right)\left(\frac{q,q'}{2}\right)=\left(\frac{q'}{q}\right)\left(\frac{q}{q'}\right)(-1)^{\frac{q'-1}{2}\cdot\frac{q-1}{2}}=1.$$

Проведенные выкладки, в которых q и q' обозначают различные нечетные простые числа, и доказывают соотношение (17).

Заметим, что в проведенном доказательстве формулы (17) мы использовали квадратичный закон взаимности Гаусса. Легко видеть, что, наоборот, зная явные выражения для символа Гильберта $\left(\frac{a,b}{p}\right)$ (теорема 7 § 6), мы можем из формулы (17) вывести закон взаимности вместе с обоими дополнениями. Таким образом, соотношение (17) эквивалентно закону взаимности Гаусса.

Предположим теперь, что форма (11) представляет нуль во всех полях $\mathbb{Q}_p$, кроме, быть может, поля $\mathbb{Q}_q$. Равенство (17) вместе с условиями $\left(\frac{a,b}{p}\right)=1$ при всех $p\neq q$ дает нам, что тогда и $\left(\frac{a,b}{q}\right)=1$. Другими словами, справедливо следующее утверждение.

Лемма 2. *Если рациональная квадратичная форма*

$$ax^2+by^2-z^2$$

представляет нуль во всех полях $\mathbb{Q}_p$ (*p пробегает все простые числа и символ* ∞), *кроме, быть может, поля* $\mathbb{Q}_q$, *то она представляет нуль и в поле* $\mathbb{Q}_q$.

3. Формы от четырех переменных. Будем считать, что форма имеет вид

$$a_1x_1^2+a_2x_2^2+a_3x_3^2+a_4x_4^2, \tag{18}$$

где все a_i целые и свободны от квадратов .В силу неопределенности формы мы можем, очевидно, потребовать, чтобы $a_1>0$ и $a_4<0$. Наряду с формой (18) мы рассмотрим формы

$$g=a_1x_1^2+a_2x_2^2 \text{ и } h=-a_3x_3^2-a_4x_4^2.$$

Идея доказательства теоремы Минковского — Хассе для форм от четырех переменных состоит в следующем. Используя факт представимости нуля формой (18) в полях $\mathbb{Q}_p$, мы покажем, что существует целое рациональное $a\neq 0$, которое представляется рационально формами g и h одновременно. Это немедленно дает нам рациональное представление нуля формой (18).

Пусть $p_1, \ldots, p_s$ — все различные нечетные простые делители коэффициентов a_1, a_2, a_3, a_4. Для каждого p, равного одному из $p_1, \ldots, p_s$, а также для $p=2$ в поле $\mathbb{Q}_p$ выберем представление нуля

$$a_1\xi_1^2+a_2\xi_2^2+a_3\xi_3^2+a_4\xi_4^2=0,$$

в котором все $\xi_i\neq 0$ (см. Дополнение, § 1, теорема 8), и положим

$$b_p=a_1\xi_1^2+a_2\xi_2^2=-a_3\xi_3^2-a_4\xi_4^2.$$

Легко видеть, что наши представления можно выбрать так, чтобы каждое $b_p\neq 0$ было целым p-адическим числом и делилось на p не выше чем в первой степени (если $b_p=0$, то формы g и h представляют нуль в $\mathbb{Q}_p$, а тогда, согласно теореме 5 § 1 Дополнения, они представляют все числа из $\mathbb{Q}_p$).

Рассмотрим систему сравнений

$$\begin{aligned} &a\equiv b_2 \pmod{16},\\ &a\equiv b_{p_1} \pmod{p_1^2},\\ &\cdots\cdots\cdots\\ &a\equiv b_{p_s} \pmod{p_s^2}. \end{aligned} \tag{19}$$

Целое рациональное a, удовлетворяющее этим сравнениям, определено однозначно по модулю $m = 16p_1^2 \dots p_s^2$. Так как b_{p_i} делится на p_i самое большее в первой степени, то $b_{p_i}a^{-1}$ — p-адическая единица, причем

$$b_{p_i}a^{-1} \equiv 1 \pmod{p_i}.$$

Согласно следствию 1 теоремы 1 § 6 отношение $b_{p_i}a^{-1}$ является квадратом в поле $\mathbb{Q}_{p_i}$. Аналогично, поскольку b_2 делится на 2 не выше чем в первой степени, то $b_2a^{-1} \equiv 1 \pmod 8$, а потому (теорема 2 § 6) b_2a^{-1} является квадратом в $\mathbb{Q}_2$.

Из того, что b_p и a отличаются на множитель, являющийся квадратом в $\mathbb{Q}_p$, вытекает, что для всех $p = 2, p_1, \dots, p_s$ формы

$$-ax_0^2 + g \quad \text{и} \quad -ax_0^2 + h \tag{20}$$

представляют нуль в $\mathbb{Q}_p$. Если число a мы выберем положительным, то в силу условий $a_1 > 0$ и $-a_4 > 0$ формы (20) представляют нуль и в поле вещественных чисел. Наконец, если p отлично от $2, p_1, \dots, p_s$ и не входит в a, т. е. если нечетное p не делит коэффициентов форм (20), то эти формы представляют нуль в $\mathbb{Q}_p$ по следствию 2 теоремы 3 § 6. Если бы в число a, помимо некоторых из простых чисел $2, p_1, \dots, p_s$, входило еще только одно простое число q, то мы могли бы к формам (20) применить лемму 2 и заключить (по теореме Минковского — Хассе для форм от трех переменных), что формы (20) представляют нуль в поле рациональных чисел. Но в таком случае для числа a мы получили бы представления

$$a = a_1c_1^2 + a_2c_2^2, \qquad a = -a_3c_3^2 - a_4c_4^2$$

с рациональными c_i, откуда

$$a_1c_1^2 + a_2c_2^2 + a_3c_3^2 + a_4c_4^2 = 0,$$

и теорема Минковского — Хассе для форм от четырех переменных была бы доказана. Оказывается, что число $a > 0$, удовлетворяющее сравнениям (19) и обладающее только что отмеченным свойством, всегда может быть найдено. Чтобы убедиться в этом, мы должны применить теорему Дирихле о простых числах в арифметической прогрессии, которая будет доказана нами в гл. V, § 3, п. 3. Теорема Дирихле утверждает, что если разность бесконечной арифметической прогрессии и первый член взаимно просты, то эта прогрессия содержит бесконечно много простых чисел. Пусть $a^* > 0$ — какое-нибудь одно из значений a, удовлетворяющих сравнениям (19). Обозначим через d общий наибольший делитель a^* и m. Так как $\frac{a^*}{d}$ и $\frac{m}{d}$ взаимно просты, то по теореме Дирихле существует такое целое $k \geqslant 0$, что $\frac{a^*}{d} + k\frac{m}{d} = q$ будет

простым. В качестве a мы возьмем теперь число

$$a = a^* + km = dq.$$

Поскольку в d входят лишь некоторые из простых чисел 2, p_1, ..., p_s, то выбранное значение a, как уже показано, дает возможность закончить доказательство теоремы 1 для форм от четырех переменных.

4. Формы от пяти и более переменных. Пусть неопределенная рациональная квадратичная форма от пяти переменных приведена к сумме квадратов

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2, \tag{21}$$

где все a_i целые и свободны от квадратов. Мы можем считать, что $a_1 > 0$ и $a_5 < 0$. Положим

$$g = a_1x_1^2 + a_2x_2^2, \qquad h = -a_3x_3^2 - a_4x_4^2 - a_5x_5^2.$$

Рассуждая дословно так же, как и в случае $n = 4$, мы найдем с помощью теоремы Дирихле целое рациональное $a > 0$, которое представляется формами g и h в поле вещественных чисел и во всех полях $\mathbb{Q}_p$, за исключением, быть может, поля $\mathbb{Q}_q$, где q — нечетное простое число, не входящее в коэффициенты a_i. Но тогда g и h представляют a и в поле $\mathbb{Q}_q$. Для формы g это устанавливается так же, как и выше, с помощью леммы 2. Что касается формы h, то она представляет нуль в $\mathbb{Q}_q$ (следствие 2 теоремы 3 § 6), а потому представляет все q-адические числа (см. Дополнение, § 1, теорема 5). По следствию теоремы Минковского — Хассе (см. конец п. 1), которое для форм от двух и трех переменных уже доказано, получаем, что формы g и h представляют a и в поле рациональных чисел. Отсюда, как и выше, легко следует, что форма (21) допускает рациональное представление нуля.

Для доказательства теоремы 1 в случае $n > 5$ достаточно заметить, что всякая неопределенная рациональная квадратичная форма f, приведенная к сумме квадратов, может быть представлена в виде $f = f_0 + f_1$, где f_0 — неопределенная форма от пяти переменных. По доказанному форма f_0, а вместе с ней и форма f представляют нуль в поле рациональных чисел. Теорема Минковского — Хассе доказана полностью.

Замечание. Теорема Минковского — Хассе допускает обобщение на случай квадратичных форм с коэффициентами из произвольного поля алгебраических чисел k. В п. 1 § 4 гл. IV нами будут перечислены все метрики φ поля алгебраических чисел k. Согласно п. 1 § 4 настоящей главы каждая метрика φ приводит нас к полному полю $\bar{k}_\varphi$, причем для эквивалентных метрик (см. задачу 2 § 4) пополнения $\bar{k}_\varphi$ совпадают. В силу естественного вложения $k \to \bar{k}_\varphi$ каждую квадратичную форму с коэффициентами из k можно рассматривать и как форму над полем $\bar{k}_\varphi$. Обобщение теоремы 1 на случай поля k формулируется следующим образом:

для того чтобы квадратичная форма $f(x_1, \ldots, x_n)$ с коэффициентами из поля алгебраических чисел k представляла нуль в поле k, необходимо и достаточно, чтобы она представляла нуль во всех пополнениях $\bar{k}_\varphi$. Доказательство этого обобщения намного труднее. Оно содержится, например, в книге [34].

5. Рациональная эквивалентность. Теорема Минковского — Хассе позволяет решить другой важный вопрос о рациональных квадратичных формах — вопрос об их эквивалентности.

Теорема 2. *Для того чтобы две неособенные квадратичные формы с рациональными коэффициентами были эквивалентны над полем рациональных чисел, необходимо и достаточно, чтобы они были эквивалентны над полем вещественных чисел и над каждым полем p-адических чисел* $\mathbb{Q}_p$.

Доказательство. Необходимость условий теоремы очевидна. Доказательство достаточности проведем индукцией по числу переменных n. Пусть $n = 1$. Эквивалентность форм ax^2 и bx^2 над некоторым полем означает, что a/b является квадратом в этом поле. Но если a/b — квадрат в поле вещественных чисел и во всех полях $\mathbb{Q}_p$, то, как мы видели в п. 1, a/b является квадратом и в поле рациональных чисел $\mathbb{Q}$. Таким образом, для случая $n = 1$ теорема 2 справедлива.

Пусть теперь $n > 1$. Выберем рациональное число $a \neq 0$, представимое формой f (над полем $\mathbb{Q}$). Так как эквивалентные формы представляют одни и те же числа, то форма g представляет a в поле вещественных чисел и во всех полях $\mathbb{Q}_p$. Но тогда по следствию теоремы Минковского — Хассе форма g представляет a и в поле $\mathbb{Q}$. Применяя теорему 2 § 1 Дополнения, заключаем, что

$$f \sim ax^2 + f_1, \quad g \sim ax^2 + g_1,$$

где f_1 и g_1 — квадратичные формы от $n-1$ переменных над полем $\mathbb{Q}$ (знак $\sim$ означает здесь эквивалентность над $\mathbb{Q}$). Из эквивалентности форм $ax^2 + f_1$ и $ax^2 + g_1$ в поле вещественных чисел и в полях $\mathbb{Q}_p$ следует, что формы f_1 и g_1 также эквивалентны во всех этих полях (см. Дополнение, § 1, теорема 4). По индуктивному предположению f_1 и g_1 эквивалентны над полем рациональных чисел $\mathbb{Q}$. Но тогда f и g также эквивалентны над $\mathbb{Q}$, и теорема 2 доказана.

В качестве примера рассмотрим вопрос об эквивалентности бинарных квадратичных форм.

Определитель $d(f)$ неособенной рациональной формы однозначно представляется в виде $d(f) = d_0(f)c^2$, где $d_0(f)$ — целое число, свободное от квадратов. Согласно теореме 1 § 1 Дополнения при переходе к эквивалентной форме значение $d_0(f)$ не меняется, а значит, оно является инвариантом класса рационально эквивалентных форм.

Пусть a — произвольное отличное от нуля рациональное число, представимое неособенной бинарной формой f. Для каждого прос-

того числа p (включая $p=\infty$) положим

$$e_p(f)=\left(\frac{a,-d(f)}{p}\right).$$

Согласно теореме 8 § 6 (которая справедлива, очевидно, и для поля вещественных чисел $\mathbb{Q}_\infty$) значение $e_p(f)$ не зависит от выбора a. Оно является, следовательно, также инвариантом формы f относительно рациональной эквивалентности.

Соединяя теорему 2 с теоремой 9 § 6 (справедливой и для поля $\mathbb{Q}_\infty$), мы получаем следующий критерий рациональной эквивалентности бинарных квадратичных форм.

Теорема 3. *Две бинарные квадратичные формы f и g рационально эквивалентны тогда и только тогда, когда*

$$d_0(f)=d_0(g) \quad \text{и} \quad e_p(f)=e_p(g) \quad \text{для всех } p.$$

Заметим, что хотя формально эквивалентность форм определяется бесконечной системой инвариантов $e_p(f)$, на самом деле число этих инвариантов конечно, так как $e_p(f)$ отлично от $+1$ только для конечного числа значений p.

Замечание. Теорема 2, так же как и теорема 1 (см. замечание в конце п. 4), допускает обобщение: для того чтобы две неособенные квадратичные формы с коэффициентами из произвольного поля алгебраических чисел k были эквивалентны над полем k, необходимо и достаточно, чтобы они были эквивалентны над каждым пополнением $\bar{k}_\varphi$.

6. **Замечания о формах высших степеней.** Аналогично тому, как это мы делали для форм с p-адическими коэффициентами в связи с теоремой 5 § 6, интересно попытаться включить теорему Минковского — Хассе и ее частный случай для $n\geqslant 5$ в систему более общих результатов или хотя бы гипотез, относящихся к формам высших степеней.

Прежде всего, естественно напрашивается вопрос, не верен ли аналог теоремы Минковского — Хассе для форм любых степеней, т. е. не будет ли представлять нуль в поле рациональных чисел всякая рациональная форма, представляющая нуль во всех полях p-адических чисел и в поле вещественных чисел. Легко построить примеры, опровергающие это предположение. Например, если q, l, q', l' — различные простые числа, такие, что $\left(\frac{l}{q}\right)=-1$, $\left(\frac{l'}{q'}\right)=-1$, и форма $x^2+qy^2-lz^2$ представляет нуль в поле 2-адических чисел, то форма четвертой степени

$$(x^2+qy^2-lz^2)(x^2+q'y^2-l'z^2) \tag{22}$$

будет представлять нуль во всех полях $\mathbb{Q}_p$ и в поле вещественных чисел, но в то же время не будет представлять нуля в поле рациональных чисел. Действительно, в поле $\mathbb{Q}_2$ первый множитель

представляет нуль по условию. Если нечетное p отлично от q и l, то в поле $\mathbb{Q}_p$ первый множитель представляет нуль в силу следствия 2 теоремы 3 § 6. Что касается полей $\mathbb{Q}_q$ и $\mathbb{Q}_l$, то в них второй множитель представляет нуль по той же причине. Однако ни один из сомножителей не представляет нуля в $\mathbb{Q}$, так как первый множитель не представляет нуля в $\mathbb{Q}_q$, а второй — в $\mathbb{Q}_{q'}$ (так как $\left(\frac{l}{q}\right) = -1$ и $\left(\frac{l'}{q'}\right) = -1$). Численным примером формы (22) может служить форма

$$(x^2 + 3y^2 - 17z^2)(x^2 + 5y^2 - 7z^2).$$

Приведенный пример может показаться несколько неубедительным, так как форма (22) приводима и может создаться впечатление, что именно в этом и кроется причина всего явления. Свободным от этого недостатка является пример уравнения

$$2x^2 + y^4 - 17z^4 = 0. \tag{23}$$

Легко проверяется (задача 14 § 5), что это уравнение имеет ненулевое решение во всех полях p-адических чисел $\mathbb{Q}_p$ (ненулевое решение имеется, очевидно, и в поле вещественных чисел). В это же время уравнение (23) в поле рациональных чисел $\mathbb{Q}$ имеет только нулевое решение $x = 0$, $y = 0$, $z = 0$. Покажем это. Допуская, что уравнение (23) имеет ненулевое решение, мы можем считать x, y, z целыми и попарно взаимно простыми. Для любого простого нечетного делителя p числа x имеем $\left(\frac{17}{p}\right) = 1$. Но тогда согласно квадратичному закону взаимности имеем также $\left(\frac{p}{17}\right) = 1$. Так как $\left(\frac{2}{17}\right) = 1$, то, следовательно, $\left(\frac{x}{17}\right) = 1$, а значит, $x \equiv u^2 \pmod{17}$ при некотором целом u. Это дает нам сравнение $2u^4 + y^4 \equiv 0 \pmod{17}$. Число u не может делится на 17 (иначе x и y одновременно делились бы на 17), поэтому $-2 \equiv v^4 \pmod{17}$ при некотором $v \in \mathbb{Z}$. Однако последнее сравнение, как легко проверить, неразрешимо, и мы получили противоречие.

Аналогичный пример однородного уравнения, а именно $3x^3 + 4y^3 + 5z^3 = 0$, указал Зельмер [123]. Тот факт, что форма $3x^3 + 4y^3 + 5z^3$ представляет нуль во всех полях p-адических чисел $\mathbb{Q}_p$, доказывается просто (задача 8 § 5). Что же касается утверждения о непредставимости нуля в поле рациональных чисел $\mathbb{Q}$, то оно более тонко (см. задачу 23 § 7 гл. III).

Аналог теоремы Минковского — Хассе для форм высших степеней неверен также и для случая, когда число переменных достаточно велико. Например, форма

$$(x_1^2 + \ldots + x_n^2)^2 - 2(y_1^2 + \ldots + y_n^2)^2$$

при $n \geqslant 5$ представляет нуль и в полях p-адических чисел, и в поле вещественных чисел, но не представляет нуля в поле

рациональных чисел ни при каком n. То же относится и к форме

$$3(x_1^2 + \ldots + x_n^2)^3 + 4(y_1^2 + \ldots + y_n^2)^3 - 5(z_1^2 + \ldots + z_n^2)^3,$$

которая, в отличие от предыдущей, абсолютно неприводима.

В приведенных примерах обе формы имеют четную степень. Для форм нечетной степени положение иное. Именно, Берч показал, что для нечетного r существует такое натуральное $N(r)$, что всякая рациональная форма степени r, число переменных которой больше $N(r)$, представляет нуль в поле рациональных чисел (см. [61]; как и в случае теоремы Брауэра, оценка сверху для $N(r)$, получающаяся из доказательства Берча, заведомо чрезмерно завышена). Ввиду неравенства (14) § 6 для $N(r)$ имеем следующую оценку снизу: $N(r) \geqslant r^2$.

К настоящему времени нет никаких данных, которые подвергали бы сомнению равенство $N(r) = r^2$ (все имеющиеся примеры неравенства $N_p(r) > r^2$ в полях p-адических чисел относятся к случаю форм четной степени). В применении к случаю $r = 3$ (случай $r = 1$ тривиален) это предположение означает, что всякая кубическая форма от 10 и более переменных представляет нуль в поле рациональных чисел (гипотеза Артина). Идеальный результат в этом направлении получен в работе [79]. В ней доказано, что всякая неособенная рациональная кубическая форма от десяти переменных рационально представляет нуль (неособенность формы $F(x_1, \ldots, x_n)$ означает, что для всех значений переменных $x_1, \ldots, x_n$, не равных одновременно нулю, хотя бы одна частная производная $\frac{\partial F}{\partial x_i}$ отлична от нуля). Остается, однако, неясным, можно ли этот результат распространить на кубические формы, имеющие особенности. Неизвестно также, верно ли аналогичное утверждение для кубических форм над полями алгебраических чисел. Для произвольных кубических форм (с особенностями) наилучший результат принадлежит Давенпорту [70], который доказал, что $N(3) \leqslant 15$. Кубические формы от 16 переменных представляют нуль и в любом поле алгебраических чисел [115]. О формах более высокой нечетной степени почти ничего не известно.

Задачи

1. Доказать следующую теорему Лежандра: если a, b и c — попарно взаимно простые целые рациональные числа, свободные от квадратов и не все одного знака, то неопределенное уравнение

$$ax^2 + by^2 + cz^2 = 0$$

разрешимо в рациональных числах $\neq 0$ тогда и только тогда, когда разрешимы все три сравнения:

$$x^2 \equiv -bc \pmod{a}, \qquad x^2 \equiv -ca \pmod{b}, \qquad x^2 \equiv -ab \pmod{c}.$$

2. Представляют ли нуль в поле рациональных чисел формы $3x^2 + 5y^2 - 7z^2$ и $3x^2 - 5y^2 - 7z^2$?

3. Какие простые рациональные числа представляются формами x^2+y^2, x^2+5y^2, x^2-5y^2?

4. Дать описание всех рациональных чисел, представимых формой $2x^2-5y^2$.

5. Какие рациональные числа представляются формой $2x^2-6y^2+15z^2$?

6. Пусть f — неособенная квадратичная форма над полем рациональных чисел, число переменных которой не равно 4. Доказать, что f представляет все рациональные числа тогда и только тогда, когда она представляет нуль.

7. При каких целых рациональных a форма $x^2+2y^2-az^2$ представляет нуль рационально?

8. Найти все решения уравнения $x^2+y^2-2z^2=0$ в рациональных числах.

9. Какие из форм

$$x^2-2y^2+5z^2, \qquad x^2-y^2+10z^2, \qquad 3x^2-y^2+30z^2$$

эквивалентны между собой в поле рациональных чисел?

10. Пусть форма $ax^2+by^2-z^2$, где целые рациональные a и b свободны от квадратов и $|a|>|b|$, представляет нуль во всех полях p-адических чисел. Доказать, что тогда найдутся такие целые рациональные a_1 и c, что

$$aa_1=c^2-b, \qquad |a_1|<|a|.$$

(Равенство $aa_1+b-c^2=0$ показывает, что форма $aa_1x^2+by^2-z^2$ представляет нуль рационально.)

11. Рассматривая формы вида $ax^2+by^2-z^2$ с целыми и свободными от квадратов a и b, доказать теорему Минковского — Хассе для случая трех переменных индукцией по $m=\max(|a|, |b|)$ (использовать задачу 10 и задачу 3 § 1 Дополнения).

12. Для каждого p (включая $p=\infty$) через W_p обозначим группу классов Витта квадратичных форм над полем $\mathbb{Q}_p$. Доказать, что группа классов Витта квадратичных форм над полем рациональных чисел $\mathbb{Q}$ изоморфна некоторой подгруппе декартова произведения $\prod_p W_p$.

Глава II

ПРЕДСТАВЛЕНИЕ ЧИСЕЛ РАЗЛОЖИМЫМИ ФОРМАМИ

В предшествующей главе мы занимались вопросами о существовании и нахождении рациональных решений неопределенных уравнений. Эта глава посвящена тем же вопросам, но относительно целочисленных решений. Поясним ее содержание простым примером.

Задача заключается в нахождении всех целочисленных решений неопределенного уравнения

$$x^2 - 2y^2 = 7. \tag{1}$$

Ограничимся решениями $x > 0$, $y > 0$ (*остальные получаются изменением знаков*). Уравнение имеет решения (3, 1) и (5, 3). Из этих двух решений можно получить бесконечно много других на основании следующего замечания: если (x, y) — решение уравнения (1), то, как показывает подстановка, $(3x + 4y, 2x + 3y)$ также является решением. Отправляясь от решения $(x_0, y_0) = (3, 1)$, мы получим, таким образом, бесконечную серию решений (x_n, y_n), определенных рекуррентными формулами

$$x_{n+1} = 3x_n + 4y_n, \quad y_{n+1} = 2x_n + 3y_n. \tag{2}$$

Отправляясь от решения $(x_0', y_0') = (5,3)$, мы получим по тем же формулам другую бесконечную серию решений (x_n', y_n'). Можно доказать, что этими двумя сериями исчерпываются все решения уравнения (1) с $x > 0$, $y > 0$.

Это совершенно элементарное решение уравнения (1) основывается на вычислениях и формулах. Мы можем связать его с некоторыми общими понятиями и тем подготовить почву для дальнейших обобщений.

Для этого заметим, что форма $x^2 - 2y^2$ в поле рациональных чисел $\mathbb{Q}$ неприводима, однако в более широком поле $\mathbb{Q}(\sqrt{2})$ она разлагается на линейные множители $(x + y\sqrt{2})(x - y\sqrt{2})$. Если воспользоваться понятием нормы для расширения $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ (см. Дополнение, § 2, п. 2), то уравнение (1) можно будет переписать также в виде

$$N(\xi) = N(x + y\sqrt{2}) = 7. \tag{3}$$

Вопрос свелся, таким образом, к определению в поле $\mathbb{Q}(\sqrt{2})$ тех чисел $\xi = x + y\sqrt{2}$ с целыми рациональными x и y, норма которых равна 7. Если норма числа $\varepsilon = u + v\sqrt{2}$ (u и v целые рацио-

нальные) равна 1, то, в силу мультипликативности нормы, вместе с ξ все числа вида $\xi\varepsilon^n$ также удовлетворяют уравнению (3). Так как $N(3+2\sqrt{2})=1$, то мы можем в качестве ε взять $3+2\sqrt{2}$. Переход от ξ к $\xi\varepsilon$ и дает, как легко проверить, переход от решения (x, y) к решению $(3x+4y, 2x+3y)$. Две бесконечные серии решений, записанные рекуррентными формулами (2), принимают теперь вид

$$x_n + y_n\sqrt{2} = (3+\sqrt{2})(3+2\sqrt{2})^n,$$
$$x_n' + y_n'\sqrt{2} = (5+3\sqrt{2})(3+2\sqrt{2})^n, \qquad n \geqslant 0.$$

Возможность получать из одного решения уравнения (1) бесконечно много других решений основывается, в конечном счете, на существовании чисел $\varepsilon = u + v\sqrt{2}$ с целыми u и v, для которых $N(\varepsilon)=1$. В свою очередь числа такого типа связаны, как мы сейчас покажем, с основными понятиями арифметики алгебраических чисел. Для этого рассмотрим совокупность всех чисел вида $x+y\sqrt{2}$, где x и y — любые целые числа. Эта совокупность чисел образует, как легко видеть, кольцо, которое мы обозначим через $\mathfrak{O}$. При исследовании арифметики этого кольца большую роль играют, естественно, его единицы, т. е. такие числа $\alpha \in \mathfrak{O}$, что и $\alpha^{-1} \in \mathfrak{O}$. Очень легко показать, что число α тогда и только тогда является единицей кольца $\mathfrak{O}$, когда $N(\alpha) = \pm 1$. Это показывает, каков более глубокий смысл чисел $\varepsilon \in \mathfrak{O}$, норма которых равна 1: все они вместе с числами, норма которых равна -1, составляют все единицы кольца $\mathfrak{O}$.

В настоящей главе мы рассмотрим общую теорию, для которой уравнение (1) является одним из простейших примеров. Успех в решении уравнения (1) обусловлен в основном тем обстоятельством, что форма x^2-2y^2, неприводимая в поле рациональных чисел, раскладывается на линейные множители в поле $\mathbb{Q}(\sqrt{2})$, в связи с чем это уравнение допускает запись в виде (3). В нашей общей теории также будут рассматриваться формы, которые в надлежащем расширении поля рациональных чисел раскладываются в произведение линейных форм.

Хотя нашей основной целью является исследование неопределенных уравнений, в которых коэффициенты и значения неизвестных — целые числа, нам удобнее будет рассматривать более общий случай форм с рациональными коэффициентами. Значения же переменных всегда будут предполагаться целыми.

§ 1. Разложимые формы

1. Целочисленная эквивалентность форм.

Определение. *Две формы $F(x_1, \ldots, x_m)$ и $G(y_1, \ldots, y_l)$ одной и той же степени n с рациональными коэффициентами называются целочисленно эквивалентными, если каждая из них*

может быть преобразована в другую линейным преобразованием переменных с целыми рациональными коэффициентами.

Например, формы

$$x^2+7y+z^2-6xy-2xz+6yz \quad \text{и} \quad 2u^2-v^2$$

эквивалентны, так как при линейных преобразованиях

$$\begin{aligned} x &= \quad 3v, \\ y &= u+v, \qquad u=-x+2y+z, \\ z &= -u+v, \qquad v= x-y-z \end{aligned}$$

они переходят друг в друга. Для случая форм, зависящих от одного и того же числа переменных, условие эквивалентности, очевидно, сводится к тому, что одна из форм может быть преобразована в другую при помощи линейного преобразования переменных с унимодулярной матрицей (т. е. с целочисленной квадратной матрицей, определитель которой равен ± 1).

Если формы F и G эквивалентны, то, зная все целочисленные решения уравнения $F=a$, мы можем легко получить также все целочисленные решения уравнения $G=a$, и обратно. Таким образом, при рассмотрении вопроса о целочисленных решениях уравнения вида $F=a$ вместо формы F можно взять любую эквивалентную ей форму.

Лемма 1. *Всякая форма степени n эквивалентна форме, у которой n-я степень одной из переменных входит с отличным от нуля коэффициентом.*

Доказательство. Пусть $F(x_1, \ldots, x_m)$ — форма степени n. Покажем, что существуют такие целые рациональные числа $a_2, \ldots, a_m$, что $F(1, a_2, \ldots, a_m) \neq 0$.

Докажем это утверждение индукцией по m. При $m=1$ форма F имеет вид Ax_1^n, где $A \neq 0$, поэтому $F(1) \neq 0$. Предположим, что для форм от $m-1$ переменных ($m \geqslant 2$) наше утверждение уже доказано. Представим заданную форму F в виде

$$F = G_0 x_m^n + G_1 x_m^{n-1} + \ldots + G_n,$$

где G_k ($0 \leqslant k \leqslant n$) либо равно нулю, либо является формой k-й степени от переменных $x_1, \ldots, x_{m-1}$ (мы считаем, что формы нулевой степени — это отличные от нуля константы). Все G_k не могут быть равны нулю, так как F, являясь формой n-й степени, имеет хоть один отличный от нуля коэффициент. По индуктивному предположению хотя бы при одном k существуют такие целые числа $a_2, \ldots, a_{m-1}$, что $G_k(1, a_2, \ldots, a_{m-1}) \neq 0$. Так как многочлен $F(1, a_2, \ldots, a_{m-1}, x_m)$ от одной переменной x_m не равен тождественно нулю, то, взяв в качестве a_m любое целое число, отличное от его корней, будем иметь $F(1, a_2, \ldots, a_m) \neq 0$.

Сделаем теперь следующее линейное преобразование переменных:

$$x_1 = y_1,$$
$$x_2 = a_2y_1 + y_2,$$
$$\ldots\ldots\ldots$$
$$x_m = a_my_1 + y_m.$$

При этом преобразовании форма F перейдет в форму

$$G(y_1, \ldots, y_m) = F(y_1, a_2y_1 + y_2, \ldots, a_my_1 + y_m).$$

Так как матрица нашего преобразования целочисленна и ее определитель равен 1, то формы F и G эквивалентны, причем коэффициент при y_1^n, равный $G(1, 0, \ldots, 0) = F(1, a_2, \ldots, a_m)$, отличен от нуля. Лемма 1 доказана.

2. Построение разложимых форм.

Определение. *Форма $F(x_1, \ldots, x_m)$ с коэффициентами из поля рациональных чисел $\mathbb{Q}$ называется разложимой, если она в некотором расширении $\Omega/\mathbb{Q}$ раскладывается на линейные множители.*

Примером разложимой формы является форма

$$F(x, y) = a_0x^n + a_1x^{n-1}y + \ldots + a_ny^n$$

от двух переменных ($a_0 \neq 0$). Действительно, если Ω — поле разложения многочлена $F(x, 1)$ и $\alpha_1, \ldots, \alpha_n$ — его корни, то в Ω имеем разложение

$$F(x, y) = a_0(x - \alpha_1y)\ldots(x - \alpha_ny).$$

Среди неособенных квадратичных форм, рассматривавшихся в первой главе, разложимыми являются лишь формы от одной и двух переменных (задача 1).

Очевидно, что вместе с формой F все эквивалентные ей формы также разложимы.

В определении разложимой формы ничего не говорится о том, каким может быть поле Ω, в котором форма разлагается на линейные множители. Мы покажем сейчас, что в качестве Ω всегда можно взять некоторое конечное расширение поля рациональных чисел $\mathbb{Q}$. В связи с этим основным алгебраическим аппаратом, которым мы будем в дальнейшем пользоваться, является теория конечных расширений полей. Необходимые нам свойства конечных расширений изложены в § 2 Дополнения.

Определение. *Конечные расширения поля рациональных чисел называются полями алгебраических чисел, а их элементы — алгебраическими числами.*

Теорема 1. *Всякая рациональная разложимая форма раскладывается на линейные множители уже в некотором поле алгебраических чисел.*

Доказательство. В силу леммы 1 мы можем ограничиться рассмотрением разложимой формы

$$F = (\alpha_{11}x_1 + \ldots + \alpha_{1m}x_m)\ldots(\alpha_{n1}x_1 + \ldots + \alpha_{nm}x_m), \quad \alpha_{ij} \in \Omega,$$

у которой коэффициент при x_1^n отличен от нуля. Так как в этом случае коэффициенты α_{i1} $(1 \leqslant i \leqslant n)$ отличны от нуля, то нашу форму можно представить в виде

$$F = A(x_1 + \beta_{12}x_2 + \ldots + \beta_{1m}x_m)\ldots(x_1 + \beta_{n2}x_2 + \ldots + \beta_{nm}x_m), \quad (1)$$

где $A = \alpha_{11}\ldots\alpha_{n1}$ и $\beta_{ij} = \alpha_{ij}\alpha_{i1}^{-1}$. Число A, являясь коэффициентом при x_1^n, рационально. Для фиксированного j $(2 \leqslant j \leqslant m)$ положим в последнем разложении $x_j = 1$, а всем остальным переменным, кроме x_1, придадим нулевое значение. Мы получим

$$F(x_1, 0, \ldots, 1, \ldots, 0) = A(x_1 + \beta_{1j})\ldots(x_1 + \beta_{nj}).$$

Так как слева у нас стоит многочлен (степени n) с рациональными коэффициентами, то отсюда следует, что β_{ij} — алгебраические числа. Обозначим через L подполе поля Ω, получающееся из $\mathbb{Q}$ присоединением всех β_{ij}. Расширение $L/\mathbb{Q}$, очевидно, конечно (см. Дополнение, § 2, п. 1), т. е. L есть поле алгебраических чисел.

Дальше мы ограничимся рассмотрением лишь неприводимых в поле рациональных чисел разложимых форм, так как именно для них вопрос о целочисленных представлениях рациональных чисел наиболее интересен. Укажем способ построения неприводимых разложимых форм.

Рассмотрим произвольное поле алгебраических чисел K степени n и какой-нибудь примитивный элемент θ поля K над $\mathbb{Q}$, так что $K = \mathbb{Q}(\theta)$ (см. Дополнение, § 2, п. 3). Минимальный многочлен $\varphi(t)$ числа θ над полем $\mathbb{Q}$ имеет степень n. Построим над K расширение L, в котором $\varphi(t)$ раскладывается целиком на линейные множители:

$$\varphi(t) = (t - \theta^{(1)})\ldots(t - \theta^{(n)}), \quad \theta^{(1)} = \theta$$

(можно считать, что $L = \mathbb{Q}(\theta^{(1)}, \ldots, \theta^{(n)})$). Для всякого числа $\alpha = f(\theta) \in K$ ($f(t)$ — многочлен с рациональными коэффициентами) положим $\alpha^{(i)} = f(\theta^{(i)}) \in \mathbb{Q}(\theta^{(i)}) \subset L$. Тогда для нормы $N(\alpha) = N_{K/\mathbb{Q}}(\alpha)$ будет справедлива формула

$$N(\alpha) = \alpha^{(1)}\alpha^{(2)}\ldots\alpha^{(n)}$$

(см. Дополнение, § 2, п. 3).

Пусть теперь $\mu_1, \ldots, \mu_m$ — произвольная система отличных от нуля чисел поля K. Эти числа определяют форму

$$F(x_1, \ldots, x_m) = \prod_{i=1}^{n}(x_1\mu_1^{(i)} + \ldots + x_m\mu_m^{(i)}). \quad (2)$$

Так как $\mu_k^{(i)} = f_k(\theta^{(i)})$ $(1 \leqslant k \leqslant m$, $f_k(t)$ — многочлены с рациональными коэффициентами), то коэффициенты формы (2) являются симметрическими функциями от $\theta^{(1)}, \ldots, \theta^{(n)}$, а значит, они рационально выражаются через коэффициенты многочлена $\varphi(t)$. Этим доказано, что форма (2) имеет рациональные коэффициенты. Если вместо переменных $x_1, \ldots, x_m$ мы подставим произвольные рациональные числа, то, поскольку

$$x_1\mu_1^{(i)} + \ldots + x_m\mu_m^{(i)} = (x_1\mu_1 + \ldots + x_m\mu_m)^{(i)},$$

произведение (2) будет нормой числа $x_1\mu_1 + \ldots + x_m\mu_m$ (относительно расширения $K/\mathbb{Q}$) В силу этого мы можем форму (2) условно записать в виде

$$F(x_1, \ldots, x_m) = N(x_1\mu_1 + \ldots + x_m\mu_m). \tag{3}$$

Форма вида (2) не всегда неприводима. Например, если в поле $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ мы возьмем $\mu_1 = \sqrt{2}$, $\mu_2 = \sqrt{3}$, то соответствующая форма будет равна $(2x_1^2 - 3x_2^2)^2$. Однако имеет место следующая теорема.

Теорема 2. *Если числа* $\mu_2, \ldots, \mu_m$ *порождают поле* K, *т. е.* $K = \mathbb{Q}(\mu_2, \ldots, \mu_m)$, *то форма*

$$F(x_1, \ldots, x_m) = N(x_1 + x_2\mu_2 + \ldots + x_m\mu_m) \tag{4}$$

неприводима (над полем рациональных чисел). Обратно, всякая неприводимая разложимая форма эквивалентна с точностью до постоянного множителя форме вида (4).

Доказательство. Допустим, что $F = GH$, где множители G и H имеют рациональные коэффициенты. Так как в кольце многочленов от m переменных разложение на неприводимые множители однозначно (с точностью до постоянных множителей), то каждая из линейных форм

$$L_i = x_1 + x_2\mu_2^{(i)} + \ldots + x_m\mu_m^{(i)}$$

должна быть делителем либо G, либо H. Пусть $L_1 = x_1 + x_2\mu_2 + \ldots + x_m\mu_m$ есть делитель G, т. е.

$$G = L_1M_1.$$

Заменим в последнем равенстве все коэффициенты их образами при изоморфизме $\alpha \to \alpha^{(i)}$ поля $K = \mathbb{Q}(\theta)$ на поле $\mathbb{Q}(\theta^{(i)})$. Так как коэффициенты формы G рациональны, то при такой замене она не изменится и мы получим равенство

$$G = L_iM_i,$$

означающее, что G делится на L_i при любом $i = 1, \ldots, n$ $(n = (K:\mathbb{Q}))$. Заметим теперь, что изоморфизм $\alpha \to \alpha^{(i)}$, $\alpha \in \mathbb{Q}(\mu_2, \ldots, \mu_m)$, вполне определен заданием образов $\mu_2^{(i)}, \ldots, \mu_m^{(i)}$ чисел $\mu_2, \ldots, \mu_m$. Отсюда следует, что наборы чисел

$\mu_2^{(i)}, \ldots, \mu_m^{(i)}$ $(1 \leqslant i \leqslant n)$ попарно различны (ибо изоморфизмы $\alpha \to \alpha^{(i)}$ попарно различны), а значит, и формы $L_1, \ldots, L_n$ попарно различны. Коэффициент при x_1 у всех форм L_i равен 1, поэтому эти формы также попарно непропорциональны. Воспользовавшись опять однозначностью разложения, заключаем, что G делится на произведение $L_1 \ldots L_n$, т. е. делится на F. Множитель H, следовательно, является константой, и первое утверждение теоремы доказано.

Докажем второе утверждение. Пусть $F^*(x_1, \ldots, x_m)$ — произвольная неприводимая разложимая форма степени n. В силу леммы 1 можно считать, что коэффициент при x_1^n отличен от нуля, а тогда для F^* будем иметь разложение вида (1), где β_{ij} — некоторые алгебраические числа. Положим $\beta_{1j} = \mu_j$ $(2 \leqslant j \leqslant m)$ и рассмотрим поле $K = \mathbb{Q}(\mu_2, \ldots, \mu_m)$, степень которого обозначим через r. По доказанному форма

$$F = N(x_1 + x_2\mu_2 + \ldots + x_m\mu_m)$$

неприводима, причем один из ее линейных множителей, $L_1 = x_1 + x_2\mu_2 + \ldots + x_m\mu_m$, является делителем и формы F^*. Подвергая все коэффициенты равенства $F^* = L_1M_1$ действию изоморфизма $\alpha \to \alpha^{(i)}$ $(\alpha \in K,\ 1 \leqslant i \leqslant r)$, мы получим разложение $F^* = L_iM_i$. Формы $L_1, \ldots, L_r$, как мы видели, попарно не пропорциональны, поэтому F^* делится на их произведение $L_1 \ldots L_r$, совпадающее с F. В силу неприводимости F^* отсюда следует, что $F^* = AF$, где A — константа, и теорема 2 доказана полностью. (В процессе доказательства получено также, что $r = n$.)

3. Модули. Ясно, что для формы (3) вопрос о целочисленных решениях неопределенного уравнения $F(x_1, \ldots, x_m) = a$ сводится к разысканию в поле K чисел ξ, которые представимы в виде

$$\xi = x_1\mu_1 + \ldots + x_m\mu_m \tag{5}$$

с целыми рациональными $x_1, \ldots, x_m$ и для которых $N(\xi) = a$. В силу этого естественно обратиться к изучению совокупностей чисел вида (5).

Определение. *Пусть K — поле алгебраических чисел и $\mu_1, \ldots, \mu_m$ — произвольная конечная система чисел из K. Совокупность M всех линейных комбинаций $c_1\mu_1 + \ldots + c_m\mu_m$ с целыми рациональными коэффициентами c_i $(1 \leqslant i \leqslant m)$ называется модулем в поле K. Сами числа $\mu_1, \ldots, \mu_m$ называются при этом образующими модуля M.*

Конечно, один и тот же модуль M может быть задан различными системами образующих. Если $\mu_1, \ldots, \mu_m$ — система образующих модуля M, то будем писать $M = \{\mu_1, \ldots, \mu_m\}$.

Посмотрим, как изменится форма (3), если вместо $\mu_1, \ldots, \mu_m$ взять другую систему чисел $\rho_1, \ldots, \rho_l$, определяющих тот же

модуль M. Мы имеем

$$\rho_j = \sum_{k=1}^{m} c_{jk}\mu_k, \qquad 1 \leqslant j \leqslant l,$$

с целыми рациональными c_{jk}. Пусть

$$G(y_1, \ldots, y_l) = N(y_1\rho_1 + \ldots + y_l\rho_l).$$

Так как $\sum_{j=1}^{l} y_j\rho_j = \sum_{k=1}^{m} \left(\sum_{j=1}^{l} c_{jk}y_j\right)\mu_k$, то при линейном преобразовании

$$x_k = \sum_{j=1}^{l} c_{jk}y_j, \qquad 1 \leqslant k \leqslant m,$$

форма F переходит в G. Поскольку системы образующих μ_k и ρ_j модуля M играют симметричную роль, то аналогично существует целочисленное линейное преобразование переменных, переводящее G в F. Этим доказано, что разным системам образующих модуля M соответствуют эквивалентные формы, т. е. с каждым модулем M в поле K однозначно связывается некоторый класс эквивалентных разложимых форм.

Для всякого модуля $M = \{\mu_1, \ldots, \mu_m\}$ и числа $\alpha \in K$ через αM будем обозначать совокупность всех произведений $\alpha\xi$, где ξ пробегает все элементы из M. Очевидно, что αM совпадает с совокупностью всех целочисленных линейных комбинаций чисел $\alpha\mu_1, \ldots, \alpha\mu_m$, т. е. $\alpha M = \{\alpha\mu_1, \ldots, \alpha\mu_m\}$.

Определение. *Два модуля M и M_1 в поле алгебраических чисел K называются подобными, если $M_1 = \alpha M$ при некотором $\alpha \neq 0$ из K.*

Формы, связанные с подобными модулями M и αM, различаются между собой лишь постоянным множителем, равным $N(\alpha)$. Поэтому, рассматривая формы с точностью до постоянного множителя, мы всегда можем вместо модуля M взять любой подобный ему модуль, в силу чего можно считать, что одна из образующих модуля, скажем μ_1, равна 1.

Изложенное выше позволяет дать задаче о представлении чисел неприводимыми разложимыми формами следующую формулировку. Если форма F представлена в виде

$$F(x_1, \ldots, x_m) = AN(x_1\mu_1 + \ldots + x_m\mu_m)$$

(при надлежащем выборе поля K), то решение в целых числах неопределенного уравнения $F(x_1, \ldots, x_m) = a$ равносильно нахождению в модуле $M = \{\mu_1, \ldots, \mu_m\}$ всех чисел α, норма которых $N(\alpha)$ равна рациональному числу a/A. Ввиду этого в дальнейшем мы будем заниматься именно этой задачей нахождения в данном модуле чисел с заданной нормой. Как мы уже видели, последняя задача равносильна также задаче о нахождении в подобном

модуле μM чисел с нормой $N(\mu)a/A$. В силу этого вместо заданного модуля можно рассматривать, если это будет целесообразно, любой подобный ему модуль.

Если степень поля алгебраических чисел K равна n, то во всяком модуле M поля K содержится не более n линейно независимых чисел (над полем $\mathbb{Q}$).

Определение. *Если модуль M в поле алгебраических чисел K степени n содержит n линейно независимых чисел (над полем рациональных чисел), то он называется полным, в противном случае — неполным. Связанные с модулем M формы также называются соответственно полными или неполными.*

Например, если целое рациональное число d не является кубом, то числа $1, \sqrt[3]{d}, \sqrt[3]{d^2}$ образуют базис поля $\mathbb{Q}(\sqrt[3]{d})$ над $\mathbb{Q}$, поэтому форма

$$N(x + y\sqrt[3]{d} + z\sqrt[3]{d^2}) = x^3 + dy^3 + d^2z^3 - 3dxyz$$

полная. Примером неполной формы может служить форма

$$N(x + y\sqrt[3]{d}) = x^3 + dy^3.$$

Если $\{1, \mu_2, \ldots, \mu_m\}$ — полный модуль поля K, то, очевидно, $K = \mathbb{Q}(\mu_2, \ldots, \mu_m)$. В силу теоремы 2 отсюда легко следует, что всякая полная форма всегда неприводима.

Вопрос о представлении чисел неполными неприводимыми формами весьма сложен, и к настоящему времени сколько-нибудь удовлетворительной общей теории на этот счет нет. Частный случай мы рассмотрим в гл. IV.

Что касается задачи о представлении рациональных чисел полными формами, то она намного проще и решена до конца. Ею мы и будем заниматься в настоящей главе. Эта задача, как уже было отмечено, равносильна вопросу о нахождении в фиксированном полном модуле поля алгебраических чисел K всех чисел с заданной нормой.

Задачи

1. Показать, что рациональная квадратичная форма разложима тогда и только тогда, когда ее ранг $\leqslant 2$.
2. Доказать, что форма, связанная с произвольным модулем поля алгебраических чисел K, является степенью неприводимой формы.
3. Доказать, что в поле рациональных чисел $\mathbb{Q}$ всякий модуль имеет вид $a\mathbb{Z}$, где $a \in \mathbb{Q}$ ($\mathbb{Z}$ — кольцо целых рациональных чисел).

§ 2. Полные модули и их кольца множителей

1. Базис модуля.

Определение. *Система образующих $\alpha_1, \ldots, \alpha_m$ модуля M называется его базисом, если она линейно независима над*

кольцом целых чисел, т. е. если равенство

$$a_1\alpha_1 + \ldots + a_m\alpha_m = 0, \quad a_i \in \mathbb{Z},$$

имеет место только при нулевых коэффициентах a_i.

Очевидно, что если $\alpha_1, \ldots, \alpha_m$ — базис модуля M, то любое число $\alpha \in M$ допускает одно и только одно представление в виде

$$\alpha = c_1\alpha_1 + \ldots + c_m\alpha_m, \quad c_i \in \mathbb{Z}. \tag{1}$$

Мы докажем сейчас, что любой модуль имеет базис. Доказательство не использует на самом деле того, что модуль состоит из чисел некоторого поля алгебраических чисел. Существенным является только то, что относительно операций сложения модуль образует абелеву группу, в которой нет элементов конечного порядка и в которой все элементы линейно выражаются с целыми коэффициентами через некоторую конечную систему элементов (существование системы образующих модуля). Поэтому мы и докажем нужный нам результат как теорему об абелевых группах. При этом мы будем пользоваться следующей терминологией. Систему элементов $\alpha_1, \ldots, \alpha_m$ абелевой группы M (действие в которой будет записываться аддитивно) назовем системой образующих, если любой элемент $\alpha \in M$ представим в виде (1). Мы пишем в этом случае: $M = \{\alpha_1, \ldots, \alpha_m\}$. Если же система $\alpha_1, \ldots, \alpha_m$ удовлетворяет данному выше определению, то будем ее называть базисом группы M.

Теорема 1. *Если абелева группа без элементов конечного порядка обладает конечной системой образующих, то она обладает и базисом.*

Доказательство. Обозначим через $\alpha_1, \ldots, \alpha_s$ произвольную систему образующих группы M. Заметим прежде всего, что если мы к одной образующей прибавим другую, умноженную на произвольное целое число, то новая система элементов будет также системой образующих. Пусть, например, $\alpha_1' = \alpha_1 + k\alpha_2$. Тогда для любого $\alpha \in M$ имеем

$$\alpha = c_1\alpha_1 + c_2\alpha_2 + \ldots + c_s\alpha_s = c_1\alpha_1' + (c_2 - kc_1)\alpha_2 + \ldots + c_s\alpha_s,$$

где все коэффициенты целые, а значит, $M = \{\alpha_1', \alpha_2, \ldots, \alpha_s\}$.

Если элементы $\alpha_1, \ldots, \alpha_s$ линейно независимы, то они образуют базис M. Допустим, что они линейно зависимы, т. е. что

$$c_1\alpha_1 + c_2\alpha_2 + \ldots + c_s\alpha_s = 0 \tag{2}$$

при некоторых не равных одновременно нулю целых c_i. Выберем среди отличных от нуля коэффициентов c_i наименьший по абсолютной величине. Пусть это будет, например, c_1. Предположим, что не все коэффициенты c_i делятся на c_1, скажем, $c_2 = c_1q + c'$, где $0 < c' < |c_1|$. Если мы перейдем к новой системе образующих

$\alpha_1' = \alpha_1 + q\alpha_2, \alpha_2, \ldots, \alpha_s$, то соотношение (2) примет вид

$$c_1\alpha_1' + c'\alpha_2 + \ldots + c_s\alpha_s = 0,$$

и в этом соотношении мы имеем коэффициент $c' > 0$, который меньше, чем $|c_1|$. Итак, если для образующих $\alpha_1, \ldots, \alpha_s$ мы имеем нетривиальное соотношение (2), в котором наименьший по абсолютной величине и отличный от нуля коэффициент не является делителем остальных коэффициентов, то мы можем построить другую систему образующих, для которой также имеется нетривиальная зависимость с целыми коэффициентами, причем наименьший по абсолютной величине и не равный нулю коэффициент этой новой зависимости меньше (по абсолютной величине), чем аналогичный коэффициент в первой зависимости. В результате конечного числа таких преобразований мы придем наконец к новой системе образующих $\beta_1, \ldots, \beta_s$, для которой имеется зависимость

$$k_1\beta_1 + k_2\beta_2 + \ldots + k_s\beta_s = 0 \tag{3}$$

с целыми коэффициентами k_i, причем один из коэффициентов, например k_1, является делителем всех остальных. Сократив соотношение (3) на k_1 (это можно сделать, так как по предположению в M нет элементов конечного порядка, отличных от нуля), получим

$$\beta_1 + l_2\beta_2 + \ldots + l_s\beta_s = 0 \tag{4}$$

с целыми $l_2, \ldots, l_s$. Из (4) следует, что β_1 можно исключить из построенной системы образующих, т. е. что $M = \{\beta_2, \ldots, \beta_s\}$.

Нами доказано, что если некоторая система образующих M линейно зависима, то можно построить новую систему образующих, число элементов которой на единицу меньше. Повторив это рассуждение несколько раз, мы получим в конце концов линейно независимую систему образующих, которая и будет базисом группы M.

Следствие. *Для всякого модуля в поле алгебраических чисел K существует базис.*

Число элементов m, входящих в какой-нибудь базис модуля M, равно, очевидно, максимальному числу линейно независимых (над $\mathbb{Q}$) элементов из M. Следовательно, это число m для всех базисов одно и то же. Оно называется рангом модуля M. Ранг модуля, состоящего из одного нуля, считается равным нулю.

Пусть $\omega_1, \ldots, \omega_m$ и $\omega_1', \ldots, \omega_m'$ — два базиса модуля M ранга m. Ясно, что матрица перехода C от первого базиса ко второму целочисленна. В силу симметрии матрица перехода от второго базиса к первому, т. е. матрица C^{-1}, также целочисленна. Следовательно, $\det C = \pm 1$. Мы получаем, таким образом, что матрица перехода от одного базиса модуля ранга m к его другому базису является унимодулярной матрицей порядка m.

Если степень поля K над $\mathbf{Q}$ равна n, то ранг всякого модуля в K не превосходит n. Очевидно, что ранг модуля равен n тогда и только тогда, когда этот модуль полный. Неполные модули характеризуются, следовательно, тем, что их ранг меньше степени поля n.

Любая система образующих модуля ранга m содержит не менее m элементов. Отсюда следует, что среди форм, связанных с этим модулем, существуют формы от m переменных и не существует форм с меньшим числом переменных. Полные формы степени n могут быть определены, следовательно, как такие разложимые неприводимые формы, которые не эквивалентны формам с числом переменных, меньшим степени n.

Теорема 2. *В абелевой группе M без элементов конечного порядка и с конечным числом образующих всякая подгруппа N также имеет конечное число образующих и, следовательно, обладает базисом. При этом для любого базиса $\omega_1, \ldots, \omega_m$ группы M (при надлежащей нумерации его элементов) для N существует базис вида*

$$\begin{aligned}
\eta_1 &= c_{11}\omega_1 + c_{12}\omega_2 + \ldots + c_{1k}\omega_k + \ldots + c_{1m}\omega_m,\\
\eta_2 &= \qquad c_{22}\omega_2 + \ldots + c_{2k}\omega_k + \ldots + c_{2m}\omega_m,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\eta_k &= \qquad\qquad\qquad c_{kk}\omega_k + \ldots + c_{km}\omega_m,
\end{aligned}$$

где c_{ij} целые, $c_{ii} > 0$, $k \leqslant m$.

Доказательство. Докажем теорему индукцией по рангу m группы M, т. е. по числу элементов, входящих в ее базис. Для случая $m = 0$ утверждение теоремы тривиально. Пусть $m \geqslant 1$. Если N состоит только из нуля, то $k = 0$, и теорема справедлива. Если же $\alpha \in N$, $\alpha \neq 0$, то

$$\alpha = c_1\omega_1 + \ldots + c_m\omega_m, \tag{5}$$

где хоть один из коэффициентов c_i не равен нулю. Изменив в случае надобности нумерацию элементов базиса, мы можем считать, что $c_1 \neq 0$. Если $c_1 < 0$, то для $-\alpha$ коэффициент при ω_1 будет положителен. Среди элементов подгруппы N выберем элемент

$$\eta_1 = c_{11}\omega_1 + c_{12}\omega_2 + \ldots + c_{1m}\omega_m,$$

у которого коэффициент $c_{11} > 0$ при ω_1 наименьший. Тогда для любого $\alpha \in N$ коэффициент c_1 будет делиться на c_{11}. Действительно, если $c_1 = c_{11}q + c'$, $0 \leqslant c' < c_{11}$ (q целое), то для элемента $\alpha - q\eta_1$ имеем

$$\alpha - q\eta_1 = c'\omega_1 + c_2'\omega_2 + \ldots + c_m'\omega_m,$$

откуда в силу минимальности c_{11} следует, что $c' = 0$. Рассмотрим теперь в M подгруппу $M_0 = \{\omega_2, \ldots, \omega_m\}$. Так как пересечение $N \cap M_0$ является подгруппой группы M_0, то по индуктивному

предположению в $N \cap M_0$ существует базис вида

$$\begin{aligned}
\eta_2 &= c_{22}\omega_2 + c_{23}\omega_3 + \ldots + c_{2k}\omega_k + \ldots + c_{2m}\omega_m,\\
\eta_3 &= \qquad c_{33}\omega_3 + \ldots + c_{3k}\omega_k + \ldots + c_{3m}\omega_m,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\eta_k &= \qquad\qquad\qquad c_{kk}\omega_k + \ldots + c_{km}\omega_m,
\end{aligned}$$

где c_{ij} целые, $c_{ii} > 0$, $k - 1 \leqslant m - 1$ (при надлежащей нумерации элементов базиса $\omega_2, \ldots, \omega_m$). Утверждаем, что N совпадает с совокупностью всех целочисленных линейных комбинаций элементов $\eta_1, \eta_2, \ldots, \eta_k$. Пусть α — произвольный элемент из N. Если его представить в виде (5), то по доказанному $c_1 = c_{11}q_1$ с целым q_1, а тогда

$$\alpha - q_1\eta_1 = c_2'\omega_2 + \ldots + c_m'\omega_m$$

принадлежит пересечению $M_0 \cap N$. По индуктивному предположению имеем

$$\alpha - q_1\eta_1 = q_2\eta_2 + \ldots + q_k\eta_k$$

с целыми q_i, откуда $\alpha = q_1\eta_1 + \ldots + q_k\eta_k$. Этим и доказано, что $N = \{\eta_1, \eta_2, \ldots, \eta_k\}$. Образующие $\eta_1, \ldots, \eta_k$, как легко видеть, линейно независимы над $\mathbb{Z}$, а значит, они образуют базис N требуемого вида.

Проведенное доказательство теоремы 2 воспроизводит, по существу, метод Гаусса исключения неизвестных в системах линейных уравнений. Различия вызваны тем, что в нашем случае коэффициенты принадлежат не полю, а кольцу целых чисел.

Следствие. *Всякая подгруппа N модуля M в поле алгебраических чисел K является также модулем (подмодулем модуля M).*

2. Кольца множителей.

Определение. *Число α поля алгебраических чисел K называется множителем полного модуля M поля K, если $\alpha M \subset M$, т. е. если для любого $\xi \in M$ произведение $\alpha\xi$ также принадлежит M.*

Совокупность $\mathfrak{O}_M$ всех множителей модуля M является кольцом. В самом деле, если α и β принадлежат $\mathfrak{O}_M$, то при любом $\xi \in M$ имеем: $(\alpha - \beta)\xi = \alpha\xi - \beta\xi \in M$ и $(\alpha\beta)\xi = \alpha(\beta\xi) \in M$, т. е. $\alpha - \beta \in \mathfrak{O}_M$ и $\alpha\beta \in \mathfrak{O}_M$. Кольцо $\mathfrak{O}_M$ называется кольцом множителей полного модуля M. Так как $1 \in \mathfrak{O}_M$, то $\mathfrak{O}_M$ есть кольцо с единицей.

Чтобы удостовериться в том, что данное число $\alpha \in K$ принадлежит кольцу $\mathfrak{O}_M$, нет необходимости проверять для всех $\xi \in M$, будет ли произведение $\alpha\xi$ принадлежать M. Достаточно проверить это лишь для чисел какого-нибудь базиса $\mu_1, \ldots, \mu_n$ модуля M. В самом деле, если $\alpha\mu_i \in M$ для всех $i = 1, \ldots, n$, то и

для любого $\xi = c_1\mu_1 + \ldots + c_n\mu_n \in M$ будем иметь

$$\alpha\xi = c_1(\alpha\mu_1) + \ldots + c_n(\alpha\mu_n) \in M.$$

Докажем, что кольцо множителей $\mathfrak{O}_M$ есть полный модуль в K. Пусть γ — произвольное отличное от нуля число из M. Так как $\alpha\gamma \in M$ при любом $\alpha \in \mathfrak{O}_M$, то $\gamma\mathfrak{O}_M \subset M$. Множество чисел $\gamma\mathfrak{O}_M$ является, очевидно, группой относительно действия сложения, поэтому, согласно следствию теоремы 2, $\gamma\mathfrak{O}_M$ есть модуль. Но тогда $\mathfrak{O}_M = \gamma^{-1}(\gamma\mathfrak{O}_M)$ также является модулем. Остается доказать, что этот модуль полный. Возьмем произвольное отличное от нуля число α из K и обозначим через c общий знаменатель всех рациональных чисел a_{ij}, определенных разложениями

$$\alpha\mu_i = \sum_{j=1}^{n} a_{ij}\mu_j, \qquad 1 \leqslant i \leqslant n. \tag{6}$$

Так как произведения ca_{ij} целые, то $c\alpha\mu_i \in M$, а значит, $c\alpha \in \mathfrak{O}_M$. Если теперь мы возьмем произвольный базис $\alpha_1, \ldots, \alpha_n$ поля K, то по только что доказанному при некоторых целых рациональных $c_1, \ldots, c_n$ произведения $c_1\alpha_1, \ldots, c_n\alpha_n$ будут содержаться в $\mathfrak{O}_M$. Мы видим, таким образом, что в $\mathfrak{O}_M$ имеется n линейно независимых чисел, а это и означает, что $\mathfrak{O}_M$ — полный модуль.

Определение. *Полный модуль в поле алгебраических чисел K, содержащий число 1 и являющийся кольцом, называется порядком поля K.*

Принимая это определение, мы можем полученный нами результат сформулировать следующим образом.

Теорема 3. *Кольцо множителей для произвольного полного модуля поля алгебраических чисел K является порядком этого поля.*

Справедливо и обратное утверждение: всякий порядок $\mathfrak{O}$ поля K является кольцом множителей для некоторого полного модуля, например для самого себя (так как $1 \in \mathfrak{O}$, то включение $\alpha\mathfrak{O} \subset \mathfrak{O}$ равносильно условию $\alpha \in \mathfrak{O}$).

Для произвольного числа $\gamma \neq 0$ из K условие $\alpha\xi \in M$ равносильно условию $\alpha(\gamma\xi) \in \gamma M$ (здесь $\xi \in M$). Отсюда следует, что подобные модули M и γM имеют одно и то же кольцо множителей, т. е. $\mathfrak{O}_{\gamma M} = \mathfrak{O}_M$.

Пусть $\mu_1, \ldots, \mu_n$ — базис модуля M, а $\omega_1, \ldots, \omega_n$ — базис его кольца множителей $\mathfrak{O}_M$. Для каждого $i = 1, \ldots, n$ имеем

$$\mu_i = \sum_{j=1}^{n} b_{ij}\omega_j,$$

где b_{ij} — рациональные числа. Если b — общий знаменатель всех коэффициентов b_{ij}, то числа $b\mu_i$ будут выражаться через базис порядка $\mathfrak{O}_M$ уже с целыми коэффициентами, т. е. будут принад-

лежать $\mathfrak{O}_M$. Для Модуля bM имеем, следовательно, включение $bB \subset \mathfrak{O}_M$.

Сформулируем полученные результаты.

Лемма 1. *Кольца множителей подобных полных модулей совпадают. Для каждого полного модуля существует подобный ему модуль, содержащийся в своем кольце множителей.*

Замечание. Рассмотрение полного модуля M вместе с его кольцом множителей $\mathfrak{O}_M$ может быть охвачено общим понятием модуля над кольцом. Для аддитивной подгруппы A поля K часто приходится рассматривать подкольца Λ поля K, для которых A является Λ-модулем (произведение λx элементов $\lambda \in \Lambda$ и $x \in A$ здесь определено умножением в K). Кольцо множителей $\mathfrak{O}_M$ для полного модуля M в поле алгебраических чисел K — это наибольшее из подколец Λ поля K, относительно которых M является Λ-модулем. С точки зрения абстрактной теории колец рассматриваемые нами модули M над порядком Λ, содержащимся в $\mathfrak{O}_M$, характеризуются тем, что они конечно порождены, не имеют кручения (если $x \in M$, $x \neq 0$, то из $\lambda x = 0$, $\lambda \in \Lambda$, следует, что $\lambda = 0$) и имеют ранг, равный 1 (под рангом Λ-модуля понимается максимальное число линейно независимых над Λ элементов). При этом два Λ-модуля M и M_1 (содержащиеся в K) Λ-изоморфны тогда и только тогда, когда они подобны. В самом деле, если $M_1 = \gamma M$, то отображение $\xi \to \gamma\xi$ ($\xi \in M$) будет, очевидно, Λ-изоморфизмом M на M_1. Обратно, пусть f — Λ-изоморфизм M на M_1, так что $f(\lambda\xi) = \lambda f(\xi)$, $\xi \in M$, $\lambda \in \Lambda$. Выберем произвольно $\alpha \in M$, $\alpha \neq 0$, и положим $\gamma = f(\alpha)/\alpha$. Если целое рациональное $b \neq 0$ таково, что $bM \subset \Lambda$, то для любого $\xi \in M$ имеем

$$\gamma\xi = \frac{b\xi f(\alpha)}{b\alpha} = \frac{f(b\alpha\xi)}{b\alpha} = f(\xi),$$

а значит, $M_1 = f(M) = \gamma M$.

3. Единицы. Вернемся к нашей задаче о целочисленных представлениях рациональных чисел полными разложимыми формами. В § 1, п. 3 мы видели, что эта задача сводится к разысканию в полном модуле M чисел μ, для которых

$$N(\mu) = a. \tag{7}$$

Для любого ω из кольца множителей $\mathfrak{O} = \mathfrak{O}_M$ произведение $\omega\mu$ принадлежит M, при этом по мультипликативности нормы

$$N(\omega\mu) = N(\omega)a.$$

Если $N(\omega) = 1$, то вместе с μ произведение $\omega\mu$ также будет решением уравнения (7). Таким образом, множители ω, норма которых равна 1, дают возможность из одного решения интересующего нас уравнения (7) получить целый класс новых решений. Это обстоятельство и лежит в основе того метода решения уравнения (7), который мы собираемся изложить.

Докажем, что множитель $\omega \in \mathfrak{O}$ с условием $N(\omega) = 1$ следует искать среди тех чисел ε кольца $\mathfrak{O}$, для которых ε^{-1} также принадлежит $\mathfrak{O}$. В соответствии с определением п. 1 § 4 Дополнения такие числа ε называются единицами кольца $\mathfrak{O}$. Так как включения $\varepsilon M \subset M$ и $\varepsilon^{-1} M \subset M$ эквивалентны равенству $\varepsilon M = M$, то единицы кольца $\mathfrak{O} = \mathfrak{O}_M$ могут быть охарактеризованы также как такие числа $\alpha \in K$, для которых $\alpha M = M$.

Лемма 2. *Если число α принадлежит порядку $\mathfrak{O}$, то его характеристический и минимальный многочлены имеют целые коэффициенты. В частности, норма $N(\alpha) = N_{K/\mathbb{Q}}(\alpha)$ и след $\mathrm{Sp}(\alpha) = \mathrm{Sp}_{K/\mathbb{Q}}(\alpha)$ — целые рациональные числа.*

Доказательство. Пусть порядок $\mathfrak{O}$ является кольцом множителей для модуля $M = \{\mu_1, \ldots, \mu_n\}$ (можно взять, например, $M = \mathfrak{O}$). Если $\alpha \in \mathfrak{O}$, то в равенствах (6) коэффициенты a_{ij} целые, откуда и следует, что характеристический многочлен числа α (относительно расширения $K/\mathbb{Q}$), имеет целые коэффициенты. Остальные утверждения леммы теперь уже очевидны.

Теорема 4. *Пусть $\mathfrak{O}$ — произвольный порядок поля алгебраических чисел K. Для того чтобы число $\varepsilon \in \mathfrak{O}$ было единицей кольца $\mathfrak{O}$, необходимо и достаточно, чтобы $N(\varepsilon) = \pm 1$.*

Доказательство. Покажем сначала, что для всякого $\alpha \neq 0$ из $\mathfrak{O}$ его норма $N(\alpha)$ делится (в кольце $\mathfrak{O}$) на α. По лемме 2 характеристический многочлен $\varphi(t) = t^n + c_1 t^{n-1} + \ldots + c_n$ числа α имеет целые коэффициенты. Так как $\varphi(\alpha) = 0$, то

$$\frac{N(\alpha)}{\alpha} = \frac{(-1)^n c_n}{\alpha} = (-1)^{n-1}(\alpha^{n-1} + c_1\alpha^{n-2} + \ldots + c_{n-1}).$$

Отношение $N(\alpha)/\alpha$ принадлежит, таким образом, кольцу $\mathfrak{O}$, а это и значит, что $N(\alpha)$ делится на α.

Если теперь $N(\alpha) = \pm 1$, то 1 делится на α, т. е. α есть единица кольца $\mathfrak{O}$. Обратно, если ε — единица кольца $\mathfrak{O}$, т. е. $\varepsilon\varepsilon' = 1$ при некотором $\varepsilon' \in \mathfrak{O}$, то, поскольку $N(\varepsilon)$ и $N(\varepsilon')$ целые, из равенства $N(\varepsilon)N(\varepsilon') = 1$ должно следовать, что $N(\varepsilon) = \pm 1$. Теорема 4, таким образом, доказана.

Для нахождения множителей $\omega \in \mathfrak{O}$, для которых $N(\omega) = 1$, мы должны, следовательно, определить все единицы кольца $\mathfrak{O}$, а затем среди них выделить единицы с нормой $+1$.

Два числа μ_1 и μ_2 из полного модуля M назовем *ассоциированными*, если их отношение $\mu_1/\mu_2 = \varepsilon$ есть единица кольца множителей $\mathfrak{O} = \mathfrak{O}_M$. Ясно, что в случае $M = \mathfrak{O}$ введенное понятие ассоциированности совпадает с обычной ассоциированностью элементов в коммутативном кольце с единицей (см. Дополнение, § 4, п. 1). Легко видеть также, что это отношение ассоциированности в применении лишь к решениям уравнения (7) обладает обычными свойствами эквивалентности, а потому все решения уравнения (7) разбиваются на классы ассоциированных решений. Если μ_1 и μ_2 — два ассоциированных решения, т. е. $\mu_1 = \mu_2\varepsilon$, где

ε — единица кольца $\mathfrak{O}$, то $N(\varepsilon)=1$. Обратно, для всякой единицы ε из $\mathfrak{O}$ с нормой $+1$ вместе с решением μ произведение $\mu\varepsilon$ будет ассоциированным с ним решением. Таким образом, все решения некоторого класса ассоциированных решений получаются из одного умножением на единицы с нормой 1. Сейчас мы покажем, что число таких классов решений конечно.

Теорема 5. *Среди чисел порядка $\mathfrak{O}$ с заданной нормой имеется только конечное число попарно не ассоциированных между собой.*

Доказательство. Пусть $\omega_1, \ldots, \omega_n$ — базис порядка $\mathfrak{O}$ и $c>1$ — произвольное натуральное число.

В соответствии с общим определением п. 1 § 4 Дополнения будем говорить, что два числа α и β из $\mathfrak{O}$ сравнимы между собой по модулю c, если их разность $\alpha-\beta$ делится (в кольце $\mathfrak{O}$) на c. Очевидно, что всякое $\alpha\in\mathfrak{O}$ сравнимо по модулю c с одним и только с одним из чисел

$$x_1\omega_1+\ldots+x_n\omega_n, \qquad 0\leqslant x_i<c, \qquad 1\leqslant i\leqslant n.$$

Все числа из $\mathfrak{O}$ разбиваются, следовательно, на c^n классов чисел, сравнимых между собой по модулю c. Пусть теперь два числа α и β, принадлежащие одному и тому же классу, таковы, что $|N(\alpha)|=|N(\beta)|=c$. Из равенства $\alpha-\beta=c\gamma$, $\gamma\in\mathfrak{O}$, следует, что $\frac{\alpha}{\beta}=1\pm\frac{N(\beta)}{\beta}\gamma\in\mathfrak{O}$ (ибо $\frac{N(\beta)}{\beta}\in\mathfrak{O}$, см. начало доказательства теоремы 4) и аналогично $\frac{\beta}{\alpha}=1\pm\frac{N(\alpha)}{\alpha}\gamma\in\mathfrak{O}$. Таким образом, числа α и β делятся друг на друга, а значит, в кольце $\mathfrak{O}$ они ассоциированы между собой. Этим и доказано, что в $\mathfrak{O}$ может существовать лишь конечное число (не более c^n) попарно не ассоциированных чисел, нормы которых по абсолютной величине равны заданному числу c.

Следствие. *Среди чисел полного модуля M поля K с заданной нормой имеется лишь конечное число попарно не ассоциированных между собой.*

Действительно, если $\mathfrak{O}$ — кольцо множителей модуля M, то при некотором натуральном b модуль bM будет содержаться в $\mathfrak{O}$. Если $\gamma_1, \ldots, \gamma_k$ — попарно не ассоциированные числа из M с нормой c, то числа $b\gamma_1, \ldots, b\gamma_k$ из $\mathfrak{O}$ имеют норму b^nc и попарно не ассоциированы в $\mathfrak{O}$. Число k не может быть, следовательно, сколь угодно большим.

Замечание. Доказательство теоремы 5 показывает, что в кольце $\mathfrak{O}$ (а также в модуле M) существует конечное множество чисел с данной нормой c, обладающих тем свойством, что всякое число из $\mathfrak{O}$ (или из M) с той же нормой ассоциировано с одним из них. Однако это доказательство неэффективно, т. е. оно не дает возможности на самом деле эти числа найти, хотя и указывает эффективную границу для их числа.

Наша основная задача о нахождении всех решений уравнения (7) разбивается, таким образом, на две следующие задачи:

1) В кольце множителей $\mathfrak{O}_M$ найти все единицы ε с нормой $N(\varepsilon)=1$.

2) В модуле M найти числа $\mu_1, \ldots, \mu_k$ с нормой a так, чтобы они были попарно не ассоциированы и в то же время чтобы всякое $\mu \in M$ с нормой a было ассоциировано с одним из них, т. е. имело вид $\mu = \mu_i\varepsilon$, где $1 \leqslant i \leqslant k$ и ε — единица кольца множителей $\mathfrak{O}_M$.

Если эти две задачи будут решены, то тем самым будет решена и задача о целочисленных представлениях рациональных чисел полными разложимыми формами.

4. Максимальный порядок. Поскольку в п. 2 мы столкнулись с понятием порядка, то естественно рассмотреть вопрос о взаимоотношениях между различными порядками в одном и том же поле алгебраических чисел K. В этом пункте мы покажем, что среди порядков поля K имеется один максимальный, содержащий в себе все прочие порядки. По лемме 2 минимальный многочлен всякого числа из какого-нибудь порядка имеет целые коэффициенты. Ниже мы увидим (теорема 6), что максимальный порядок поля алгебраических чисел K совпадает с совокупностью $\widetilde{\mathfrak{O}}$ всех тех чисел из K, минимальные многочлены которых имеют целые коэффициенты. Докажем сначала следующую лемму.

Лемма 3. *Если $\alpha \in \widetilde{\mathfrak{O}}$, т. е. минимальный многочлен $t^m + c_1t^{m-1} + \ldots + c_m$ числа α имеет целые коэффициенты, то модуль $M = \{1, \alpha, \ldots, \alpha^{m-1}\}$ является кольцом.*

Доказательство. Достаточно, очевидно, показать, что всякая степень α^k $(k \geqslant 0)$ числа α принадлежит M. При $k \leqslant m-1$ это верно по определению M. Далее, $\alpha^m = -c_1\alpha^{m-1} - \ldots - c_m$ с целыми c_i, так что $\alpha^m \in M$. Пусть $k > m$, и пусть уже доказано, что $\alpha^{k-1} \in M$, т. е. $\alpha^{k-1} = a_1\alpha^{m-1} + \ldots + a_m$ с целыми a_i. Тогда

$$\alpha^k = \alpha\alpha^{k-1} = a_1\alpha^m + a_2\alpha^{m-1} + \ldots + a_m\alpha.$$

Так как все слагаемые справа принадлежат M, то и α^k принадлежит M. Лемма 3 доказана.

Лемма 4. *Если $\mathfrak{O}$ — произвольный порядок поля K и $\alpha \in \widetilde{\mathfrak{O}}$, то кольцо $\mathfrak{O}[\alpha]$, состоящее из всех многочленов от α с коэффициентами из $\mathfrak{O}$, также является порядком поля K.*

Доказательство. Так как $\mathfrak{O} \subset \mathfrak{O}[\alpha]$, то в кольце $\mathfrak{O}[\alpha]$ имеется $n = (K:\mathbb{Q})$ линейно независимых над $\mathbb{Q}$ чисел. Мы должны, следовательно, доказать только, что $\mathfrak{O}[\alpha]$ является модулем (т. е. обладает конечной системой образующих). Пусть $\omega_1, \ldots, \omega_n$ — базис порядка $\mathfrak{O}$. Согласно лемме 3 всякая степень α^k $(k \geqslant 0)$ представляется в виде $a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1}$ с целыми рациональными a_i, где m — степень минимального многочлена числа α. Отсюда легко следует, что каждое число из $\mathfrak{O}[\alpha]$

можно представить в виде целочисленной линейной комбинации произведений $\omega_i\alpha^j$ $(1 \leqslant i \leqslant n,\ 0 \leqslant j \leqslant m-1)$, а это и значит, что $\mathfrak{O}[\alpha]$ — модуль.

Повторное применение леммы 4 дает нам следующее

Следствие. *Если $\mathfrak{O}$ — порядок и $\alpha_1, \ldots, \alpha_p$ — числа из $\widetilde{\mathfrak{O}}$, то кольцо $\mathfrak{O}[\alpha_1, \ldots, \alpha_p]$ всех многочленов от $\alpha_1, \ldots, \alpha_p$ с коэффициентами из $\mathfrak{O}$ также является порядком.*

Теорема 6. *Все числа поля алгебраических чисел K, минимальные многочлены которых имеют целые рациональные коэффициенты, образуют максимальный порядок поля K.*

Доказательство. Пусть $\mathfrak{O}$ — какой-нибудь порядок поля K, а α и β — произвольные числа из $\widetilde{\mathfrak{O}}$. По следствию леммы 4 кольцо $\mathfrak{O}[\alpha, \beta]$ является порядком, а значит, оно содержится в $\widetilde{\mathfrak{O}}$ (лемма 2). Но тогда разность $\alpha-\beta$ и произведение $\alpha\beta$ также содержатся в $\widetilde{\mathfrak{O}}$. Этим доказано, что $\widetilde{\mathfrak{O}}$ является кольцом. Так как $\mathfrak{O} \subset \widetilde{\mathfrak{O}}$, то $\widetilde{\mathfrak{O}}$ содержит n линейно независимых чисел. Нам остается лишь проверить, что $\widetilde{\mathfrak{O}}$ — модуль.

Выберем в порядке $\mathfrak{O}$ какой-нибудь базис $\omega_1, \ldots, \omega_n$ и построим для него в поле K взаимный базис $\omega_1^*, \ldots, \omega_n^*$ (см. Дополнение, § 2, п. 3). Покажем, что кольцо $\widetilde{\mathfrak{O}}$ содержится в модуле $\mathfrak{O}^* = [\omega_1^*, \ldots, \omega_n^*]$. Пусть α — произвольное число из кольца $\widetilde{\mathfrak{O}}$. Представим его в виде

$$\alpha = c_1\omega_1^* + \ldots + c_n\omega_n^*$$

с рациональными c_i. Умножив это равенство на ω_i и переходя к следу, получим

$$c_i = \operatorname{Sp}\alpha\omega_i, \qquad 1 \leqslant i \leqslant n$$

(мы воспользовались тем, что $\operatorname{Sp}\omega_i\omega_i^* = 1$ и $\operatorname{Sp}\omega_i\omega_j^* = 0$ при $i \neq j$). Все произведения $\alpha\omega_i$ содержатся в порядке $\mathfrak{O}[\alpha]$, поэтому по лемме 2 все числа c_i целые, а значит, $\alpha \in \mathfrak{O}^*$. Таким образом, $\widetilde{\mathfrak{O}} \subset \mathfrak{O}^*$. Применяя теперь следствие теоремы 2, заключаем, что $\widetilde{\mathfrak{O}}$ есть модуль, и теорема 6 доказана.

Проведенное нами доказательство того факта, что $\widetilde{\mathfrak{O}}$ является кольцом, имеет общий характер, т. е. оно сохраняет свою силу (с незначительным изменением) и в общей теории коммутативных колец без делителей нуля. Соответствующие понятия в общем случае изложены в § 4 Дополнения. Применяя введенную там терминологию, можно сказать, что максимальный порядок поля алгебраических чисел K — это целое замыкание кольца целых рациональных чисел $\mathbb{Z}$ в поле K. В связи с этим числа из максимального порядка $\widetilde{\mathfrak{O}}$ часто будут называться целыми числами поля K. Сам же порядок $\widetilde{\mathfrak{O}}$ будет называться также кольцом целых чисел поля K.

Единицы максимального порядка $\widetilde{\mathfrak{O}}$ называются также *единицами поля алгебраических чисел* K.

5. Дискриминант полного модуля. Пусть $\mu_1, \ldots, \mu_n$ и $\mu_1', \ldots, \mu_n'$ — два базиса полного модуля M в поле алгебраических чисел K. Как мы знаем (см. п. 1), матрица перехода от первого базиса ко второму унимодулярна (т. е. является целочисленной матрицей с определителем ± 1). Отсюда следует, что дискриминанты $D(\mu_1, \ldots, \mu_n)$ и $D(\mu_1', \ldots, \mu_n')$ базисов равны (см. Дополнение, § 2, п. 3, формула (12)). Все базисы модуля M имеют, таким образом, один и тот же дискриминант. Это общее значение дискриминантов всех базисов модуля M, являющееся, очевидно, рациональным числом, называется *дискриминантом данного модуля* M.

Всякий порядок поля K является полным модулем в K. Можно говорить поэтому о дискриминанте того или иного порядка. Так как след всякого числа из порядка есть целое число, то дискриминант порядка всегда является целым рациональным числом (это же справедливо, разумеется, и для всякого полного модуля, содержащегося в $\widetilde{\mathfrak{O}}$).

Базис максимального порядка $\widetilde{\mathfrak{O}}$ поля алгебраических чисел K часто называют также *фундаментальным базисом* этого поля, а его дискриминант — *дискриминантом поля* K. Дискриминант поля алгебраических чисел является весьма важной его арифметической характеристикой и в дальнейшем во многих вопросах будет играть существенную роль.

Задачи

1. Пусть $\omega_1, \omega_2, \omega_3$ — линейно независимые числа поля алгебраических чисел K. Доказать, что все числа вида $a\omega_1 + b\omega_2 + c\omega_3$, где целые рациональные a, b, c связаны соотношением $2a + 3b + 5c = 0$, образуют модуль в K, и найти его базис.

2. Найти кольцо множителей модуля $\{2, \sqrt{2}/2\}$ в поле $\mathbb{Q}(\sqrt{2})$. Показать, далее, что в поле $\mathbb{Q}(\sqrt{2})$ модуль $\{1, \sqrt{2}\}$ является максимальным порядком.

3. Показать, что в поле рациональных чисел $\mathbb{Q}$ имеется единственный порядок — кольцо всех целых рациональных чисел.

4. Доказать, что в порядке $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ поля $\mathbb{Q}(\sqrt[3]{2})$ всякое число с нормой 2 ассоциировано с $\sqrt[3]{2}$.

5. Доказать, что пересечение двух полных модулей есть также полный модуль.

6. Доказать, что всякий модуль поля алгебраических чисел, являющийся кольцом, содержится в максимальном порядке.

7. Пусть $M = \{\alpha_1, \ldots, \alpha_n\}$ и $N = \{\beta_1, \ldots, \beta_n\}$ — два полных модуля поля K. Модуль, порожденный произведениями $\alpha_i\beta_j$ $(1 \leqslant i, j \leqslant n)$, не зависит от выбора базисов α_i и β_j. Он называется произведением модулей M и N и обозначается через MN. Доказать, что кольца множителей модулей M и N содержатся в кольце множителей их произведения MN.

8. Пусть M — полный модуль, содержащийся в максимальном порядке $\widetilde{\mathfrak{O}}$ поля алгебраических чисел K. Доказать, что если дискриминант модуля M не делится на квадрат целого числа $\neq 1$, то он совпадает с $\widetilde{\mathfrak{O}}$.

9. Пусть θ — примитивное число поля алгебраических чисел K степени n, содержащееся в максимальном порядке. Доказать, что если дискриминант минимального многочлена числа θ не делится на квадрат, то числа $1, \theta, \ldots, \theta^{n-1}$ образуют фундаментальный базис поля K.

10. Найти фундаментальный базис и дискриминант поля $\mathbb{Q}\left(\sqrt[3]{2}\right)$.

11. Найти фундаментальный базис и дискриминант поля $\mathbb{Q}(\rho)$, где ρ — корень уравнения $x^3 - x - 1 = 0$.

12. Пусть M — полный модуль поля алгебраических чисел K. Доказать, что совокупность M^* тех $\xi \in K$, для которых $\mathrm{Sp}\,\alpha\xi \in \mathbb{Z}$ при всех $\alpha \in M$, является также полным модулем поля K. Модуль M^* называется взаимным для модуля M. Показать, далее, что если $\mu_1, \ldots, \mu_n$ — базис M, то взаимный базис $\mu_1^*, \ldots, \mu_n^*$ в поле K (относительно $\mathbb{Q}$) является базисом M^*.

13. Доказать, что $(M^*)^* = M$, т. е. что взаимный модуль для M^* совпадает с M.

14. Доказать, что взаимные модули M и M^* имеют одно и то же кольцо множителей.

15. Показать, что для полных модулей M_1 и M_2 включения $M_1 \subset M_2$ и $M_1^* \supset M_2^*$ эквивалентны.

16. Пусть θ — примитивное число поля алгебраических чисел K степени n, принадлежащее максимальному порядку $\widetilde{\mathfrak{O}}$, и $f(t)$ — его минимальный многочлен над $\mathbb{Q}$. Показать, что для модуля $M = \{1, \theta, \ldots, \theta^{n-1}\}$ (являющегося, очевидно, порядком) взаимный модуль M^* совпадает с $\frac{1}{f'(\theta)} M$.

17. Пусть M — полный модуль в K и $\mathfrak{O}$ — его кольцо множителей. Доказать, что произведение MM^* (см. задачу 7) совпадает с $\mathfrak{O}^*$.

18. Доказать, что в поле $\mathbb{Q}(\theta)$, $\theta^3 = 2$, для модуля $M = \{4, \theta, \theta^2\}$ кольцом множителей является порядок $\{1, 2\theta, 2\theta^2\}$, а для модуля $M^2 = \{2, 2\theta, \theta^2\}$ — максимальный порядок $\{1, \theta, \theta^2\}$.

19. Многочлен $t^n + a_1 t^{n-1} + \ldots + a_n$ с целыми рациональными коэффициентами называется многочленом Эйзенштейна относительно простого числа p, если все коэффициенты $a_1, \ldots, a_n$ делятся на p, а свободный член a_n, делясь на p, не делится на p^2. Доказать, что если целое примитивное число θ поля алгебраических чисел K степени n является корнем многочлена Эйзенштейна относительно p, то

$$N\left(c_0 + c_1\theta + \ldots + c_{n-1}\theta^{n-1}\right) \equiv c_0^n \pmod{p}$$

при любых целых рациональных $c_0, c_1, \ldots, c_{n-1}$.

20. Если θ — примитивное целое число поля алгебраических чисел K степени n, то индекс порядка $\{1, \theta, \ldots, \theta^{n-1}\}$ в максимальном порядке называется также индексом числа θ. Доказать, что если θ является корнем многочлена Эйзенштейна относительно простого числа p, то p не входит в индекс числа θ.

21. Доказать, что для каждого из трех кубических полей:

$$K_1 = \mathbb{Q}(\theta), \qquad \theta^3 - 18\theta - 6 = 0,$$

$$K_2 = \mathbb{Q}(\theta), \qquad \theta^3 - 36\theta - 78 = 0,$$

$$K_3 = \mathbb{Q}(\theta), \qquad \theta^3 - 54\theta - 150 = 0,$$

фундаментальным базисом является степенной базис $1, \theta, \theta^2$. Убедиться, далее, что все эти поля имеют один и тот же дискриминант, равный $22\,356 =$

$= 23\cdot 2^2\cdot 3^5$. (Поля K_1, K_2, K_3, как это следует из задачи 14 § 7 гл. III, различны.)

22. Показать, что для кубического поля $\mathbb{Q}(\theta)$, $\theta^3-\theta-4=0$, фундаментальным базисом является базис $1, \theta, \dfrac{\theta+\theta^2}{2}$.

23. Пусть a и b — взаимно простые натуральные числа, свободные от квадратов. Положим $k=ab$, если $a^2-b^2\equiv 0 \pmod 9$, и $k=3ab$, если $a^2-b^2\not\equiv 0 \pmod 9$. Показать, что дискриминант поля $\mathbb{Q}\left(\sqrt[3]{ab^2}\right)$ равен $D=-3k^2$.

Указание. Положим $\theta=\sqrt[3]{ab^2}$, $\bar\theta=\theta^2/b=\sqrt[3]{a^2b}$. Показать, что в случае $a^2-b^2\not\equiv 0 \pmod 9$ числа $1, \theta, \bar\theta$ образуют фундаментальный базис. Пусть $a^2-b^2\equiv 0 \pmod 9$. Выберем $\sigma=\pm 1$ и $\tau=\pm 1$ так, чтобы $a\equiv \sigma \pmod 3$ и $b\equiv\tau \pmod 3$. Показать, что в этом случае в качестве фундаментального базиса можно взять числа $1, \theta, \dfrac{1+\sigma\theta+\tau\bar\theta}{3}$.

24. Доказать, что если натуральное a свободно от квадратов и $a\not\equiv \pm 1 \pmod 9$, то в поле $\mathbb{Q}\left(\sqrt[3]{a}\right)$ числа $1, \sqrt[3]{a}, \sqrt[3]{a^2}$ образуют фундаментальный базис.

25. Доказать, что кубическое поле является чисто кубическим (т. е. имеет вид $\mathbb{Q}\left(\sqrt[3]{m}\right)$) тогда и только тогда, когда его дискриминант равен $-3d^2$ (при некотором натуральном d).

26. Пусть a, b, c, d — свободные от квадратов попарно взаимно простые натуральные числа >1, одно из которых делится на 3. Доказать, что чисто кубические поля $\mathbb{Q}(\theta)$, $\theta^3=abc^2d^2$, и $\mathbb{Q}(\eta)$, $\eta^3=acb^2d^2$, имеющие один и тот же дискриминант $-27a^2b^2c^2d^2$, различны.

Указание. Рассмотреть поля $\mathbb{Q}(\eta/\theta)=\mathbb{Q}\left(\sqrt[3]{bc^2}\right)$ и $\mathbb{Q}(\eta^2/\theta)=\mathbb{Q}\left(\sqrt[3]{ad^2}\right)$.

27. Доказать, что для любого натурального n можно указать n различных чисто кубических полей с одним и тем же дискриминантом (использовать предыдущую задачу).

§ 3. Геометрический метод

Сформулированные в конце п. 3 § 2 две задачи (к которым сводится вопрос о представлениях чисел полными разложимыми формами) для своего решения требуют привлечения новых соображений геометрического характера. В основе этих соображений лежит метод изображения алгебраических чисел точками n-мерного пространства, аналогичный хорошо известному способу изображения комплексных чисел на плоскости Коши.

1. Геометрическое изображение алгебраических чисел. Если поле алгебраических чисел K имеет степень n над полем рациональных чисел $\mathbb{Q}$, то для него имеется равно n различных изоморфизмов в поле всех комплексных чисел $\mathbb{C}$ (см. Дополнение, § 2, п. 3).

Определение. *Если при изоморфизме $\sigma: K\to\mathbb{C}$ образ поля K содержится в поле вещественных чисел, то этот изоморфизм σ называется вещественным; в противном случае он называется комплексным.*

Так, для кубического поля $K = \mathbb{Q}(\theta)$, где $\theta^3 = 2$, изоморфизм $\mathbb{Q}(\theta) \to \mathbb{Q}(\sqrt[3]{2})$, при котором $\theta \to \sqrt[3]{2}$, вещественный (под $\sqrt[3]{2}$ понимаем здесь вещественное значение корня). Два других изоморфизма $\mathbb{Q}(\theta) \to \mathbb{Q}(\varepsilon\sqrt[3]{2})$ и $\mathbb{Q}(\theta) \to \mathbb{Q}(\varepsilon^2\sqrt[3]{2})$ $\left(\varepsilon = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right)$ комплексные. Если d — рациональное число, не являющееся квадратом, то для поля $\mathbb{Q}(\theta)$, $\theta^2 = d$, оба изоморфизма вещественны при $d > 0$ и комплексны при $d < 0$. Вообще, если в произвольном поле алгебраических чисел K выбран примитивный элемент θ, являющийся корнем неприводимого над $\mathbb{Q}$ многочлена $\varphi(t)$, и если $\theta_1, \ldots, \theta_n$ — корни $\varphi(t)$ в поле $\mathbb{C}$, то изоморфизм

$$K = \mathbb{Q}(\theta) \to \mathbb{Q}(\theta_i) \subset \mathbb{C}, \quad \theta \to \theta_i, \tag{1}$$

будет вещественным, если корень θ_i вещественный, и комплексным в противном случае.

Условимся для любого комплексного числа $\gamma = x + yi$ (x и y вещественные) через $\overline{\gamma}$ обозначать сопряженное комплексное число $x - yi$.

Пусть $\sigma\colon K \to \mathbb{C}$ — комплексный изоморфизм. Очевидно, что отображение $\overline{\sigma}\colon K \to \mathbb{C}$, определенное равенством

$$\overline{\sigma}(\alpha) = \overline{\sigma(\alpha)}, \quad \alpha \in K,$$

является также комплексным изоморфизмом K в $\mathbb{C}$. Этот изоморфизм $\overline{\sigma}$ называется сопряженным с σ. Так как $\overline{\sigma} \neq \sigma$ и $\overline{\overline{\sigma}} = \sigma$, то все комплексные изоморфизмы K в $\mathbb{C}$ разбиваются, следовательно, на пары сопряженных между собой изоморфизмов. В частности, число комплексных изоморфизмов всегда четное. Два комплексных изоморфизма вида (1) сопряжены между собой тогда и только тогда, когда соответствующие им корни θ_i и θ_j являются комплексно сопряженными числами.

Предположим, что среди изоморфизмов K в $\mathbb{C}$ имеется s вещественных $\sigma_1, \ldots, \sigma_s$ и $2t$ комплексных, так что $s + 2t = n = (K{:}\mathbb{Q})$. Из каждой пары сопряженных между собой комплексных изоморфизмов выберем какой-нибудь один. Полученную систему комплексных изоморфизмов обозначим через $\sigma_{s+1}, \ldots, \sigma_{s+t}$. Система всех изоморфизмов поля K в $\mathbb{C}$ запишется тогда в виде

$$\sigma_1, \ldots, \sigma_s, \sigma_{s+1}, \overline{\sigma}_{s+1}, \ldots, \sigma_{s+t}, \overline{\sigma}_{s+t}.$$

Именно такая нумерация изоморфизмов в дальнейшем постоянно будет предполагаться. Конечно, для некоторых полей может оказаться, что вещественных изоморфизмов нет ($s = 0$) или, наоборот, что все изоморфизмы вещественные ($t = 0$).

Рассмотрим совокупность $\mathfrak{L}^{s,t}$ строчек вида

$$x = (x_1, \ldots, x_s; x_{s+1}, \ldots, x_{s+t}), \tag{2}$$

в которых первые s компонент $x_1, \ldots, x_s$ — вещественные, а ос-

тальные $x_{s+1}, \ldots, x_{s+t}$ — произвольные комплексные числа. Определим сложение и умножение этих строчек, а также умножение их на вещественные числа покомпонентно. Ясно, что относительно этих действий $\mathfrak{L}^{s,t}$ является коммутативным кольцом с единицей $(1, \ldots, 1)$ и в то же время вещественным линейным пространством. Строчки (2) мы будем называть векторами или точками пространства $\mathfrak{L}^{s,t}$.

В качестве базиса $\mathfrak{L}^{s,t}$ (над полем вещественных чисел) можно взять, очевидно, векторы

$$\left.\begin{array}{l}(1, \ldots, 0;\ 0, \ldots, 0)\\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\\ (0, \ldots, 1;\ 0, \ldots, 0)\end{array}\right\} s,$$

$$\left.\begin{array}{l}(0, \ldots, 0;\ 1, \ldots, 0)\\ (0, \ldots, 0;\ i, \ldots, 0)\\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\\ (0, \ldots, 0;\ 0, \ldots, 1)\\ (0, \ldots, 0;\ 0, \ldots, i)\end{array}\right\} 2t. \tag{3}$$

Размерность вещественного пространства $\mathfrak{L}^{s,t}$ равна, следовательно, $n = s + 2t$. Если мы положим

$$x_{s+j} = y_j + iz_j \qquad (j = 1, \ldots, t),$$

то вектор (2) в базисе (3) будет иметь координаты

$$(x_1, \ldots, x_s;\ y_1, z_1, \ldots, y_t, z_t). \tag{4}$$

В тех случаях, когда $\mathfrak{L}^{s,t}$ будет рассматриваться только как n-мерное линейное вещественное пространство, мы будем обозначать его также через $\mathbb{R}^n$.

Зафиксируем в $\mathfrak{L}^{s,t}$ некоторую точку x. Отображение $x' \to xx'$ $(x' \in \mathfrak{L}^{s,t})$, т. е. умножение произвольной точки из $\mathfrak{L}^{s,t}$ на x, является, очевидно, линейным преобразованием вещественного пространства $\mathfrak{L}^{s,t} = \mathbb{R}^n$. В базисе (3) матрица этого преобразования, как легко видеть, имеет вид

$$\begin{pmatrix} x_1 & & & & & & \\ & \ddots & & & & & \\ & & x_s & & & & \\ & & & \begin{matrix} y_1 & -z_1 \\ z_1 & y_1 \end{matrix} & & & \\ & & & & \ddots & & \\ & & & & & \begin{matrix} y_t & -z_t \\ z_t & y_t \end{matrix} \end{pmatrix},$$

где все невыписанные элементы равны нулю. Определитель этой матрицы равен

$$x_1 \dots x_s (y_1^2 + z_1^2) \dots (y_t^2 + z_t^2) = x_1 \dots x_s |x_{s+1}|^2 \dots |x_{s+t}|^2.$$

Это подсказывает нам следующее определение. Под *нормой* $N(x)$ произвольной точки $x = (x_1, \dots, x_{s+t}) \in \mathfrak{L}^{s,t}$ будем понимать выражение

$$N(x) = x_1 \dots x_s |x_{s+1}|^2 \dots |x_{s+t}|^2.$$

Проведенная только что выкладка показывает, что норма $N(x)$ точки x может быть определена также как определитель матрицы линейного преобразования $x' \to x'x$.

Введенное понятие нормы обладает, очевидно, свойством мультипликативности: $N(xx') = N(x)N(x')$.

Перейдем теперь к изображению чисел поля K точками пространства $\mathfrak{L}^{s,t}$. Каждому числу α из K поставим в соответствие точку

$$x(\alpha) = (\sigma_1(\alpha), \dots, \sigma_s(\alpha); \sigma_{s+1}(\alpha), \dots, \sigma_{s+t}(\alpha)) \tag{5}$$

из $\mathfrak{L}^{s,t}$. Эта точка и является геометрическим изображением числа α.

Если α и β — различные числа из K, то при любом $k = 1, \dots, s+t$ числа $\sigma_k(\alpha)$ и $\sigma_k(\beta)$ также различны, а значит, $x(\alpha) \neq x(\beta)$. Таким образом, отображение

$$\alpha \to x(\alpha), \qquad \alpha \in K,$$

взаимно однозначно. (Конечно, оно не является отображением «на», т. е. не всякая точка из $\mathfrak{L}^{s,t}$ является изображением числа из поля K).

Так как $\sigma_k(\alpha + \beta) = \sigma_k(\alpha) + \sigma_k(\beta)$ и $\sigma_k(\alpha\beta) = \sigma_k(\alpha)\sigma_k(\beta)$, то

$$x(\alpha + \beta) = x(\alpha) + x(\beta), \tag{6}$$

$$x(\alpha\beta) = x(\alpha)x(\beta), \tag{7}$$

т. е. при сложении и умножении чисел в K соответствующие им точки также складываются и умножаются. Далее, если a — рациональное число, то $\sigma_k(a\alpha) = \sigma_k(a)\sigma_k(\alpha) = a\sigma_k(\alpha)$, откуда

$$x(a\alpha) = ax(\alpha). \tag{8}$$

Так как согласно § 2 (п. 3) Дополнения мы имеем

$$N(\alpha) = N_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) \dots \sigma_s(\alpha)\, \sigma_{s+1}(\alpha)\, \bar{\sigma}_{s+1}(\alpha) \dots \sigma_{s+t}(\alpha)\, \bar{\sigma}_{s+t}(\alpha) =$$

$$= \sigma_1(\alpha) \dots \sigma_s(\alpha) |\sigma_{s+1}(\alpha)|^2 \dots |\sigma_{s+t}(\alpha)|^2,$$

то норма $N(x(\alpha))$ точки $x(\alpha)$ совпадает с нормой $N(\alpha)$ числа α:

$$N(x(\alpha)) = N(\alpha), \quad \alpha \in K.$$

Рассмотрим два простых примера. Если d — положительное рациональное число, не являющееся квадратом, то для вещест-

венного квадратичного поля $\mathbb{Q}(\theta)$, $\theta^2 = d$, геометрическим изображением числа $\alpha = a + b\theta$ (a и b рациональны) будет точка $x(\alpha) = (a + b\sqrt{d},\ a - b\sqrt{d})$. В случае мнимого квадратичного поля $\mathbb{Q}(\eta)$, $\eta^2 = -d$, изображением числа $\beta = a + b\eta$ будет точка на комплексной плоскости с координатами $(a,\ b\sqrt{d})$(базис (3) в этом случае состоит из чисел $1,\ i$).

Покажем, что для произвольного базиса $\alpha_1, \ldots, \alpha_n$ поля K (над $\mathbb{Q}$) соответствующие им векторы $x(\alpha_1), \ldots, x(\alpha_n)$ из $\mathfrak{L}^{s,t} = \mathbb{R}^n$ линейно независимы (в вещественном смысле). Для этого положим

$$\sigma_k(\alpha_l) = x_k^{(l)}, \qquad 1 \leqslant k \leqslant s,$$
$$\sigma_{s+j}(\alpha_l) = y_j^{(l)} + iz_j^{(l)}, \qquad 1 \leqslant j \leqslant t.$$

Так как вектор

$$x(\alpha_l) = \left(x_1^{(l)}, \ldots, x_s^{(l)}; y_1^{(l)} + iz_1^{(l)}, \ldots, y_t^{(l)} + iz_t^{(l)}\right)$$

в базисе (3) имеет координаты $\left(x_1^{(l)}, \ldots, x_s^{(l)}, y_1^{(l)}, z_1^{(l)}, \ldots, y_t^{(l)}, z_t^{(l)}\right)$, то для доказательства нашего утверждения надо лишь проверить, что определитель

$$d = \begin{vmatrix} x_1^{(1)} \ldots x_s^{(1)} & y_1^{(1)} & z_1^{(1)} \ldots y_t^{(1)} & z_t^{(1)} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ x_1^{(n)} \ldots x_s^{(n)} & y_1^{(n)} & z_1^{(n)} \ldots y_t^{(n)} & z_t^{(n)} \end{vmatrix}$$

отличен от нуля. Рассмотрим вместо d другой определитель:

$$d^* = \begin{vmatrix} x_1^{(1)} \ldots x_s^{(1)} & y_1^{(1)} + iz_1^{(1)} & y_1^{(1)} - iz_1^{(1)} \ldots \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ x_1^{(n)} \ldots x_s^{(n)} & y_1^{(n)} + iz_1^{(n)} & y_1^{(n)} - iz_1^{(n)} \ldots \end{vmatrix},$$

который можно записать также в виде

$$d^* = \begin{vmatrix} \sigma_1(\alpha_1) \ldots \sigma_s(\alpha_1) & \sigma_{s+1}(\alpha_1) & \bar{\sigma}_{s+1}(\alpha_1) \ldots \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \sigma_1(\alpha_n) \ldots \sigma_s(\alpha_n) & \sigma_{s+1}(\alpha_n) & \bar{\sigma}_{s+1}(\alpha_n) \ldots \end{vmatrix}.$$

В определителе d^* к столбцу с номером $s+1$ прибавим последующий столбец и вынесем 2 за знак определителя. Этот новый столбец вычтем из последующего, а затем из полученного столбца с номером $s+2$ вынесем $-i$ за знак определителя. Проделав такие же операции с каждой парой следующих столбцов, мы придем в конце концов к равенству

$$d^* = (-2i)^t d. \tag{9}$$

В § 2 (п. 3) Дополнения доказано, что

$$d^{*2} = D, \tag{10}$$

где $D = D(\alpha_1, \ldots, \alpha_n)$ — дискриминант базиса $\alpha_1, \ldots, \alpha_n$ (отно-

сительно расширения $K/\mathbb{Q}$). Так как $D \neq 0$, то из (9) и (10) следует, что определитель d также отличен от нуля.

Будем считать теперь, что $\alpha_1, \ldots, \alpha_n$ — базис полного модуля M в поле K. В силу (6) и (8) для всякого $\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n$ из M ($a_1, \ldots, a_n$ целые рациональные) его геометрическим изображением в $\mathbb{R}^n$ будет вектор $x(\alpha) = a_1x(\alpha_1) + \ldots + a_nx(\alpha_n)$. Мы получили, таким образом, следующий результат.

Теорема 1. *При геометрическом изображении чисел поля K степени $n = s + 2t$ точками пространства $\mathbb{R}^n$ совокупность всех векторов, изображающих числа полного модуля $M = \{\alpha_1, \ldots, \alpha_n\}$, совпадает с совокупностью всех целочисленных линейных комбинаций n линейно независимых (в пространстве $\mathbb{R}^n$) векторов $x(\alpha_1), \ldots, x(\alpha_n)$.*

Замечание. Линейное пространство $\mathfrak{L}^{s,t}$, в котором мы изображаем числа поля K, является алгеброй над полем вещественных чисел $\mathbb{R}$. Эта алгебра может быть отождествлена с тензорным произведением $\mathfrak{A} = \mathbb{R} \otimes_{\mathbb{Q}} K$ полей $\mathbb{R}$ и K, рассматриваемых как алгебры над полем рациональных чисел $\mathbb{Q}$. Именно, алгебра $\mathfrak{A}$ (над полем вещественных чисел $\mathbb{R}$) однозначно распадается в прямую сумму полей, каждое из которых изоморфно либо полю вещественных чисел $\mathbb{R}$, либо полю комплексных чисел $\mathbb{C}$. Пусть

$$\mathfrak{A} = \mathbb{R}_1 \oplus \ldots \oplus \mathbb{R}_s \oplus \mathbb{C}_1 \oplus \ldots \oplus \mathbb{C}_t,$$

где $\mathbb{R}_i \approx \mathbb{R}$ $(1 \leqslant i \leqslant s)$ и $\mathbb{C}_j \approx \mathbb{C}$ $(1 \leqslant j \leqslant t)$. Пусть, далее, φ_i — однозначно определенный изоморфизм $\mathbb{R}_i$ на $\mathbb{R}$ и φ_{s+j} — один из двух изоморфизмов $\mathbb{C}_j$ на $\mathbb{C}$. Каждый элемент $\xi \in \mathfrak{A}$ однозначно представляется в виде

$$\xi = \xi_1 + \ldots + \xi_s + \xi_{s+1} + \ldots + \xi_{s+t},$$

где $\xi_i \in \mathbb{R}_i$ и $\xi_{s+j} \in \mathbb{C}_j$. Положим

$$\varphi(\xi) = (\varphi_1(\xi_1), \ldots, \varphi_{s+t}(\xi_{s+t})) \in \mathfrak{L}^{s,t}.$$

Можно показать, что отображение $\xi \to \varphi(\xi)$ $(\xi \in \mathfrak{A})$ является изоморфизмом алгебры $\mathfrak{A}$ на алгебру $\mathfrak{L}^{s,t}$. При этом $\varphi(1 \otimes \alpha) = x(\alpha)$ для любого $\alpha \in K$.

2. Решетки. Геометрическое изучение полных модулей основывается на том их свойстве, которое установлено в теореме 1. Рассмотрим поэтому в $\mathbb{R}^n$ совокупности векторов такого же типа независимо от того, являются они образами чисел некоторого модуля или нет.

Определение. *Пусть $e_1, \ldots, e_m$, $m \leqslant n$, — линейно независимая система векторов пространства $\mathbb{R}^n$. Совокупность $\mathfrak{M}$ всех векторов вида*

$$a_1e_1 + \ldots + a_me_m,$$

где a_i независимо друг от друга пробегают все целые рациональные числа, называется m-мерной решеткой в $\mathbb{R}^n$, а сами векторы $e_1, \ldots, e_m$ — базисом этой решетки. Если $m = n$, то решетка называется полной, в противном случае — неполной.

Содержание теоремы 1 заключается, следовательно, в том, что числа полного модуля геометрически изображаются векторами некоторой полной решетки.

Легко видеть, что две линейно независимые системы векторов $e_1, \ldots, e_m$ и $f_1, \ldots, f_m$ определяют одну и ту же решетку тогда и только тогда, когда они связаны между собой унимодулярным преобразованием, т. е. когда

$$f_i = \sum_{j=1}^{m} c_{ij} e_j, \quad 1 \leqslant i \leqslant m,$$

где (c_{ij}) — целочисленная матрица с определителем ± 1.

Более детальное изучение решеток основывается на привлечении метрических свойств пространства $\mathbb{R}^n$. Введем в $\mathfrak{L}^{s,t} = \mathbb{R}^n$ скалярное произведение, считая, что векторы (3) образуют ортонормированный базис. Если векторы x и x' в базисе (3) имеют соответственно координаты $(x_1, \ldots, x_n)$ и $(x_1', \ldots, x_n')$, то для скалярного произведения (x, x') имеем, следовательно, формулу

$$(x, x') = x_1 x_1' + \ldots + x_n x_n'.$$

Длина вектора x будет обозначаться через $\|x\|$.

Пусть r — вещественное положительное число. Совокупность всех точек x с координатами $(x_1, \ldots, x_n)$ (в базисе (3)), для которых

$$\|x\| = \sqrt{x_1^2 + \ldots + x_n^2} < r,$$

обозначим через $U(r)$. Это множество $U(r)$ называется (открытым) шаром радиуса r с центром в начале.

Множество точек из $\mathbb{R}^n$ называется *ограниченным*, если оно содержится в некотором шаре $U(r)$.

Множество точек пространства $\mathbb{R}^n$ называется *дискретным*, если для любого $r > 0$ только конечное число точек этого множества содержится в шаре $U(r)$.

Лемма 1. *Множество точек произвольной решетки $\mathfrak{M}$ в $\mathbb{R}^n$ дискретно.*

Доказательство. Так как всякая неполная решетка может быть вложена в полную (многими способами), то достаточно провести доказательство для полной решетки $\mathfrak{M}$. Выберем в $\mathfrak{M}$ какой-нибудь базис $e_1, \ldots, e_n$. Условия

$$(x, e_2) = 0, \ \ldots, \ (x, e_n) = 0$$

дают нам систему $n - 1$ однородных линейных уравнений с n

неизвестными. Так как у этой системы имеется ненулевое решение, то существует ненулевой вектор x, ортогональный к векторам $e_2, \ldots, e_n$. Если бы мы имели также $(x, e_1) = 0$, то вектор x был бы ортогонален ко всем векторам пространства $\mathbb{R}^n$, что невозможно. Следовательно, $(x, e_1) \neq 0$. Вектор $f_1 = \frac{1}{(x, e_1)} x$ будет также ортогонален ко всем векторам $e_2, \ldots, e_n$, и для него $(f_1, e_1) = 1$. Таким образом, для каждого i $(1 \leqslant i \leqslant n)$ мы можем найти вектор f_i, для которого

$$(f_i, e_j) = \begin{cases} 1 & \text{при } j = i, \\ 0 & \text{при } j \neq i. \end{cases}$$

Пусть теперь вектор $z = a_1 e_1 + \ldots + a_n e_n$ из $\mathfrak{M}$ (a_i целые рациональные) принадлежит шару $U(r)$, т. е. $\|z\| < r$. Так как $a_k = (z, f_k)$, то в силу неравенства Коши — Буняковского имеем

$$|a_k| = |(z, f_k)| \leqslant \|z\| \cdot \|f_k\| < r\|f_k\|,$$

где $r\|f_k\|$ не зависит от z. Таким образом, для целых чисел a_k мы имеем только конечное число возможностей, а значит, число тех $z \in \mathfrak{M}$, для которых $\|z\| < r$, конечно. Лемма 1 доказана.

Пусть X — некоторое множество точек пространства $\mathbb{R}^n$ и z — точка из $\mathbb{R}^n$. Совокупность точек вида $x + z$, где x пробегает все точки из X, называется сдвигом множества X на вектор z и обозначается через $X + z$.

Определение. *Пусть $e_1, \ldots, e_m$ — какой-нибудь базис решетки $\mathfrak{M}$. Множество T точек вида*

$$\alpha_1 e_1 + \ldots + \alpha_m e_m,$$

где $\alpha_1, \ldots, \alpha_m$ независимо друг от друга пробегают вещественные числа, удовлетворяющие условиям $0 \leqslant \alpha_i < 1$, называется основным параллелепипедом решетки $\mathfrak{M}$.

Основной параллелепипед определен, следовательно, своей решеткой не однозначно; он зависит от выбора базиса.

Лемма 2. *Если T — основной параллелепипед полной решетки $\mathfrak{M}$, то множества $T_z = T + z$, где z пробегает все точки из $\mathfrak{M}$, попарно не пересекаясь, заполняют все пространство $\mathbb{R}^n$.*

Доказательство. Пусть $e_1, \ldots, e_n$ — базис решетки $\mathfrak{M}$, на котором построен параллелепипед T. Мы должны показать, что всякая точка $x = x_1 e_1 + \ldots + x_n e_n$ из $\mathbb{R}^n$ принадлежит одному и только одному множеству T_z. Для каждого i представим вещественное число x_i в виде $x_i = k_i + \alpha_i$, где k_i целое рациональное, а α_i удовлетворяет условию $0 \leqslant \alpha_i < 1$. Полагая $z = k_1 e_1 + \ldots + k_n e_n$ и $u = \alpha_1 e_1 + \ldots + \alpha_n e_n$, будем иметь

$$x = u + z, \qquad u \in T, \ z \in \mathfrak{M},$$

а это означает, что $x \in T_z$. Если теперь $x \in T_{z'}$, т. е. $x = u' + z'$

($u' \in T$, $z' \in \mathfrak{M}$), то сравнивая в равенстве $u+z=u'+z'$ коэффициенты при e_i, легко получим, что $z=z'$. Лемма 2, таким образом, доказана.

Лемма 3. *Для любого вещественного числа $r>0$ существует только конечное число множеств T_z* (см. обозначения леммы 2), *пересекающихся с шаром $U(r)$.*

Доказательство. Пусть $e_1, \ldots, e_n$ — базис решетки $\mathfrak{M}$, на котором построен параллелепипед T. Если мы положим $d=\|e_1\|+\ldots+\|e_n\|$, то для любого вектора $u=\alpha_1 e_1+\ldots+\alpha_n e_n \in T$ будем иметь

$$\|u\| \leqslant \|\alpha_1 e_1\|+\ldots+\|\alpha_n e_n\| = \alpha_1\|e_1\|+\ldots+\alpha_n\|e_n\| < d.$$

Пусть множество T_z ($z \in \mathfrak{M}$) пересекается с $U(r)$. Это значит, что для некоторого вектора $x=u+z$, где $u \in T$, $z \in \mathfrak{M}$, имеем $\|x\|<r$. Так как $z=x-u$, то

$$\|z\| \leqslant \|x\|+\|-u\| < r+d,$$

т. е. точка z содержится в шаре $U(r+d)$. Согласно лемме 1 таких точек $z \in \mathfrak{M}$ существует только конечное число, и лемма 3 доказана.

Очевидно, что векторы решетки образуют группу относительно операции сложения векторов. Другими словами, каждая решетка является подгруппой аддитивной группы $\mathbb{R}^n$. Лемма 1 показывает, однако, что это далеко не произвольная подгруппа. Мы докажем сейчас, что свойство решеток, установленное в этой лемме, характеризует решетки среди всех подгрупп группы $\mathbb{R}^n$.

Лемма 4. *Подгруппа $\mathfrak{M}$ группы $\mathbb{R}^n$, множество точек которой дискретно, является решеткой.*

Доказательство. Обозначим через $\mathfrak{S}$ наименьшее линейное подпространство пространства $\mathbb{R}^n$, содержащее множество $\mathfrak{M}$, и через m — размерность $\mathfrak{S}$. Мы можем тогда в $\mathfrak{M}$ выбрать m векторов $e_1, \ldots, e_m$, образующих базис подпространства $\mathfrak{S}$. Обозначим через $\mathfrak{M}_0$ решетку с базисом $e_1, \ldots, e_m$. Очевидно, что $\mathfrak{M}_0 \subset \mathfrak{M}$. Докажем, что индекс $(\mathfrak{M}:\mathfrak{M}_0)$ конечен. Действительно, мы можем представить любой вектор x из $\mathfrak{M}$ (даже любой вектор из $\mathfrak{S}$) в виде

$$x=u+z, \tag{11}$$

где $z \in \mathfrak{M}_0$, а u лежит в основном параллелепипеде T решетки $\mathfrak{M}_0$, построенном на базисе $e_1, \ldots, e_m$. По условию $x \in \mathfrak{M}$ и $z \in \mathfrak{M}_0 \subset \mathfrak{M}$, а так как $\mathfrak{M}$ является группой, то и $u \in \mathfrak{M}$. Но T является ограниченным множеством, и ввиду дискретности $\mathfrak{M}$ в нем может содержаться только конечное число векторов из $\mathfrak{M}$. Это показывает, что число векторов u, которые мы можем получить в разложении (11) для любых $x \in \mathfrak{M}$, конечно, а это и означает конечность индекса $(\mathfrak{M}:\mathfrak{M}_0)$. Положим $(\mathfrak{M}:\mathfrak{M}_0)=j$. Так как порядок каждого элемента фактор-группы $\mathfrak{M}/\mathfrak{M}_0$ является делителем j, то $jx \in \mathfrak{M}_0$

для любого $x \in \mathfrak{M}$, а значит, x линейно выражается через $\frac{1}{j} e_1, \ldots, \frac{1}{j} e_m$ с целыми коэффициентами. Группа $\mathfrak{M}$ содержится, следовательно, в решетке $\mathfrak{M}^*$ с базисом $\frac{1}{j} e_1, \ldots, \frac{1}{j} e_m$. Применяя теперь теорему 2 из § 2, мы видим, что подгруппа $\mathfrak{M}$ группы $\mathfrak{M}^*$ должна обладать базисом из $l \leqslant m$ векторов $f_1, \ldots, f_l$. Чтобы удостовериться, что $\mathfrak{M}$ является решеткой, нам остается только проверить, что векторы $f_1, \ldots, f_l$ линейно независимы над полем вещественных чисел. Но это следует из того, что через них линейно выражаются m линейно независимых в $\mathbb{R}^n$ векторов $e_1, \ldots, e_m$ (так как $\mathfrak{M}_0 \subset \mathfrak{M}$). Лемма 4 доказана.

3. **Логарифмическое пространство.** Наряду с введенным раньше геометрическим изображением чисел поля K, при котором операция сложения чисел интерпретировалась как операция сложения векторов в $\mathbb{R}^n$, нам нужно другое геометрическое изображение, при котором такую же простую интерпретацию будет иметь операция умножения чисел.

Пусть среди изоморфизмов поля алгебраических чисел K в поле комплексных чисел $\mathbb{C}$ имеется s вещественных и $2t$ комплексных. Будем считать, что они занумерованы так, как это было указано в п. 1.

Рассмотрим вещественное линейное пространство $\mathbb{R}^{s+t}$ размерности $s+t$, состоящее из строчек $(\lambda_1, \ldots, \lambda_{s+t})$ с вещественными компонентами. Для точки $x \in \mathfrak{L}^{s,t}$ вида (2), все компоненты которой отличны от нуля, положим

$$\begin{aligned} l_k(x) &= \ln |x_k| \quad \text{при} \quad k = 1, \ldots, s, \\ l_{s+j}(x) &= \ln |x_{s+j}|^2 \quad \text{при} \quad j = 1, \ldots, t. \end{aligned} \tag{12}$$

Сопоставим, далее, каждой такой точке x из $\mathfrak{L}^{s,t}$ вектор

$$l(x) = (l_1(x), \ldots, l_{s+t}(x)) \tag{13}$$

пространства $\mathbb{R}^{s+t}$. Так как для любых точек x и x' из $\mathfrak{L}^{s,t}$ с отличными от нуля компонентами имеем, очевидно,

$$l_k(xx') = l_k(x) + l_k(x'), \quad 1 \leqslant k \leqslant s+t,$$

то

$$l(xx') = l(x) + l(x'). \tag{14}$$

Все точки $x \in \mathfrak{L}^{s,t}$ вида (2) с отличными от нуля компонентами (т. е. для которых $N(x) \neq 0$) образуют группу относительно покомпонентного умножения. Равенство (14) означает, что отображение $x \to l(x)$ является гомоморфизмом этой мультипликативной группы на аддитивную группу векторов пространства $\mathbb{R}^{s+t}$.

Сопоставляя равенства (12) с определением нормы $N(x)$ точки $x \in \mathfrak{L}^{s,t}$, легко получаем для суммы компонент $l_k(x)$ вектора $l(x)$ формулу

$$\sum_{k=1}^{s+t} l_k(x) = \ln|N(x)|. \tag{15}$$

Пусть теперь α — отличное от нуля число поля K. Положим

$$l(\alpha) = l(x(\alpha)),$$

где $x(\alpha)$ — указанное в п. 1 изображение числа α в пространстве $\mathfrak{L}^{s,t}$. Ввиду (5), (12) и (13) для вектора $l(\alpha)$ подробная запись имеет вид

$$l(\alpha) = (\ln|\sigma_1(\alpha)|, \ldots, \ln|\sigma_s(\alpha)|, \ln|\sigma_{s+1}(\alpha)|^2, \ldots, \ln|\sigma_{s+t}(\alpha)|^2).$$

Вектор $l(\alpha) \in \mathbb{R}^{s+t}$ мы будем называть *логарифмическим изображением числа* $\alpha \neq 0$ из K, а само пространство $\mathbb{R}^{s+t}$ — *логарифмическим пространством поля* K.

Из (7) и (14) вытекает, что

$$l(\alpha\beta) = l(\alpha) + l(\beta), \qquad \alpha \neq 0, \quad \beta \neq 0. \tag{16}$$

Отображение $\alpha \to l(\alpha)$ является, таким образом, гомоморфизмом мультипликативной группы поля K в группу векторов пространства $\mathbb{R}^{s+t}$. Отсюда, в частности, следует, что

$$l(\alpha^{-1}) = -l(\alpha), \quad \alpha \neq 0.$$

Для суммы компонент

$$l_k(\alpha) = l_k(x(\alpha)), \qquad 1 \leqslant k \leqslant s+t,$$

вектора $l(\alpha)$ имеет место формула

$$\sum_{k=1}^{s+t} l_k(\alpha) = \ln|N(\alpha)|. \tag{17}$$

Действительно, сумма слева равна логарифму модуля произведения

$$\sigma_1(\alpha)\ldots\sigma_s(\alpha)\sigma_{s+1}(\alpha)\overline{\sigma_{s+1}(\alpha)}\ldots\sigma_{s+t}(\alpha)\overline{\sigma_{s+t}(\alpha)},$$

а это произведение согласно п. 3 § 2 Дополнения равно норме $N(\alpha)$ (относительно расширения $K/\mathbb{Q}$).

Проведенное нами доказательство формулы (17) (без ссылки на равенство (15)) делает понятным, почему при определении компонент $l_k(x)$ вектора $l(x)$ равенствами (12) делалось различие между компонентами, соответствующими вещественным и комплексным изоморфизмам: компонента $l_{s+j}(x)$ соответствует не одному, а двум сопряженным между собой комплексным изоморфизмам σ_{s+j} и $\overline{\sigma_{s+j}}$.

4. Геометрическое изображение единиц. Пусть теперь $\mathfrak{O}$ — некоторый фиксированный порядок поля K. Рассмотрим в логарифмическом пространстве $\mathbb{R}^{s+t}$ векторы $l(\varepsilon)$ для всех единиц ε кольца $\mathfrak{O}$. Отображение $\varepsilon \to l(\varepsilon)$ не является взаимно однозначным. Действительно, если единица $\eta \in \mathfrak{O}$ является корнем из 1, т. е. $\eta^m = 1$ при некотором натуральном m, то $|\sigma_k(\eta)| = 1$ при всех $k = 1, \ldots, s+t$, а значит, $l(\eta)$ есть нулевой вектор. Таким образом, все корни из 1 (а в порядке $\mathfrak{O}$ их имеется по крайней мере два: $+1$ и -1) изображаются одним и тем же (нулевым) вектором. Чтобы выяснить строение группы единиц порядка $\mathfrak{O}$ при помощи гомоморфизма $\varepsilon \to l(\varepsilon)$, нам надо дать ответы на следующие два вопроса:

1) Какие единицы $\varepsilon \in \mathfrak{O}$ изображаются нулевым вектором?

2) Что представляет собой множество всех векторов $l(\varepsilon)$?

Начнем с первого вопроса. Обозначим через W совокупность всех чисел $\alpha \in \mathfrak{O}$, для которых $l(\alpha) = 0$. Ввиду (16) произведение двух чисел из W также принадлежит W. Так как условие $l(\alpha) = 0$ эквивалентно равенствам

$$|\sigma_k(\alpha)| = 1 \qquad (1 \leqslant k \leqslant s+t),$$

то множество точек $x(\alpha) \in \mathbb{R}^n = \mathfrak{L}^{s,t}$ для всех $\alpha \in W$ ограничено, т. е. оно содержится в некотором шаре $U(r)$. Применяя лемму 1, получаем, что совокупность чисел W конечна. Для произвольного числа $\alpha \in W$ рассмотрим его степени 1, $\alpha, \ldots, \alpha^k, \ldots$ Так как все эти степени содержатся в W, то среди них должны встретиться равные, скажем $\alpha^k = \alpha^l$, $l > k$. Но тогда, полагая $l - k = m$, получаем, что $\alpha^m = 1$. Таким образом, все числа из W являются корнями из 1, а значит, W есть конечная группа, содержащаяся, очевидно, в группе единиц кольца $\mathfrak{O}$.

Поскольку группа W содержит подгруппу второго порядка (состоящую из $+1$ и -1), то она имеет четный порядок. Далее, всякая конечная подгруппа мультипликативной группы поля всегда циклична (см. Дополнение, § 3), поэтому и группа W циклична.

На первый из поставленных вопросов получаем, таким образом, следующий ответ.

Теорема 2. *Единицы ε порядка $\mathfrak{O}$, для которых $l(\varepsilon)$ есть нулевой вектор, образуют конечную циклическую группу четного порядка. Элементами этой группы являются все корни из 1, содержащиеся в $\mathfrak{O}$, и только они.*

Перейдем теперь ко второму вопросу, т. е. займемся выяснением структуры множества $\mathfrak{E}$ в $\mathbb{R}^{s+t}$, состоящего из векторов $l(\varepsilon)$, где ε пробегает все единицы кольца $\mathfrak{O}$.

По теореме 4 § 2 норма всякой единицы ε из $\mathfrak{O}$ равна ± 1, поэтому $\ln|N(\varepsilon)| = 0$. В силу равенства (17) получаем,

следовательно,

$$\sum_{k=1}^{s+t} l_k(\varepsilon) = 0. \tag{18}$$

Это означает, что все точки $l(\varepsilon)$ находятся в подпространстве $\mathfrak{L} \subset \mathbb{R}^{s+t}$, состоящем из точек $(\lambda_1, \ldots, \lambda_{s+t}) \in \mathbb{R}^{s+t}$, для которых $\lambda_1 + \ldots + \lambda_{s+t} = 0$. Размерность подпространства $\mathfrak{L}$ равна, очевидно, $s+t-1$.

Докажем, что $\mathfrak{E}$ — решетка. Так как $\mathfrak{E}$ является, очевидно, подгруппой аддитивной группы векторов пространства $\mathbb{R}^{s+t}$, то ввиду леммы 4 нам надо лишь убедиться в том, что множество точек $\mathfrak{E}$ дискретно. (В качестве ортонормированного базиса в $\mathbb{R}^{s+t}$ мы берем, разумеется, векторы, у которых одна компонента равна единице, а остальные — нулю.) Пусть r — произвольное вещественное положительное число, и пусть $\|l(\varepsilon)\| < r$. Так как $l_k(\varepsilon) \leqslant |l_k(\varepsilon)| \leqslant \|l(\varepsilon)\|$, то $l_k(\varepsilon) < r$ $(1 \leqslant k \leqslant s+t)$, а значит,

$$|\sigma_k(\varepsilon)| < e^r, \quad k = 1, \ldots, s,$$
$$|\sigma_{s+j}(\varepsilon)|^2 < e^r, \quad j = 1, \ldots, t.$$

Отсюда следует, что для тех единиц $\varepsilon \in \mathfrak{O}$, для которых $\|l(\varepsilon)\| < r$, точки $x(\varepsilon)$ из $\mathbb{R}^n$ ограничены. Но так как векторы $x(\alpha) \in \mathbb{R}^n$ для всех $\alpha \in \mathfrak{O}$ образуют решетку (теорема 1), то по лемме 1 число таких единиц ε конечно. Следовательно, число векторов $l(\varepsilon)$ с условием $\|l(\varepsilon)\| < r$ также конечно, а это и значит, что множество $\mathfrak{E}$ дискретно.

Так как решетка $\mathfrak{E}$ содержится в подпространстве $\mathfrak{L}$, то ее размерность не превосходит $s+t-1$.

Нами доказан, таким образом, следующий факт.

Теорема 3. *При геометрическом изображении единиц порядка $\mathfrak{O}$ точками $l(\varepsilon)$ в логарифмическом пространстве $\mathbb{R}^{s+t}$ все эти изображения образуют решетку $\mathfrak{E}$ размерности $r \leqslant s+t-1$.*

5. **Первые сведения о группе единиц.** Уже теоремы 2 и 3, выведенные нами из самых простых геометрических соображений, содержат в себе важную информацию о строении группы единиц любого порядка $\mathfrak{O}$. Именно, из этих теорем легко следует, что в $\mathfrak{O}$ существуют такие единицы $\varepsilon_1, \ldots, \varepsilon_r$, $r \leqslant s+t-1$, что каждая единица $\varepsilon \in \mathfrak{O}$ однозначно представляется в виде

$$\varepsilon = \zeta \varepsilon_1^{a_1} \ldots \varepsilon_r^{a_r}, \tag{19}$$

где $a_1, \ldots, a_r$ — целые рациональные числа, а ζ — некоторый содержащийся в $\mathfrak{O}$ корень из 1. Другими словами, группа единиц порядка $\mathfrak{O}$ представляется в виде произведения одной конечной и r бесконечных циклических групп.

Для доказательства этого утверждения выберем в решетке $\mathfrak{E}$ какой-нибудь базис, скажем $l(\varepsilon_1), \ldots, l(\varepsilon_r)$, и покажем, что еди-

ницы $\varepsilon_1, \ldots, \varepsilon_r$ обладают требуемым свойством. Пусть ε — произвольная единица кольца $\mathfrak{O}$. Так как $l(\varepsilon) \in \mathfrak{E}$, то

$$l(\varepsilon) = a_1 l(\varepsilon_1) + \ldots + a_r l(\varepsilon_r),$$

где a_i — целые рациональные числа. Рассмотрим единицу

$$\zeta = \varepsilon \varepsilon_1^{-a_1} \ldots \varepsilon_r^{-a_r}.$$

В силу формулы (16) для этой единицы имеем $l(\zeta) = l(\varepsilon) - a_1 l(\varepsilon_1) - \ldots - a_r l(\varepsilon_r) = 0$, а значит, по теореме 2 она есть корень из 1. Таким образом, для единицы ε имеем представление (19). Остается доказать его однозначность. Пусть для ε имеем другое представление: $\varepsilon = \zeta' \varepsilon_1^{b_1} \ldots \varepsilon_r^{b_r}$. В силу линейной независимости векторов $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ из равенства $l(\varepsilon) = b_1 l(\varepsilon_1) + \ldots + b_r l(\varepsilon_r)$ следует, что $a_1 = b_1, \ldots, a_r = b_r$. Но тогда имеем также $\zeta = \zeta'$, и наше утверждение доказано полностью.

В доказанном нами утверждении остался нерешенным важный вопрос о точном значении числа r, про которое мы знаем только, что оно не превосходит $s + t - 1$. В следующем параграфе мы покажем, что на самом деле $r = s + t - 1$. Однако сейчас на основании тех методов, которыми мы располагали до сих пор, нельзя даже гарантировать неравенства $r > 0$ (если, конечно, $s + t - 1 > 0$). Равенство $r = s + t - 1$ является, по существу, теоремой существования: оно устанавливает существование $s + t - 1$ независимых единиц. Не удивительно поэтому, что для его доказательства надо привлечь некоторые новые соображения.

Ввиду теоремы 3 утверждение, которое нам осталось доказать, равносильно тому, что размерность решетки $\mathfrak{E}$, изображающей единицы порядка $\mathfrak{O}$ в логарифмическом пространстве, строго равна $s + t - 1$.

Задачи

1. Доказать, что все изображения $x(\alpha) \in \mathbb{R}^n$ чисел α из поля алгебраических чисел K степени n образуют всюду плотное подмножество пространства $\mathbb{R}^n$.

2. Доказать, что если $s \neq 0$, т. е. среди изоморфизмов поля K в поле всех комплексных чисел имеется хоть один вещественный, то группа корней из 1, содержащихся в K, состоит только из двух чисел: $+1$ и -1. (Это обстоятельство всегда имеет место в случае, когда степень поля K нечетная.)

3. Определить все корни из 1, которые могут содержаться в поле алгебраических чисел степени 4.

4. Найти все единицы поля $\mathbb{Q}(\sqrt{3})$.

5. Показать, что в поле $\mathbb{Q}(\theta)$, $\theta^3 = 2$, всякая единица имеет вид $\pm(1 - \theta)^k$.

6. Пусть в поле алгебраических чисел K содержится комплексный корень из 1. Доказать, что тогда норма всякого $\alpha \neq 0$ из K положительна.

§ 4. Группа единиц

1. Критерий полноты решетки. В этом параграфе мы доведем до конца исследование строения группы единиц в порядках полей алгебраических чисел. Основная задача, которую нам предстоит решить, уже обсуждалась в конце предшествующего параграфа. Она заключается в доказательстве того, что решетка $\mathfrak{E}$, векторы которой изображают единицы порядка $\mathfrak{O}$ при логарифмическом изображении, имеет размерность $s+t-1$ (мы сохраняем здесь все обозначения предыдущего параграфа).

Решетка $\mathfrak{E}$ расположена в пространстве $\mathbb{R}^{s+t}$ и содержится в его линейном подпространстве $\mathfrak{L}$, состоящем из точек $(\lambda_1, \ldots, \lambda_{s+t})$, для которых $\lambda_1+\ldots+\lambda_{s+t}=0$. Так как размерность $\mathfrak{L}$ равна $s+t-1$, то наша задача эквивалентна доказательству того, что $\mathfrak{E}$ есть полная решетка пространства $\mathfrak{L}$. Мы докажем это в п. 3, пользуясь следующим критерием полноты решетки.

Теорема 1. *Решетка $\mathfrak{M}$ в линейном пространстве $\mathfrak{L}$ полна тогда и только тогда, когда в $\mathfrak{L}$ существует ограниченное множество U, сдвиги которого на все векторы из $\mathfrak{M}$ полностью заполняют все пространство $\mathfrak{L}$ (возможно, с пересечениями).*

Доказательство. Если решетка $\mathfrak{M}$ полная, то в качестве U можно взять какой-нибудь из ее основных параллелепипедов: согласно лемме 2 § 3 все сдвиги основного параллелепипеда на векторы полной решетки заполняют все пространство (ограниченность основного параллелепипеда очевидна). Пусть теперь решетка $\mathfrak{M}$ неполная, и пусть U — произвольное ограниченное подмножество пространства $\mathfrak{L}$. Покажем, что в этом случае сдвиги множества U на векторы из $\mathfrak{M}$ не могут заполнить всего пространства $\mathfrak{L}$. В силу ограниченности U существует такое вещественное число $r>0$, что $\|u\|<r$ при всех $u\in U$. Обозначим через $\mathfrak{L}'$ подпространство, порожденное векторами решетки $\mathfrak{M}$. Так как решетка $\mathfrak{M}$ неполная, то $\mathfrak{L}'$ есть собственное подпространство, а потому в $\mathfrak{L}$ существуют векторы y сколь угодно большой длины и ортогональные к подпространству $\mathfrak{L}'$ (и, следовательно, ко всем векторам из $\mathfrak{M}$). Утверждаем, что все такие векторы y, для которых $\|y\|\geqslant r$, не могут быть покрыты сдвигами U на векторы из $\mathfrak{M}$. Действительно, если вектор y (ортогональный к $\mathfrak{L}'$) содержится в некотором сдвиге, то это значит, что он имеет вид $y=u+z$, где $u\in U$, $z\in\mathfrak{M}$. Но тогда ввиду неравенства Коши — Буняковского будем иметь

$$\|y\|^2=(y, y)=(y, u)\leqslant\|y\|\|u\|<r\|y\|,$$

откуда $\|y\|<r$. Теорема 1, таким образом, доказана. (Геометрический смысл проведенного доказательства состоит в том, что все сдвиги множества U на векторы неполной решетки лежат в слое, состоящем из точек, расстояния которых до подпространства $\mathfrak{L}'$ не превышают r.)

Замечание. В топологических терминах полнота решетки $\mathfrak{M}$ в пространстве $\mathfrak{L}$ равносильна, как легко видеть, компактности фактор-группы $\mathfrak{L}/\mathfrak{M}$ (если $\mathfrak{L}$ рассматривать как топологическую группу относительно сложения).

2. Лемма Минковского. Наше доказательство существования $s+t-1$ независимых единиц будет основываться на одном простом геометрическом утверждении, которое имеет, однако, исключительно много приложений в теории чисел. Формулировка и доказательство этого утверждения (теорема 3) используют понятие объема в n-мерном пространстве и некоторые его свойства.

Объем $v(X)$ множества X в n-мерном пространстве $\mathbb{R}^n$ может быть определен как кратный интеграл

$$v(X) = \int\limits_{(X)} \dots \int dx_1 dx_2 \dots dx_n,$$

распространенный по этому множеству X. (Здесь мы несколько отступаем от обозначения (4) § 3 и координаты точки $x \in \mathbb{R}^n$ записываем в виде $(x_1, \dots, x_n)$.) Мы не будем заниматься исследованием условий, при которых объем существует. В интересующих нас случаях множество X будет задаваться несколькими неравенствами с весьма простыми входящими в них функциями и вопрос о существовании объема будет решаться элементарным образом. Отметим несколько простейших свойств объема, легко вытекающих из свойств интегралов (предполагается, что все встречающиеся объемы существуют).

1) Если X содержится в X', то $v(X) \leqslant v(X')$.

2) Если множества X и X' не пересекаются, то

$$v(X \cup X') = v(X) + v(X').$$

3) При сдвиге множества его объем сохраняется, т. е.

$$v(X+z) = v(X).$$

4) Пусть α — вещественное положительное число. Обозначим через αX совокупность точек вида αx, где x пробегает все точки из X. (Множество αX называется растяжением X в α раз.) Тогда

$$v(\alpha X) = \alpha^n v(X).$$

Вычислим объем основного параллелепипеда T полной решетки $\mathfrak{M}$ в $\mathbb{R}^n$, построенного на некотором ее базисе $e_1, \dots, e_n$. Пусть

$$e_j = (a_{1j}, \dots, a_{nj}), \qquad 1 \leqslant j \leqslant n.$$

Мы покажем, что тогда

$$v(T) = |\det(a_{ij})|. \tag{1}$$

Сделаем в интеграле $v(T) = \int\limits_{(T)} \dots \int dx_1 \dots dx_n$ замену переменных

по формулам

$$x_i = \sum_{j=1}^{n} a_{ij} x_j', \quad 1 \leqslant i \leqslant n.$$

Якобиан этого преобразования равен, очевидно, определителю $\det(a_{ij})$, который отличен от нуля ввиду линейной независимости векторов $e_1, \ldots, e_n$. Так как при нашем преобразовании множество T перейдет, как легко видеть, в множество T_0, состоящее из точек $(x_1', \ldots, x_n')$, для которых $0 \leqslant x_i' < 1$ $(i = 1, \ldots, n)$, то

$$v(T) = \int\limits_{(T_0)} \ldots \int |\det(a_{ij})| \, dx_1' \ldots dx_n' = |\det(a_{ij})| \int\limits_0^1 \ldots \int\limits_0^1 dx_1' \ldots dx_n' =$$

$$= |\det(a_{ij})|,$$

и формула (1) доказана.

Подвергнем пространство $\mathbb{R}^n$ некоторому линейному неособенному преобразованию $x \to x'$. Решетка $\mathfrak{M}$ перейдет при этом преобразовании в некоторую (очевидно, полную) решетку $\mathfrak{M}'$, а ее основной параллелепипед T — в основной параллелепипед T' решетки $\mathfrak{M}'$. Ясно, что параллелепипед T' будет построен на образах $e_1', \ldots, e_n'$ векторов базиса $e_1, \ldots, e_n$. Если $e_j' = (b_{1j}, \ldots, b_{nj})$ $(1 \leqslant j \leqslant n)$, то по доказанному объем $v(T')$ равен $|\det(b_{ij})|$. Обозначим через $C = (c_{ij})$ матрицу линейного преобразования $x \to x'$ в базисе $e_1, \ldots, e_n$, так что

$$e_j' = \sum_{i=1}^{n} c_{ij} e_i, \quad 1 \leqslant j \leqslant n.$$

Легко видеть, что $b_{ij} = \sum_{s=1}^{n} a_{is} c_{sj}$, т. е. матрица (b_{ij}) является произведением (a_{ij}) на (c_{ij}), а значит, имеет место формула

$$v(T') = v(T) \cdot |\det C|. \tag{2}$$

Предположим теперь, что $e_1, \ldots, e_n$ и $e_1', \ldots, e_n'$ — два базиса одной и той же решетки $\mathfrak{M}$. Так как эти базисы связаны между собой унимодулярным преобразованием (с целочисленной матрицей C определителя ± 1), то ввиду (2) получаем, что $v(T') = v(T)$. Этим показано, что объем основного параллелепипеда базиса решетки зависит только от самой решетки и не зависит от выбора в ней базиса.

Сопоставление формулы (1) с равенствами (9) и (10) § 3 приводит нас к следующему уточнению теоремы 1 § 3:

Теорема 2. *При геометрическом изображении чисел поля K степени $n = s + 2t$ точками пространства $\mathfrak{L}^{s,t} = \mathbb{R}^n$ все точки, изображающие числа полного модуля M с дискриминантом D,*

образуют полную решетку, объем основного параллелепипеда которой равен $2^{-t}\sqrt{|D|}$.

Для формулировки основного предложения этого пункта нам нужны еще два геометрических понятия.

Множество $X \subset \mathbb{R}^n$ называется *центрально симметричным*, если вместе с любой точкой x в этом множестве содержится и симметричная ей относительно начала точка $-x$.

Множество X называется *выпуклым*, если для любых двух точек $x \in X$ и $x' \in X$ в этом множестве содержатся и все точки вида $\alpha x + (1-\alpha)x'$, где α — вещественное число, удовлетворяющее условию $0 \leqslant \alpha \leqslant 1$. Другими словами, множество X выпукло, если всякий отрезок, соединяющий две точки из X, целиком содержится в этом множестве.

Теорема 3 (лемма Минковского о выпуклом теле). *Пусть в* n*-мерном вещественном пространстве* $\mathbb{R}^n$ *задана полная решетка* $\mathfrak{M}$, *объем основного параллелепипеда которой равен* Δ, *и ограниченное центрально симметричное выпуклое множество* X *с объемом* $v(X)$. *Если* $v(X) > 2^n\Delta$, *то множество* X *содержит по крайней мере одну отличную от начала точку решетки* $\mathfrak{M}$.

Доказательство. Мы будем основываться на следующем интуитивно ясном предложении: если ограниченное множество точек $Y \subset \mathbb{R}^n$ таково, что все его сдвиги $Y_z = Y + z$ на векторы $z \in \mathfrak{M}$ попарно не пересекаются, то $v(Y) \leqslant \Delta$. Для доказательства выберем некоторый основной параллелепипед T решетки $\mathfrak{M}$ и рассмотрим пересечения $Y \cap T_{-z}$ множества Y со всеми сдвигами $T_{-z} = T - z$ параллелепипеда T. Очевидно, что

$$v(Y) = \sum_{z \in \mathfrak{M}} v(Y \cap T_{-z})$$

(в этой формально бесконечной сумме только конечное число членов отлично от нуля, так как ограниченное множество Y может пересекаться лишь с конечным числом параллелепипедов T_{-z}; лемма 3 § 3). Сдвиг множества $Y \cap T_{-z}$ на вектор z равен, очевидно, $Y_z \cap T$, поэтому $v(Y \cap T_{-z}) = v(Y_z \cap T)$, а значит,

$$v(Y) = \sum_{z \in \mathfrak{M}} v(Y_z \cap T).$$

Если теперь сдвиги Y_z попарно не пересекаются, то пересечения $Y_z \cap T$ также попарно не пересекаются, а так как все они содержатся в T, то сумма в правой части последнего равенства не может быть больше $v(T)$. Следовательно, $v(Y) \leqslant v(T)$, и наше утверждение доказано.

Рассмотрим теперь множество $\frac{1}{2}X$ (получающееся из X сжатием в два раза). Из условий теоремы следует, что $v\left(\frac{1}{2}X\right) =$

$= \frac{1}{2^n} v(X) > \Delta$. Если бы все сдвиги $\frac{1}{2} X + z$ на векторы $z \in \mathfrak{M}$ попарно не пересекались, то по доказанному мы должны были бы иметь $v\left(\frac{1}{2} X\right) \leqslant \Delta$, что на самом деле не так. Следовательно, для некоторых различных векторов z_1 и z_2 из $\mathfrak{M}$ множества $\frac{1}{2} X + z_1$ и $\frac{1}{2} X + z_2$ имеют общую точку:

$$\frac{1}{2} x' + z_1 = \frac{1}{2} x'' + z_2, \quad x', x'' \in X.$$

Перепишем последнее равенство в виде

$$z_1 - z_2 = \frac{1}{2} x'' - \frac{1}{2} x'.$$

Так как множество X центрально симметрично, то $-x' \in X$; ввиду его выпуклости имеем также

$$\frac{1}{2} x'' - \frac{1}{2} x' = \frac{1}{2} x'' + \frac{1}{2} (-x') \in X.$$

Таким образом, отличная от начала точка $z_1 - z_2$ из $\mathfrak{M}$ принадлежит множеству X, а это и требовалось доказать.

Из рассуждений первой части доказательства теоремы 3 легко вытекает также следующее довольно очевидное утверждение (оно понадобится нам в § 5).

Лемма 1. *Если все сдвиги множества Y на векторы решетки $\mathfrak{M}$ полностью покрывают пространство $\mathbb{R}^n$, то $v(Y) \geqslant \Delta$.*

Действительно, в этом случае пересечения $Y_z \cap T$ полностью покроют основной параллелепипед T (возможно, с пересечениями), а потому $v(Y) = \sum\limits_{z \in \mathfrak{M}} v(Y_z \cap T) \geqslant v(T) = \Delta$.

При исследовании группы единиц лемма Минковского будет применяться нами к решетке в пространстве $\mathfrak{L}^{s,t}$ и к телу X, которое состоит из тех точек x вида (2) § 3, для которых

$$|x_1| < c_1, \ldots, |x_s| < c_s; \quad |x_{s+1}|^2 < c_{s+1}, \ldots, |x_{s+t}|^2 < c_{s+t},$$

где $c_1, \ldots, c_{s+t}$ — вещественные положительные числа. Выпуклость и центральная симметричность этого тела X очевидна. Вычислим его объем. Используя для координат точки x обозначения (4) § 3, получаем

$$v(X) = \int\limits_{-c_1}^{c_1} dx_1 \ldots \int\limits_{-c_s}^{c_s} dx_s \iint\limits_{y_1^2 + z_1^2 < c_{s+1}} dy_1 dz_1 \ldots \iint\limits_{y_t^2 + z_t^2 < c_{s+t}} dy_t dz_t =$$

$$= 2^s \pi^t \prod_{i=1}^{s+t} c_i.$$

Применение леммы Минковского к рассмотренному телу X дает нам следующий результат (именно на него мы и будем в дальнейшем ссылаться).

Теорема 4. *Если объем основного параллелепипеда полной решетки $\mathfrak{M}$ пространства $\mathfrak{L}^{s,t}$ равен Δ и если вещественные положительные числа $c_1, \ldots, c_{s+t}$ таковы, что* $\prod_{i=1}^{s+t} c_i > \left(\frac{4}{\pi}\right)^t \Delta$, *то в решетке $\mathfrak{M}$ имеется ненулевой вектор $x = (x_1, \ldots, x_{s+t})$, для которого*

$$|x_1| < c_1, \ldots, |x_s| < c_s; \ |x_{s+1}|^2 < c_{s+1}, \ldots, |x_{s+t}|^2 < c_{s+t}. \quad (3)$$

3. Структура группы единиц. Теперь мы можем до конца решить вопрос о строении группы единиц произвольного порядка.

Теорема 5 (теорема Дирихле). *В произвольном порядке $\mathfrak{O}$ поля алгебраических чисел K степени $n = s + 2t$ существуют такие единицы $\varepsilon_1, \ldots, \varepsilon_r$, $r = s + t - 1$, что каждая единица $\varepsilon \in \mathfrak{O}$ однозначно представляется в виде*

$$\varepsilon = \zeta \varepsilon_1^{a_1} \ldots \varepsilon_r^{a_r},$$

где $a_1, \ldots, a_r$ — целые рациональные числа, а ζ — некоторый содержащийся в $\mathfrak{O}$ корень из 1.

Доказательство. Как уже говорилось в конце предшествующего и в начале этого параграфа, нам надо лишь установить полноту решетки $\mathfrak{E}$, изображающей единицы порядка $\mathfrak{O}$, в пространстве $\mathfrak{L}$ (размерность которого равна $s + t - 1$). Согласно теореме 1 для этого, в свою очередь, достаточно убедиться в том, что в $\mathfrak{L}$ существует ограниченное подмножество U, сдвиги которого на все векторы из $\mathfrak{E}$ заполняют все пространство $\mathfrak{L}$.

Так как норма всякого целого числа из K есть целое рациональное число, то ввиду формулы (17) § 3 для отличных от нуля чисел α из $\mathfrak{O}$ точки $l(\alpha)$ расположены в полупространстве $\lambda_1 + \ldots + \lambda_{s+t} \geqslant 0$ пространства $\mathbb{R}^{s+t}$. При этом, если $|N(\alpha)| < Q$ при некотором вещественном числе $Q > 1$, то точка $l(\alpha)$ будет находиться в полосе, определяемой неравенствами

$$0 \leqslant \lambda_1 + \ldots + \lambda_{s+t} < \ln Q.$$

Обозначим через $\mathfrak{T}$ гиперплоскость в $\mathbb{R}^{s+t}$, определяемую уравнением $\lambda_1 + \ldots + \lambda_{s+t} = \ln Q$. Ясно, что $\mathfrak{T}$ получается из подпространства $\mathfrak{L}$ сдвигом, например, на вектор $\frac{\ln Q}{s+t}(1, \ldots, 1)$.

Для всякого отличного от нуля α из $\mathfrak{O}$, для которого $|N(\alpha)| < Q$, через Y_α обозначим совокупность всех точек $(\lambda_1, \ldots, \lambda_{s+t})$ гиперплоскости $\mathfrak{T}$, для которых

$$\lambda_k > l_k(\alpha), \quad k = 1, \ldots, s + t.$$

Так как наряду с последними неравенствами мы имеем также

$$\lambda_k = \ln Q - \sum_{i \neq k} \lambda_i < \ln Q - \sum_{i \neq k} l_i(\alpha),$$

то все множества Y_α ограничены. Далее, из формулы (16) § 3 легко следует, что для всякой единицы ε кольца $\mathfrak{O}$ справедлива формула

$$Y_{\alpha\varepsilon} = Y_\alpha + l(\varepsilon), \tag{4}$$

т. е. множество $Y_{\alpha\varepsilon}$ получается из Y_α сдвигом на вектор $l(\varepsilon)$.

Покажем, что если Q выбрано достаточно большим, а именно

$$Q > \left(\frac{4}{\pi}\right)^t \Delta, \tag{5}$$

где Δ — объем основного параллелепипеда решетки в $\mathfrak{L}^{s,t}$, изображающей числа рассматриваемого порядка $\mathfrak{O}$, то множества Y_α (для $\alpha \in \mathfrak{O}$, $\alpha \neq 0$ $|N(\alpha)| < Q$) покрывают всю гиперплоскость $\mathfrak{T}$. В самом деле, пусть $(\lambda_1^0, \ldots, \lambda_{s+t}^0)$ — произвольная точка из $\mathfrak{T}$, и пусть $c_1, \ldots, c_{s+t}$ — вещественные положительные числа, для которых $\lambda_k^0 = \ln c_k$. Ввиду (5) числа c_k удовлетворяют неравенству $c_1 \ldots c_{s+t} > \left(\frac{4}{\pi}\right)^t \Delta$, поэтому согласно теореме 4 в порядке $\mathfrak{O}$ существует число $\alpha \neq 0$, для которого

$$|\sigma_k(\alpha)| < c_k, \quad k = 1, \ldots, s,$$
$$|\sigma_{s+j}(\alpha)|^2 < c_{s+j}, \quad j = 1, \ldots, t.$$

В других обозначениях последние неравенства могут быть переписаны в виде

$$l_k(\alpha) < \lambda_k^0 \quad (k = 1, \ldots, s+t).$$

Мы получили, таким образом, что точка $(\lambda_1^0, \ldots, \lambda_{s+t}^0)$ принадлежит множеству Y_α, причем $|N(\alpha)| < Q$.

По теореме 5 § 2 в порядке $\mathfrak{O}$ существует только конечное число попарно не ассоциированных чисел, нормы которых по абсолютной величине меньше Q. Зафиксируем какую-нибудь систему $\alpha_1, \ldots, \alpha_N$ отличных от нуля чисел из $\mathfrak{O}$, обладающую тем свойством, что всякое $\alpha \neq 0$ из $\mathfrak{O}$, для которого $|N(\alpha)| < Q$, ассоциировано с одним из них, т. е. $\alpha = \alpha_i \varepsilon$ при некотором i $(1 \leqslant i \leqslant N)$ и некоторой единице ε кольца $\mathfrak{O}$. Положим

$$Y = \bigcup_{i=1}^{N} Y_{\alpha_i}.$$

Так как все Y_α покрывают $\mathfrak{T}$ и $Y_\alpha = Y_{\alpha_i} + l(\varepsilon)$ (формула (4)), то сдвиги ограниченного множества Y на все векторы $l(\varepsilon)$ решетки $\mathfrak{E}$ покроют всю гиперплоскость $\mathfrak{T}$. Но в таком случае сдвиги

содержащегося в $\mathfrak{L}$ подмножества

$$U = Y - \frac{\ln Q}{s+t}(1, \ldots, 1)$$

на векторы $l(\varepsilon) \in \mathfrak{E}$ (для всех единиц ε из $\mathfrak{O}$) покроют все подпространство $\mathfrak{L}$, а это, как уже было сказано, и доказывает теорему 5.

Как уже отмечалось в п. 5 § 3, теорема Дирихле означает, что группа единиц всякого порядка $\mathfrak{O}$ в поле алгебраических чисел степени $n = s + 2t$ представляется в виде прямого произведения одной конечной и $s+t-1$ бесконечных циклических групп.

Если $s+t=1$ (а это имеет место лишь для поля рациональных чисел и мнимого квадратичного поля), то $r=0$. В этом случае решетка $\mathfrak{E}$ состоит только из нулевого вектора, а группа единиц порядка $\mathfrak{O}$ исчерпывается конечной группой корней из 1.

Единицы $\varepsilon_1, \ldots, \varepsilon_r$, существование которых устанавливается теоремой Дирихле, называются *основными единицами порядка* $\mathfrak{O}$. Из рассуждений, проведенных в п. 5 § 3, ясно, что единицы $\varepsilon_1, \ldots, \varepsilon_r$ являются основными тогда и только тогда, когда векторы $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ образуют базис решетки $\mathfrak{E}$. Отсюда легко следует, что единицы

$$\varepsilon_i' = \zeta_i \varepsilon_1^{a_{i1}} \ldots \varepsilon_r^{a_{ir}}, \quad 1 \leqslant i \leqslant r$$

(где ζ_i — произвольные содержащиеся в $\mathfrak{O}$ корни из 1) будут также основными в том и только в том случае, если целочисленная матрица (a_{ij}) унимодулярна.

Замечание. Изложенное доказательство теоремы Дирихле не является эффективным в том смысле, что оно не дает алгоритма для отыскания какой-либо системы основных единиц порядка $\mathfrak{O}$. Эта неэффективность вызвана тем, что в наших рассуждениях участвовала полная система неассоциированных чисел $\alpha_1, \ldots, \alpha_N$, нормы которых не превосходят некоторого числа Q. Существование же такой системы чисел доказано нами неэффективно (теорема 5 § 2), как об этом уже говорилось. К вопросам эффективности мы вернемся в следующем параграфе.

Теорема Дирихле (так же, как и теорема 2 § 3) справедлива, разумеется, и для максимального порядка $\widetilde{\mathfrak{O}}$ поля K. Основные единицы максимального порядка $\widetilde{\mathfrak{O}}$ называют также *основными единицами поля алгебраических чисел* K.

4. **Регулятор.** Согласно построениям пп. 3 и 4 § 3 с каждым порядком $\mathfrak{O}$ поля алгебраических чисел K степени $n = s + 2t$ связывается решетка $\mathfrak{E}$ размерности $r = s+t-1$ в подпространстве $\mathfrak{L} \subset \mathbb{R}^{s+t}$. Объем v основного параллелепипеда этой решетки не зависит от выбора в ней базиса, а значит, он вполне определен самим порядком $\mathfrak{O}$. Вычислим этот объем. Пусть T_0 — основной параллелепипед решетки $\mathfrak{E}$, построенный на базисе

$l(\varepsilon_1), \ldots, l(\varepsilon_r)$ (здесь $\varepsilon_1, \ldots, \varepsilon_r$ — система основных единиц порядка $\mathfrak{O}$). Вектор

$$l_0 = \frac{1}{\sqrt{s+t}}(1, \ldots, 1) \in \mathbb{R}^{s+t},$$

очевидно, ортогонален к подпространству $\mathfrak{L}$ и имеет единичную длину. Ясно, что r-мерный объем $v = v(T_0)$ равен $(s+t)$-мерному объему параллелепипеда T, построенного на векторах l_0, $l(\varepsilon_1), \ldots, l(\varepsilon_r)$. Поэтому в силу формулы (1) объем v равен абсолютной величине определителя, строчки которого составлены из компонент этих векторов. Если в последнем определителе мы все столбцы прибавим к столбцу с номером i, а затем, воспользовавшись свойством (18) § 3, разложим его по этому столбцу, то получим

$$v = \sqrt{s+t}\,\mathrm{R},$$

где R — абсолютная величина одного из миноров r-го порядка матрицы

$$\begin{pmatrix} l_1(\varepsilon_1) & \ldots & l_{s+t}(\varepsilon_1) \\ \ldots & \ldots & \ldots \\ l_1(\varepsilon_r) & \ldots & l_{s+t}(\varepsilon_r) \end{pmatrix}. \tag{6}$$

Из наших рассуждений вытекает, в частности, что все миноры r-го порядка последней матрицы по абсолютной величине равны между собой и не зависят от выбора системы основных единиц $\varepsilon_1, \ldots, \varepsilon_r$. Число R (так же, как и v) зависит, следовательно, только от $\mathfrak{O}$. Оно называется *регулятором порядка* $\mathfrak{O}$.

Регулятор максимального порядка $\tilde{\mathfrak{O}}$ называется также *регулятором поля алгебраических чисел* K. (Для поля рациональных чисел и мнимого квадратичного поля регулятор, по определению, равен 1.)

Задачи

1. Доказать, что неравенство $v(X) > 2^n\Delta$ в лемме Минковского нельзя заменить более слабым. Для этого построить выпуклое ограниченное центрально симметричное множество X с объемом $v(X) = 2^n\Delta$, не содержащее, кроме начала, никаких других точек решетки.

2. Пусть a — вещественное положительное число. Доказать, что объем множества $X \subset \mathfrak{L}^{s,t}$, состоящего из точек x, для которых

$$|x_1| + \ldots + |x_s| + 2\sqrt{y_1^2+z_1^2} + \ldots + 2\sqrt{y_t^2+z_t^2} < a$$

(в координатах (4) § 3), равен

$$v(X) = 2^s\left(\frac{\pi}{2}\right)^t \frac{1}{n!}a^n.$$

Проверить, далее, что множество X ограничено, центрально симметрично и выпукло.

3. Пусть a и b — натуральные числа, не являющиеся квадратами. Показать, что основная единица порядка $\{1, \sqrt{a}\}$ поля $\mathbb{Q}(\sqrt{a})$ является также и основной единицей порядка $\{1, \sqrt{a}, \sqrt{-b}, \sqrt{a}\sqrt{-b}\}$ в поле $\mathbb{Q}(\sqrt{a}, \sqrt{-b})$.

4. Показать, что группа единиц произвольного порядка $\mathfrak{O}$ является подгруппой конечного индекса в группе единиц максимального порядка $\tilde{\mathfrak{O}}$.

5. Пусть единицы $\eta_1, \ldots, \eta_r$ $(r = s + t - 1)$ порядка $\mathfrak{O}$ таковы, что векторы $l(\eta_1), \ldots, l(\eta_r)$ линейно независимы. Показать, что тогда группа, состоящая из единиц вида $\eta_1^{c_1} \ldots \eta_r^{c_r}$ с целыми рациональными c_i, является подгруппой конечного индекса в группе всех единиц порядка $\mathfrak{O}$.

6. Пусть $c_1, \ldots, c_n$ — вещественные положительные числа и (a_{ij}) — вещественная неособенная матрица порядка n. Доказать, что если $c_1 \ldots c_n > d = |\det(a_{ij})|$, то существуют такие целые рациональные $x_1, \ldots, x_n$, не равные нулю одновременно, что

$$\left|\sum_{j=1}^{n} a_{ij}x_j\right| < c_i, \qquad i = 1, \ldots, n.$$

Указание. Убедиться, что в пространстве $\mathbb{R}^n$ множество точек $(x_1, \ldots, x_n)$, удовлетворяющих последним неравенствам, ограничено, центрально симметрично, выпукло и имеет объем $\frac{1}{d} 2^n c_1 \ldots c_n$. Применить затем лемму Минковского о выпуклом теле.

7. Пусть a_{ij} $(1 \leqslant i \leqslant k, \quad 1 \leqslant j \leqslant n)$ — целые рациональные и m_i $(1 \leqslant i \leqslant k)$ — натуральные числа. Доказать, что в пространстве $\mathbb{R}^n$ совокупность целочисленных точек $(x_1, \ldots, x_n)$, для которых

$$\sum_{j=1}^{n} a_{ij}x_j \equiv 0 \pmod{m_i}, \qquad 1 \leqslant i \leqslant k,$$

образует полную решетку, объем основного параллелепипеда которой не превосходит $m_1 \ldots m_k$.

8. Пусть a, b, c — отличные от нуля целые рациональные числа, попарно взаимно простые и свободные от квадратов, и пусть $|abc| = 2^\lambda p_1 \ldots p_s$ (p_i — нечетные простые числа, λ равно 0 или 1). Предположим, что форма $ax^2 + by^2 + cz^2$ представляет нуль во всех полях p-адических чисел. Доказать, что тогда существуют такие целочисленные линейные формы $L_1, \ldots, L_s, L', L''$ от трех переменных, что для целых u, v и w будет выполняться сравнение

$$au^2 + bv^2 + cw^2 \equiv 0 \pmod{4|abc|},$$

если только

$$\begin{aligned} &L_i(u, v, w) \equiv 0 \pmod{p_i}, \quad 1 \leqslant i \leqslant s, \\ &L'(u, v, w) \equiv 0 \pmod{2^{1+\lambda}}, \\ &L''(u, v, w) \equiv 0 \pmod{2}. \end{aligned} \qquad (*)$$

9. Сохраним условия предшествующей задачи и обозначим через $\mathfrak{M}$ решетку целочисленных точек $(u, v, w) \in \mathbb{R}^3$, удовлетворяющих сравнениям $(*)$. Согласно задаче 7 объем основного параллелепипеда решетки $\mathfrak{M}$ не превосходит $4|abc|$. Обозначим, далее, через X эллипсоид

$$|a|x^2 + |b|y^2 + |c|z^2 < 4|abc|,$$

объем которого, как легко подсчитать, равен $\frac{32}{3}\pi|abc|$. Применив к решет-

ке $\mathfrak{M}$ и эллипсоиду X лемму Минковского о выпуклом теле, доказать, что форма $ax^2 + by^2 + cz^2$ представляет нуль рационально. (В этом доказательстве теоремы Минковского — Хассе для форм от трех переменных не использован факт неопределенности формы.)

§ 5. Решение задачи о представлениях рациональных чисел полными разложимыми формами

1. Единицы с нормой +1. В § 2 п. 3 мы видели, что для решения задачи о нахождении в некотором полном модуле чисел с заданной нормой имеют значение лишь те единицы ε его кольца множителей $\mathfrak{O}$, для которых $N(\varepsilon) = +1$. Такие единицы, очевидно, также образуют группу. Займемся изучением структуры этой группы.

Предположим сначала, что степень n поля K нечетная. В этом случае в кольце $\mathfrak{O}$ имеется только два корня из 1, а именно ± 1 (задача 2 § 3). Если для некоторой единицы $\varepsilon \in \mathfrak{O}$ мы имеем $N(\varepsilon) = -1$, то

$$N(-\varepsilon) = N(-1)N(\varepsilon) = (-1)^n(-1) = 1.$$

Пусть $\varepsilon_1, \ldots, \varepsilon_r$ $(r = s + t - 1)$ — произвольная система основных единиц кольца $\mathfrak{O}$. Может случиться, что среди ε_i имеются единицы с нормой -1. Заменяя все такие единицы ε_i на $-\varepsilon_i$, мы получим, очевидно, новую систему основных единиц $\eta_1, \ldots, \eta_r$, причем для них будем уже иметь $N(\eta_i) = 1$ при всех $i = 1, \ldots, r$. Норма произвольной единицы $\varepsilon = \pm \eta_1^{a_1} \ldots \eta_r^{a_r}$ будет равна теперь $N(\pm 1) = (\pm 1)^n = \pm 1$. Следовательно, все единицы $\varepsilon \in \mathfrak{O}$, для которых $N(\varepsilon) = 1$, имеют вид

$$\varepsilon = \eta_1^{a_1} \ldots \eta_r^{a_r}, \quad a_i \in \mathbb{Z}.$$

Пусть теперь n — четное число. Покажем, что в этом случае норма всякого корня из 1, содержащегося в K, равна $+1$. Для корней ± 1 это очевидно. Если в K содержится комплексный корень ζ из 1, то $s = 0$, а значит, все изоморфизмы поля K в поле комплексных чисел разбиваются на пары сопряженных между собой комплексных изоморфизмов и для каждой такой пары σ и $\bar{\sigma}$ имеем $\sigma(\zeta)\bar{\sigma}(\zeta) = |\sigma(\zeta)|^2 = 1$. Согласно доказанному в п. 3 § 2 Дополнения получаем, следовательно, что $N(\zeta) = 1$, и наше утверждение доказано.

Пусть опять $\varepsilon_1, \ldots, \varepsilon_r$ — произвольная система основных единиц кольца $\mathfrak{O}$. Если $N(\varepsilon_i) = 1$ при всех $i = 1, \ldots, r$, то в этом случае норма всякой единицы $\varepsilon \in \mathfrak{O}$ будет равна $+1$. Предположим теперь, что

$$N(\varepsilon_1) = 1, \ \ldots, \ N(\varepsilon_k) = 1, \quad N(\varepsilon_{k+1}) = -1, \ \ldots, \ N(\varepsilon_r) = -1,$$

где $k < r$. Полагая

$$\eta_1 = \varepsilon_1, \ \ldots, \ \eta_k = \varepsilon_k, \quad \eta_{k+1} = \varepsilon_{k+1}\varepsilon_r, \ \ldots, \ \eta_{r-1} = \varepsilon_{r-1}\varepsilon_r,$$

мы получаем новую систему основных единиц $\eta_1, \ldots, \eta_{r-1}, \varepsilon_r$, причем $N(\eta_i) = 1$ $(1 \leqslant i \leqslant r-1)$. Посмотрим, при каком условии норма единицы $\varepsilon = \zeta\eta_1^{a_1} \ldots \eta_{r-1}^{a_{r-1}}\varepsilon_r^b$ $(a_1, \ldots, a_{r-1}, b \in \mathbb{Z})$ равна $+1$. Так как $N(\varepsilon) = (-1)^b$, то $N(\varepsilon) = +1$ тогда и только тогда, когда показатель b четный, т. е. $b = 2a_r$. Мы получили, таким образом, что при четном n произвольная единица $\varepsilon \in \mathfrak{O}$ с нормой $+1$ имеет вид (в случае существования единицы с нормой -1)

$$\varepsilon = \zeta\eta_1^{a_1} \ldots \eta_{r-1}^{a_{r-1}}\eta_r^{a_r}, \qquad a_i \in \mathbb{Z},$$

где $\eta_r = \varepsilon_r^2$, а ζ — произвольный содержащийся в $\mathfrak{O}$ корень из 1.

Итак, если в порядке $\mathfrak{O}$ известна система основных единиц, то мы можем найти также и все единицы с нормой $+1$.

2. **Общий вид решений уравнения $N(\mu) = a$.** Сопоставляя вместе следствие теоремы 5 § 2 с результатом п. 1, приходим к следующему утверждению, дающему нам полное представление о совокупности решений уравнения (7) § 2.

Теорема 1. *Пусть M — полный модуль в поле алгебраических чисел K степени $n = s + 2t$, $\mathfrak{O}$ — его кольцо множителей и a — отличное от нуля рациональное число. В порядке $\mathfrak{O}$ существуют такие единицы $\eta_1, \ldots, \eta_r$ $(r = s + t - 1)$ с нормой $+1$, а в модуле M — такая конечная (возможно, и пустая) система чисел $\mu_1, \ldots, \mu_k$ с нормой a, что всякое решение $\mu \in M$ уравнения*

$$N(\mu) = a \tag{1}$$

однозначно представляется в виде

$$\mu = \mu_i\eta_1^{a_1} \ldots \eta_r^{a_r} \quad \textit{при} \quad n \quad \textit{нечетном},$$

$$\mu = \mu_i\zeta\eta_1^{a_1} \ldots \eta_r^{a_r} \quad \textit{при} \quad n \quad \textit{четном}.$$

Здесь μ_i — одно из чисел $\mu_1, \ldots, \mu_k$, ζ — корень из 1 и $a_1, \ldots, a_r$ — целые рациональные числа.

Взяв в случае четного n совокупность всех произведений $\mu_i\zeta$ за новую систему чисел μ_i, мы получим и в этом случае для решений μ представление в таком же виде, как и при нечетном n.

Во всяком порядке мнимого квадратичного поля существует лишь конечное число единиц (так как $r = s + t - 1 = 0$). Следовательно, в этом случае уравнение (1) имеет не более конечного числа решений. Если же K отлично от мнимого квадратичного поля (и, конечно, от поля рациональных чисел), то $r > 0$ и, следовательно, уравнение (1) либо вообще не имеет решений, либо имеет их бесконечно много.

Замечание. Теорема 1 указывает нам, каким является многообразие решений уравнения (1), однако она не дает способа, как все эти решения на самом деле найти. Для практического решения уравнения (1) мы должны иметь эффективный способ нахождения системы основных единиц порядка $\mathfrak{O}$ и полного набора

в модуле M попарно не ассоциированных чисел $\mu_1, \ldots, \mu_k$ с данной нормой. В следующих пунктах мы покажем, что обе эти задачи действительно могут быть решены в конечное число действий. Следует, однако, предупредить, что излагаемый в пп. 3 и 4 общий метод эффективного построения основных единиц и чисел модуля с данной нормой мало пригоден для практического использования ввиду чрезвычайно большого объема необходимых вычислений. Нашей целью является лишь доказательство принципиальной возможности провести построение в конечное число шагов. В ряде конкретных примеров, используя дополнительные соображения и учитывая специфику данного частного случая, обычно удается найти более простой путь. Так, в § 7 в качестве примера мы изложим довольно простой способ решения наших задач для случая квадратичных полей.

Здесь стоит отметить, что не всегда для заданного семейства диофантовых уравнений существует алгоритм, с помощью которого можно было бы найти решения любого из уравнений семейства или хотя бы ответить на вопрос, существуют ли решения. В свое время подразумевалось, что для диофантовых уравнений должен существовать способ, позволяющий при помощи конечного числа операций установить, разрешимо ли заданное уравнение в целых рациональных числах. Задача отыскания такого способа и составила содержание известной 10-й проблемы Гильберта (1900 г.). Однако в 1970 г. Ю. В. Матиясевич установил, что эта проблема имеет отрицательное решение, т. е. не существует алгоритма (в точном математическом его понимании), который позволял бы по произвольному диофантову уравнению узнавать, имеет ли оно решение в целых числах. Более того, можно построить однопараметрическое диофантово уравнение от 22 переменных, для которого нельзя указать алгоритм, отвечающий (при каждом значении параметра) на вопрос, существуют целочисленные решения или нет. Доступное изложение решения 10-й проблемы Гильберта можно найти в статье [18].

3. Эффективное построение системы основных единиц. Обозначая через $\sigma_1, \ldots, \sigma_n$ все изоморфизмы поля алгебраических чисел K в поле комплексных чисел, докажем предварительно следующую лемму.

Лемма 1. *Пусть $c_1, \ldots, c_n$ — произвольные вещественные положительные числа. В каждом полном модуле M поля K существует только конечное число чисел α, для которых*

$$|\sigma_1(\alpha)| < c_1, \ \ldots, \ |\sigma_n(\alpha)| < c_n, \tag{2}$$

и все эти числа α могут быть эффективно перечислены.

Доказательство. Выберем в M какой-нибудь базис $\alpha_1, \ldots, \alpha_n$ (если модуль M задан системой образующих, не являющейся базисом, то, следуя доказательству теоремы 1 § 2, мы можем в конечное число шагов построить также и базис M).

Всякое число α из M может быть представлено тогда в виде

$$\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n \tag{3}$$

с целыми рациональными a_j. Построим для базиса $\alpha_1, \ldots, \alpha_n$ взаимный базис $\alpha_1^*, \ldots, \alpha_n^*$ поля K (см. Дополнение, § 2, п. 3) и найдем вещественное число $A > 0$, для которого

$$|\sigma_i(\alpha_j^*)| \leqslant A \tag{4}$$

при всех i и j. Умножая (3) на α_j^* и переходя к следу, мы получим

$$a_j = \mathrm{Sp}\,\alpha\alpha_j^* = \sum_{i=1}^{n} \sigma_i(\alpha)\,\sigma_i(\alpha_j^*).$$

Если теперь $\alpha \in M$ удовлетворяет условию (2), то ввиду (4) для коэффициентов a_j получаем оценку

$$|a_j| \leqslant A\sum_{i=1}^{n} |\sigma_i(\alpha)| < A\sum_{i=1}^{n} c_i. \tag{5}$$

Для целых a_j мы имеем, следовательно, лишь конечное число значений. Выписав все числа вида (3) с условием (5), мы легко выделим из них те, которые удовлетворяют неравенствам (2).

В дальнейшем до конца этого параграфа мы будем пользоваться теми же понятиями и обозначениями, что и в двух предшествующих параграфах.

Возможность эффективного построения системы основных единиц в произвольном порядке поля алгебраических чисел основывается на следующей теореме.

Теорема 2. *Для каждого порядка $\mathfrak{O}$ поля алгебраических чисел K может быть указано такое вещественное число $\rho > 0$, что в шаре радиуса ρ логарифмического пространства $\mathbb{R}^{s+t}$ обязательно содержится хоть один базис решетки $\mathfrak{E}$* (изображающей единицы порядка $\mathfrak{O}$).

Покажем, что эта теорема действительно дает нам метод построения основных единиц порядка $\mathfrak{O}$. Если логарифмическое изображение $l(\varepsilon)$ единицы $\varepsilon \in \mathfrak{O}$ содержится в шаре радиуса ρ, то

$$|\sigma_k(\varepsilon)| < e^{\rho} \quad (1 \leqslant k \leqslant s), \qquad |\sigma_{s+j}(\varepsilon)| < e^{\rho/2}, \quad 1 \leqslant j \leqslant t. \tag{6}$$

По лемме 1 число единиц $\varepsilon \in \mathfrak{O}$, удовлетворяющих этому условию, конечно, и все они на самом деле могут быть выписаны (для выделения единиц среди чисел порядка $\mathfrak{O}$ следует воспользоваться теоремой 4 § 2). Из найденных единиц составим всевозможные системы $\varepsilon_1, \ldots, \varepsilon_r$ по $r = s + t - 1$ единиц, для которых векторы $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ линейно независимы. Согласно теореме 2 хоть одна из этих систем будет системой основных единиц порядка $\mathfrak{O}$. Чтобы узнать — какая именно, следует для каждой системы $\varepsilon_1, \ldots$

..., ε_r вычислить объем параллелепипеда, построенного на векторах $l(\varepsilon_1), \ldots, l(\varepsilon_r)$. Та система, для которой этот объем наименьший, и будет, очевидно, системой основных единиц.

Доказательство теоремы 2 очевидным образом вытекает из нижеследующих двух лемм, относящихся к решетке $\mathfrak{E}$. При их доказательстве следует помнить, что мы всегда можем перечислить все точки этой решетки, находящиеся в заданном ограниченном множестве. Для этого нужно заметить, что ограничения координат точки $l(\varepsilon)$ дают ограничения типа (6) для единицы ε, а все такие единицы, согласно лемме 1, мы можем перечислить. Вообще мы будем говорить, что решетка $\mathfrak{M}$ нам задана эффективно, если известен алгоритм для перечисления всех ее точек, находящихся в заданном ограниченном множестве.

Лемма 2. *Если полная решетка $\mathfrak{M}$ в m-мерном пространстве $\mathbb{R}^m$ задана эффективно и если известен объем Δ ее основного параллелепипеда, то можно указать такое число ρ, что среди векторов $x \in \mathfrak{M}$, лежащих в шаре радиуса ρ, находится базис решетки $\mathfrak{M}$.*

Доказательство. Если $m = 1$, то можно положить $\rho = 2\Delta$. В общем случае доказательство леммы проведем индукцией по m. Выберем в $\mathbb{R}^m$ какое-нибудь ограниченное, центрально симметричное и выпуклое тело, объем которого больше, чем $2^m\Delta$. Согласно лемме Минковского (§ 4, п. 2) в этом теле имеются ненулевые векторы решетки $\mathfrak{M}$. Выберем среди них такой вектор u, что $u \neq nx$ ни при каком $x \in \mathfrak{M}$ и целом $n > 1$. Обозначим через $\mathfrak{L}'$ подпространство, ортогональное к вектору u, и через $\mathfrak{M}'$ — проекцию решетки $\mathfrak{M}$ на $\mathfrak{L}'$. Если $x' \in \mathfrak{M}'$, то при некотором $x \in \mathfrak{M}$ имеем $x = \xi u + x'$ с вещественным ξ. Для любого целого k вектор $x - ku$ также принадлежит $\mathfrak{M}$, поэтому вектор x из $\mathfrak{M}$ (с данной проекцией x') мы можем выбрать так, чтобы $|\xi| < 1/2$. Для такого x будем иметь

$$\|x\|^2 = \xi^2\|u\|^2 + \|x'\|^2 \leqslant \frac{1}{4}\|u\|^2 + \|x'\|^2.$$

Это неравенство показывает, что все векторы $x' \in \mathfrak{M}'$ из ограниченной области являются проекциями векторов $x \in \mathfrak{M}$ также из ограниченной области, а значит, вместе с $\mathfrak{M}$ решетка $\mathfrak{M}'$ задана нам эффективно. Если $u_2, \ldots, u_m$ — векторы из $\mathfrak{M}$, проекции которых $u_2, \ldots, u_m$ образуют базис $\mathfrak{M}'$, то система $u, u_2, \ldots, u_m$, как легко видеть, будет базисом $\mathfrak{M}$. Отсюда следует, что объем основного параллелепипеда решетки $\mathfrak{M}'$ равен $\Delta/\|u\|$ и, значит, тоже нам известен. По индуктивному предположению мы можем найти такое число ρ', что в $\mathfrak{M}'$ имеется базис $u_2, \ldots, u_m$, для которого $\|u_i\| < \rho'$ $(i = 2, \ldots, m)$. По доказанному векторы $u_2, \ldots, u_m$ из $\mathfrak{M}$ можно выбрать так, чтобы

$$\|u_i\| < \left(\frac{1}{4}\|u\|^2 + \rho'^2\right)^{1/2}.$$

Таким образом, в шаре радиуса

$$\rho = \max\left(\|u\| + 1, \left(\frac{1}{4}\|u\|^2 + \rho'^2\right)^{1/2}\right)$$

для решетки $\mathfrak{M}$ имеется базис $u, u_2, \ldots, u_m$, а это и составляет утверждение леммы 2.

Для доказательства теоремы 2 нам достаточно теперь оценить сверху объем основного параллелепипеда решетки $\mathfrak{E}$.

Лемма 3. *Объем v основного параллелепипеда решетки $\mathfrak{E}$ удовлетворяет неравенству*

$$v \leqslant C(\ln Q)^{s+t-1} N \leqslant C(\ln Q)^{s+t-1} \sum_{a<Q} a^n,$$

где $Q = \left(\frac{2}{\pi}\right)^t \sqrt{|D|} + 1$ (D — *дискриминант порядка* $\mathfrak{O}$), N — *число попарно не ассоциированных чисел* $\alpha \neq 0$ *порядка* $\mathfrak{O}$, *для которых* $|N(\alpha)| < Q$, *и* C — *некоторая константа, зависящая только от* $s+t$ (*а пробегает все натуральные числа, меньшие* Q).

Доказательство. Воспользуемся здесь обозначениями доказательства теоремы 5 § 4. Так как $|D| = 2^t\Delta$ (теорема 2 § 4), то указанное в лемме число Q удовлетворяет неравенству (5) § 4. Все сдвиги подмножества U в $\mathfrak{L}$ на векторы решетки $\mathfrak{E}$ заполняют $\mathfrak{L}$, поэтому согласно лемме 1 § 4 имеем

$$v \leqslant v(U). \tag{7}$$

Множество U получено из Y параллельным переносом. Далее, Y есть объединение подмножеств Y_{α_i} (лежащих в гиперплоскости $\mathfrak{T}$). Отсюда следует, что

$$v(U) = v(Y) \leqslant \sum_{i=1}^{N} v(Y_{\alpha_i}). \tag{8}$$

Займемся вычислением $(s+t-1)$-мерного объема тела Y_α ($\alpha \in \mathfrak{O}$, $\alpha \neq 0$, $|N(\alpha)| = a < Q$). Это тело определяется условиями: $\lambda_1 + \ldots + \lambda_{s+t} = \ln Q$, $\lambda_k > l_k(\alpha)$ $(1 \leqslant k \leqslant s+t)$. Подвергнем его сдвигу на вектор $-l(\alpha)$. Так как $l_1(\alpha) + \ldots + l_{s+t}(\alpha) = \ln a$, то при таком сдвиге тело Y_α перейдет в тело X, которое определяется условиями: $\lambda_1 + \ldots + \lambda_{s+t} = \ln\frac{Q}{a}$ и $\lambda_k > 0$ $(1 \leqslant k \leqslant s+t)$. Обозначим через C объем тела X_0, определяемого условиями: $\lambda_1 + \ldots + \lambda_{s+t} = 1$ и $\lambda_k > 0$ $(1 \leqslant k \leqslant s+t)$. Ясно, что C зависит только от $s+t$. Тело X получается из X_0 растяжением в $\ln(Q/a)$ раз. Следовательно,

$$v(Y_\alpha) = v(X) = C\left(\ln\frac{Q}{a}\right)^{s+t-1}. \tag{9}$$

Неравенства (7) и (8) в сочетании с формулой (9) приводят нас к первому неравенству леммы. Для доказательства второго нера-

венства остается лишь заметить, что в кольце $\mathfrak{O}$ существует не более a^n попарно не ассоциированных чисел, нормы которых по абсолютной величине равны a (см. доказательство теоремы 5 § 2).

4. Числа модуля с данной нормой. Обратимся теперь к вопросу об эффективном построении в модуле полного набора попарно не ассоциированных чисел с данной нормой.

Зафиксируем в кольце множителей $\mathfrak{O}$ полного модуля M какую-нибудь систему основных единиц $\varepsilon_1, \ldots, \varepsilon_r$. Векторы $l(\varepsilon_1), \ldots, l(\varepsilon_r)$ вместе с вектором $l_0 = (1, \ldots, 1)$ образуют базис логарифмического пространства $\mathbb{R}^{s+t}$, поэтому для всякого $\mu \in M$ вектор $l(\mu)$ может быть представлен в виде

$$l(\mu) = \xi l_0 + \sum_{i=1}^{r} \xi_i l(\varepsilon_i) \tag{10}$$

с вещественными коэффициентами $\xi, \xi_1, \ldots, \xi_r$. Ввиду формул (17) и (18) § 3 для коэффициента ξ имеем формулу

$$\xi = \frac{1}{s+t} \ln |N(\mu)|.$$

Каждое вещественное число ξ_i мы можем представить в виде $\xi_i = k_i + \gamma_i$, где k_i — целое и $|\gamma_i| \leqslant 1/2$. Для ассоциированного с μ числа $\mu' = \mu\varepsilon_1^{-k_1} \ldots \varepsilon_r^{-k_r}$ разложение (10) имеет вид

$$l(\mu') = \frac{\ln a}{s+t} l_0 + \gamma_1 l(\varepsilon_1) + \ldots + \gamma_r l(\varepsilon_r),$$

где $a = |N(\mu)| = |N(\mu')|$. Мы получили, таким образом, что в $\mathbb{R}^{s+t}$ имеется ограниченное множество, обладающее тем свойством, что для всякого $\mu \in M$ с условием $|N(\mu)| = a$ существует ассоциированное с ним число μ', логарифмическое изображение которого содержится в этом множестве. Для чисел μ' мы имеем, следовательно, оценки типа (2). Согласно лемме 1 мы можем явно выписать все числа из M, для которых имеют место эти оценки. Выделяя из них все числа с заданным значением нормы $N(\mu')$ и оставляя затем для ассоциированных между собой чисел только по одному представителю, мы и получим, очевидно, систему попарно не ассоциированных чисел $\mu_1, \ldots, \mu_k$ из M с данной нормой, обладающую тем свойством, что всякое $\mu \in M$ с той же нормой ассоциировано с одним из них.

Результаты этого параграфа указывают нам, таким образом, метод, с помощью которого в конечное число операций можно найти в полном модуле все числа с данной нормой (или установить их отсутствие). Тем самым нами до конца решена также задача о целочисленных представлениях рациональных чисел полными разложимыми формами.

Задачи

1. Пусть в целое рациональное число d, свободное от квадратов, входит по крайней мере одно простое число вида $4k+3$. Доказать, что тогда норма всякой единицы порядка $\{1, \sqrt{d}\}$ поля $\mathbb{Q}(\sqrt{d})$ равна $+1$.

2. Показать, что $5+2\sqrt{6}$ является основной единицей в максимальном порядке поля $\mathbb{Q}(\sqrt{6})$.

3. Найти все целочисленные решения неопределенного уравнения $3x^2-4y^2=11$.

4. Показать, что в кубическом поле $\mathbb{Q}(\theta)$, $\theta^3=6$, число $\varepsilon=1-6\theta+3\theta^2$ является основной единицей.

§ 6. Классы модулей

В связи с той ролью, которую играет понятие модуля в рассматриваемых нами вопросах, важно составить себе более полное представление о многообразии всех полных модулей данного поля алгебраических чисел K. Число всех таких модулей, очевидно, бесконечно. Среди них имеются, однако, модули, свойства которых очень близки друг к другу. Это подобные модули, определенные в § 1, п. 3. Мы видели, что подобные модули имеют одно и то же кольцо множителей (лемма 1 § 2) и что задачи нахождения чисел с заданной нормой в подобных модулях эквивалентны (§ 1, п. 3). Ввиду этого естественно объединить все подобные модули в один класс и исследовать множество классов подобных модулей. В этом параграфе мы докажем, что в поле алгебраических чисел K существует только конечное число классов подобных модулей, имеющих заданный порядок $\mathfrak{O}$ своим кольцом множителей. Этот результат, как и теорема Дирихле о единицах, принадлежит к числу самых основных фактов теории алгебраических чисел. Доказательство его, как и доказательство теоремы о единицах, основывается на лемме Минковского о выпуклом теле. Другим важным вспомогательным средством будет понятие нормы модуля.

1. Норма модуля. Рассмотрим произвольный полный модуль M в поле алгебраических чисел K степени n и через $\mathfrak{O}$ обозначим его кольцо множителей. Выберем в $\mathfrak{O}$ какой-нибудь базис $\omega_1, \ldots, \omega_n$ и в модуле M — базис $\mu_1, \ldots, \mu_n$. Матрица перехода $A=(a_{ij})$ от первого базиса ко второму, т. е. матрица, определяемая равенствами

$$\mu_j=\sum_{i=1}^{n} a_{ij}\omega_i, \qquad 1\leqslant j\leqslant n, \quad a_{ij}\in\mathbb{Q}, \tag{1}$$

зависит, конечно, не только от модуля M, но и от выбора базисов ω_i и μ_j. Пусть $\omega_1', \ldots, \omega_n'$ и $\mu_1', \ldots, \mu_n'$ — другая пара базисов модулей $\mathfrak{O}$ и M соответственно, и пусть

$$\mu_j'=\sum_{i=1}^{n} a_{ij}'\omega_i', \qquad a_{ij}'\in\mathbb{Q}.$$

Матрица $A_1 = (a'_{ij})$ связана с матрицей A соотношением

$$A_1 = CAD, \tag{2}$$

где $C = (c_{ij})$ и $D = (d_{ij})$ — целочисленные унимодулярные матрицы, определяемые равенствами:

$$\omega_j = \sum_{i=1}^{n} c_{ij}\omega'_i, \qquad \mu'_j = \sum_{i=1}^{n} d_{ij}\mu_i, \qquad c_{ij}, d_{ij} \in \mathbb{Z}$$

(матрица перехода от одного базиса модуля к другому всегда, как мы знаем, унимодулярна). Таким образом, с модулем M инвариантно связанными будут только такие выражения от элементов матрицы A, которые инвариантны при замене A на A_1 по формуле (2). Полной системой таких инвариантов являются так называемые инвариантные множители рациональной матрицы A. Мы будем рассматривать простейший из них — абсолютную величину определителя $\det A$. Его инвариантность очевидна:

$$|\det A_1| = |\det C| \cdot |\det A| \cdot |\det D| = |\det A|.$$

Определение. *Пусть M — полный модуль в K и $\mathfrak{O}$ — его кольцо множителей. Абсолютная величина определителя матрицы перехода от базиса кольца $\mathfrak{O}$ к базису модуля M называется нормой модуля M и обозначается через $N(M)$.*

Согласно формуле (12) § 2 Дополнения дискриминанты $D = D(\mu_1, \ldots, \mu_n)$ и $D_0 = D(\omega_1, \ldots, \omega_n)$ базисов μ_i и ω_i (т. е. дискриминанты модулей M и $\mathfrak{O}$, см. п. 5 § 2) связаны между собой соотношением $D = D_0(\det A)^2$. Введенное понятие нормы позволяет переписать эту формулу в виде

$$D = D_0 N(M)^2. \tag{3}$$

Для модулей, содержащихся в своем кольце множителей, матрица (a_{ij}), определенная разложениями (1), очевидно, целочисленна, а потому норма таких модулей является целым числом. Смысл нормы модуля в этом случае выясняется следующей теоремой.

Теорема 1. *Если полный модуль M содержится в своем кольце множителей $\mathfrak{O}$, то его норма $N(M)$ равна индексу $(\mathfrak{O} : M)$.*

Эта теорема является частным случаем следующего утверждения.

Лемма 1. *Если M_0 — абелева группа без элементов конечного порядка ранга n, а M — ее подгруппа того же ранга n, то индекс $(M_0 : M)$ конечен и равен абсолютной величине определителя матрицы перехода A от какого-нибудь базиса M_0 к произвольному базису M.*

Доказательство. Пусть $\omega_1, \ldots, \omega_n$ — произвольный базис M_0. Согласно теореме 2 § 2 в подгруппе M существует базис

$\eta_1, \ldots, \eta_n$ вида

$$\begin{aligned}\eta_1 &= c_{11}\omega_1 + c_{12}\omega_2 + \ldots + c_{1n}\omega_n,\\ \eta_2 &= \qquad c_{22}\omega_2 + \ldots + c_{2n}\omega_n,\\ &\ldots\ldots\ldots\ldots\\ \eta_n &= \qquad\qquad\qquad c_{nn}\omega_n,\end{aligned}$$

где c_{ij} целые рациональные и $c_{ii} > 0$ $(1 \leqslant i \leqslant n)$. Очевидно, что $|\det A|$ не зависит от выбора базисов в M_0 и в M, поэтому

$$|\det A| = c_{11}c_{22}\ldots c_{nn}.$$

Рассмотрим элементы

$$x_1\omega_1 + \ldots + x_n\omega_n, \qquad 0 \leqslant x_i < c_{ii}, \quad 1 \leqslant i \leqslant n \tag{4}$$

и покажем, что они образуют полную систему представителей из классов смежности группы M_0 по подгруппе M. Пусть $\alpha = a_1\omega_1 + \ldots + a_n\omega_n$ — произвольный элемент из M_0. Разделим a_1 на c_{11} с остатком: $a_1 = c_{11}q_1 + x_1$, $0 \leqslant x_1 < c_{11}$. Тогда

$$\alpha - q_1\eta_1 - x_1\omega_1 = a_2'\omega_2 + \ldots + a_n'\omega_n.$$

Если теперь мы разделим a_2' на c_{22} с остатком: $a_2' = c_{22}q_2 + x_2$, $0 \leqslant x_2 < c_{22}$, то будем иметь

$$\alpha - q_1\eta_1 - q_2\eta_2 - x_1\omega_1 - x_2\omega_2 = a_3''\omega_3 + \ldots + a_n''\omega_n.$$

Повторяя этот процесс n раз, мы придем в конце концов к равенству

$$\alpha - q_1\eta_1 - \ldots - q_n\eta_n - x_1\omega_1 - \ldots - x_n\omega_n = 0,$$

в котором q_i и x_i целые рациональные, причем $0 \leqslant x_i < c_{ii}$. Так как $q_1\eta_1 + \ldots + q_n\eta_n$ принадлежит M, то последнее равенство означает, что α и элемент $x_1\omega_1 + \ldots + x_n\omega_n$ вида (4) принадлежат одному и тому же классу смежности по подгруппе M. Этим доказано, что в каждом классе смежности M_0 по M имеется представитель вида (4). Остается еще проверить, что различные элементы вида (4) содержатся в разных классах смежности. Допуская противное, предположим, что разность двух различных элементов $x_1\omega_1 + \ldots + x_n\omega_n$ и $x_1'\omega_1 + \ldots + x_n'\omega_n$ из системы (4) принадлежит M. Обозначим через s наименьший индекс $(1 \leqslant s \leqslant n)$, для которого $x_s \neq x_s'$. Тогда

$$(x_s - x_s')\omega_s + \ldots + (x_n - x_n')\omega_n = b_1\eta_1 + \ldots + b_n\eta_n$$

с целыми b_i. Подставляя сюда вместо $\eta_1, \ldots, \eta_n$ их выражения через ω_i и сравнивая коэффициенты при ω_i в обеих частях равенства, легко находим последовательно, что $b_1 = 0, \ldots, b_{s-1} = 0$ и, далее, что $c_{ss}b_s = x_s - x_s'$. Последнее равенство, однако, при це-

лом b_s невозможно, так как $0 < |x_s - x'_s| < c_{ss}$. Таким образом, элементы (4) действительно образуют полную систему представителей из классов смежности M_0 по M. Так как их число конечно и равно $c_{11}c_{22}\dots c_{nn} = |\det A|$, то лемма 1 и теорема 1 доказаны.

Теорема 2. *Нормы подобных полных модулей M и αM связаны между собой соотношением*

$$N(\alpha M) = |N(\alpha)|N(M).$$

В частности, для модулей, подобных порядку $\mathfrak{O}$, имеем

$$N(\alpha\mathfrak{O}) = |N(\alpha)|.$$

Доказательство. Если $\mu_1, \dots, \mu_n$ — базис M, то в качестве базиса для αM можно взять числа $\alpha\mu_1, \dots, \alpha\mu_n$. Норма числа $N(\alpha)$ есть определитель матрицы перехода C от базиса μ_i к базису $\alpha\mu_i$ (см. Дополнение, § 2, п. 2). Согласно лемме 1 § 2 модули M и αM имеют одно и то же кольцо множителей $\mathfrak{O}$. Обозначим через A и A_1 матрицы перехода от базиса кольца $\mathfrak{O}$ к базисам μ_i и $\alpha\mu_i$ соответственно. Тогда $A_1 = AC$, и мы получаем

$$N(\alpha M) = |\det A_1| = |\det A| \cdot |\det C| = N(M)|N(\alpha)|.$$

Второе утверждение теоремы следует из того, что $N(\mathfrak{O}) = 1$.

2. Конечность числа классов. Мы переходим к доказательству основной теоремы этого параграфа. Оно будет опираться на две леммы.

Лемма 2. *Для любого полного модуля M_1 в поле K и любого его полного подмодуля M_2 существует только конечное число промежуточных модулей M (т. е. модулей, удовлетворяющих условию $M_1 \supset M \supset M_2$).*

Доказательство. Выберем какую-нибудь систему представителей $\xi_1, \dots, \xi_s$, $s = (M_1 : M_2)$, в классах смежности M_1 по подгруппе M_2. Если $\alpha_1, \dots, \alpha_n$ — базис M_2, то каждый элемент $\theta \in M_1$ однозначно представляется в виде $\theta = \xi_k + c_1\alpha_1 + \dots + c_n\alpha_n$, где ξ_k — некоторый из представителей а $c_1, \dots, c_n$ — целые рациональные числа. Пусть $\theta_1, \dots, \theta_n$ — базис промежуточного модуля M. Для каждого θ_j мы имеем представление $\theta_j = \xi_{kj} + c_{1j}\alpha_1 + \dots + c_{nj}\alpha_n$ с целыми c_{ij}. Поэтому

$$M = \{\theta_1, \dots, \theta_n\} = \{\theta_1, \dots, \theta_n, \alpha_1, \dots, \alpha_n\} =$$
$$= \{\xi_{k_1}, \dots, \xi_{k_n}, \alpha_1, \dots, \alpha_n\}.$$

Так как для наборов представителей $\xi_{k_1}, \dots, \xi_{k_n}$ мы имеем лишь конечное число возможностей, то, следовательно, число промежуточных модулей M также конечно.

Следствие. *Для любого полного модуля $M_0 \subset K$ и любого натурального числа r в поле K существует лишь конечное число модулей M, содержащих M_0, для которых $(M : M_0) = r$.*

Действительно, ввиду конечности фактор-группы M/M_0 имеем $rM \subset M_0$, а следовательно, $\frac{1}{r} M_0 \supset M \supset M_0$.

Лемма 3. *В полном модуле M дискриминанта D поля алгебраических чисел K степени $n = s + 2t$ существует отличное от нуля число α, норма которого удовлетворяет неравенству*

$$|N(\alpha)| \leqslant (2/\pi)^t \sqrt{|D|}. \tag{5}$$

Доказательство. Выберем положительные вещественные числа $c_1, \ldots, c_{s+t}$ так, чтобы

$$c_1 \ldots c_{s+t} = (2/\pi)^t \sqrt{|D|} + \varepsilon, \tag{6}$$

где ε — произвольное положительное вещественное число. Из теорем 2 и 4 § 4 следует, что в модуле M существуют числа $\alpha \neq 0$, удовлетворяющие условиям:

$$|\sigma_k(\alpha)| < c_k \quad (1 \leqslant k \leqslant s), \quad |\sigma_{s+j}(\alpha)|^2 < c_{s+j}, \quad 1 \leqslant j \leqslant t.$$

Норма

$$N(\alpha) = \sigma_1(\alpha) \ldots \sigma_s(\alpha) |\sigma_{s+1}(\alpha)|^2 \ldots |\sigma_{s+t}(\alpha)|^2$$

таких чисел по абсолютной величине не превосходит, очевидно, произведения (6). Так как это верно при любом сколь угодно малом ε, то в M должны быть также числа $\alpha \neq 0$, удовлетворяющие неравенству (5).

Теорема 3. *Для всякого порядка $\mathfrak{O}$ поля алгебраических чисел K существует только конечное число классов подобных модулей, для которых $\mathfrak{O}$ является кольцом множителей.*

Доказательство. Пусть M — произвольный модуль, имеющий порядок $\mathfrak{O}$ в качестве кольца множителей. Обозначим через D дискриминант модуля M и через D_0 дискриминант порядка $\mathfrak{O}$. Выберем в модуле M число $\alpha \neq 0$ с условием (5). Ввиду формулы (3) условие (5) можно переписать в виде

$$|N(\alpha)| \leqslant (2/\pi)^t N(M) \sqrt{|D_0|}.$$

Так как $\alpha\mathfrak{O} \subset M$, то $\mathfrak{O} \subset \frac{1}{\alpha} M$. Кроме того, в силу леммы 1 и определения нормы модуля мы имеем

$$\left(\frac{1}{\alpha} M : \mathfrak{O}\right) = N\left(\frac{1}{\alpha} M\right)^{-1} = \frac{|N(\alpha)|}{N(M)} \leqslant \left(\frac{2}{\pi}\right)^t \sqrt{|D_0|}.$$

Этим доказано, что в каждом классе подобных модулей с кольцом множителей $\mathfrak{O}$ имеется модуль M', для которого

$$M' \supset \mathfrak{O}, \qquad (M' : \mathfrak{O}) \leqslant \left(\frac{2}{\pi}\right)^t \sqrt{|D_0|}. \tag{7}$$

По следствию леммы 2 в поле K имеется вообще только конечное число модулей M' с условием (7). Следовательно, число классов

подобных модулей с кольцом множителей $\mathfrak{O}$ также конечно, и теорема 3 доказана.

Замечание. Для любых двух полных модулей M_1 и M_2 поля алгебраических чисел K мы можем вполне эффективно решить вопрос о том, подобны они или нет. Для этого прежде всего находим их кольца множителей. Если эти кольца окажутся различными, то M_1 и M_2 не подобны. Пусть M_1 и M_2 имеют одно и то же кольцо множителей $\mathfrak{O}$. Заменяя, быть может, один из наших модулей подобным ему, мы можем добиться выполнения включения $M_1 \supset M_2$. Вычислим индекс $(M_1 : M_2) = a$. Если $\alpha M_1 = M_2$, то $\alpha \in \mathfrak{O}$ и $|N(\alpha)| = a$. Найдем поэтому в кольце $\mathfrak{O}$ полный набор попарно не ассоциированных чисел $\alpha_1, \ldots, \alpha_k$, норма которых по абсолютной величине равна a (согласно п. 4 § 5 система таких чисел находится эффективно). Если α — произвольное число кольца $\mathfrak{O}$, для которого $|N(\alpha)| = a$, то оно ассоциировано с некоторым α_i, а поэтому $\alpha M_1 = \alpha_i M_1$. Для решения вопроса о подобии модулей M_1 и M_2 нам надо, следовательно, сравнить модуль M_2 с модулями $\alpha_i M_1$ $(1 \leqslant i \leqslant k)$. Модули M_1 и M_2 будут подобны тогда и только тогда, когда M_2 совпадает с некоторым $\alpha_i M_1$.

Задачи

1. Показать, что в любом поле алгебраических чисел, отличном от поля рациональных чисел, имеется бесконечно много порядков. (Следовательно, число всех классов подобных модулей, принадлежащих всевозможным порядкам, бесконечно.)

2. Используя задачу 2 § 4, доказать, что в полном модуле M с дискриминантом D существует число $\alpha \neq 0$, для которого

$$|N(\alpha)| \leqslant \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|D|}$$

$(n = s + 2t$ — степень поля алгебраических чисел).

3. Применяя задачу 2 к максимальному порядку поля алгебраических чисел K степени $n = s + 2t$ и используя формулу Стирлинга

$$n! = \sqrt{2\pi n}(n/e)^n e^{\theta/(12n)}, \qquad 0 < \theta < 1,$$

показать, что дискриминант D_0 поля K удовлетворяет неравенству

$$|D_0| > \left(\frac{\pi}{4}\right)^{2t} \frac{1}{2\pi n} e^{2n - 1/6n}.$$

Таким образом, с возрастанием степени n дискриминант поля алгебраических чисел по абсолютной величине стремится к бесконечности.

4. Показать, что дискриминант всякого поля алгебраических чисел степени $n > 1$ отличен от ± 1 (теорема Минковского).

5. Доказать, что существует лишь конечное число полей алгебраических чисел с заданным значением дискриминанта (теорема Эрмита).

Указание. В силу задачи 3 достаточно показать, что существует лишь конечное число полей K фиксированной степени $n = s + 2t$ с данным дискриминантом D_0. Рассмотреть в пространстве $\mathbb{R}^n$ (состоящем из точек $(x_1, \ldots, x_s, y_1, z_1, \ldots, y_t, z_t)$) множество X, определяемое в случае $s > 0$

условиями

$$|x_1| < \sqrt{|D_0|+1}, \qquad |x_k| < 1, \qquad 2 \leqslant k \leqslant s,$$
$$y_j^2 + z_j^2 < 1, \qquad 1 \leqslant j \leqslant t,$$

а в случае $s = 0$ условиями

$$|y_1| < 1/2, \quad |z_1| < \sqrt{|D_0|+1}, \quad y_j^2 + z_j^2 < 1, \quad 2 \leqslant j \leqslant t.$$

Применяя к множеству X и к решетке, изображающей числа максимального порядка $\widetilde{\mathfrak{O}}$, лемму Минковского о выпуклом теле, показать, что в K существует примитивное число $\theta \in \widetilde{\mathfrak{O}}$, для которого характеристический многочлен имеет ограниченные коэффициенты.

§ 7. Представление чисел бинарными квадратичными формами

В этом параграфе мы займемся несколько более детальным изучением вопросов этой главы для случая бинарных квадратичных форм. Так как всякая рациональная неприводимая форма $ax^2 + bxy + cy^2$ разлагается на линейные множители в некотором квадратичном поле, то наша задача связана с изучением полных модулей и их колец множителей в квадратичных полях.

1. Квадратичные поля. *Квадратичным полем* называется всякое расширение поля рациональных чисел $\mathbb{Q}$ второй степени. Займемся прежде всего описанием этого наиболее простого класса полей алгебраических чисел.

Пусть $d \neq 1$ — свободное от квадратов целое рациональное число (положительное или отрицательное). Так как многочлен $t^2 - d$ неприводим над полем рациональных чисел, то поле $\mathbb{Q}(\theta)$, полученное из $\mathbb{Q}$ присоединением корня θ этого многочлена, имеет степень 2 над $\mathbb{Q}$, т. е. является квадратичным полем. Мы его будем обозначать в дальнейшем через $\mathbb{Q}(\sqrt{d})$.

Легко видеть, что и, обратно, каждое квадратичное поле K имеет только что указанный вид. Докажем это. Если α принадлежит K и не рационально, то, очевидно, $K = \mathbb{Q}(\alpha)$. Минимальный многочлен для α над $\mathbb{Q}$ имеет степень 2, поэтому при некоторых рациональных p и q имеем $\alpha^2 + p\alpha + q = 0$. Положим $\beta = \alpha + \frac{p}{2}$; тогда $\beta^2 = \frac{p^2}{4} - q$. Рациональное число $\frac{p^2}{4} - q$ можно представить в виде $c^2 d$, где d целое и свободное от квадратов. Ясно, что $d \neq 1$, ибо в противном случае β, а вместе с ним и α были бы рациональными. Если теперь $\theta = \beta/c$, то $\theta^2 = d$ и $K = \mathbb{Q}(\theta)$, т.е. $K = \mathbb{Q}(\sqrt{d})$.

Покажем, что для различных целых d (отличных от 1 и свободных от квадратов) поля $\mathbb{Q}(\sqrt{d})$ различны. Действительно, если $\mathbb{Q}(\sqrt{d'}) = \mathbb{Q}(\sqrt{d})$, то $\sqrt{d'} = x + y\sqrt{d}$ при некоторых рациональных x и y, откуда

$$d' = x^2 + dy^2 + 2xy\sqrt{d}$$

и, следовательно,

$$d' = x^2 + dy^2, \quad 2xy = 0.$$

Если $y = 0$, то $d' = x^2$, что невозможно. Если же $x = 0$, то $d' = dy^2$ и, значит, $d' = d$.

Нами доказано, таким образом, что все квадратичные поля находятся во взаимно однозначном соответствии со всеми целыми рациональными $d \neq 1$, свободными от квадратов.

2. Порядки в квадратичном поле. Числа поля $\mathbb{Q}(\sqrt{d})$ имеют вид $\alpha = x + y\sqrt{d}$, где x и y рациональные. Так как характеристический многочлен для α равен

$$t^2 - 2xt + x^2 - dy^2,$$

то α будет принадлежать максимальному порядку $\tilde{\mathfrak{O}}$ поля $\mathbb{Q}(\sqrt{d})$ тогда и только тогда, когда $2x = \mathrm{Sp}(\alpha)$ и $x^2 - dy^2 = N(\alpha)$ целые рациональные. Положим $2x = m$. Так как $\frac{m^2}{4} - dy^2$ должно быть целым, а d свободно от квадратов, то в знаменателе рационального числа y (при несократимой записи) может быть только 2, т. е. $y = n/2$ с целым n. Ясно, что $N(\alpha) = \frac{m^2}{4} - d\frac{n^2}{4}$ является целым лишь при условии

$$m^2 - dn^2 \equiv 0 \pmod 4. \tag{1}$$

Решения этого сравнения зависят, очевидно, от d, точнее, от значения d по модулю 4. Поскольку d свободно от квадратов, то $d \not\equiv 0 \pmod 4$, и мы имеем три возможности:

$$d \equiv 1 \pmod 4; \qquad d \equiv 2 \pmod 4; \qquad d \equiv 3 \pmod 4.$$

Если $d \equiv 1 \pmod 4$, то сравнение (1) принимает вид $m^2 \equiv n^2 \pmod 4$, что эквивалентно условию $m \equiv n \pmod 2$, т. е. $m = n + 2l$, и мы получаем

$$\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d} = l + n\frac{1+\sqrt{d}}{2}$$

с целыми l и n. Таким образом, в этом случае в качестве базиса максимального порядка $\tilde{\mathfrak{O}}$ (т. е. в качестве фундаментального базиса поля $\mathbb{Q}(\sqrt{d})$, см. конец § 2) можно взять числа 1 и $\omega = \frac{1+\sqrt{d}}{2}$.

Пусть теперь $d \equiv 2$ или $3 \pmod 4$. Если бы сравнение (1) имело решение с нечетным n, то из $d \equiv m^2 \pmod 4$ следовало бы $d \equiv 0 \pmod 4$ при m четном и $d \equiv 1 \pmod 4$ при m нечетном. Это, однако, противоречит нашему предположению. Но если n четное, то из сравнения $m^2 \equiv 0 \pmod 4$ получаем, что и m четное. Мы получили, таким образом, что в рассматриваемом случае чис-

ло $x+y\sqrt{d}$ принадлежит максимальному порядку $\widetilde{\mathfrak{O}}$ поля $\mathbb{Q}(\sqrt{d})$ лишь при целых $x=m/2$ и $y=n/2$. В качестве базиса порядка $\widetilde{\mathfrak{O}}$ здесь можно взять, следовательно, числа 1 и $\omega=\sqrt{d}$.

В дальнейшем, говоря о базисе максимального порядка поля $\mathbb{Q}(\sqrt{d})$, мы всегда будем иметь в виду базис 1, ω, где $\omega=\dfrac{1+\sqrt{d}}{2}$ при $d\equiv 1 \pmod 4$ и $\omega=\sqrt{d}$ при $d\equiv 2, 3 \pmod 4$.

Рассмотрим теперь произвольный порядок $\mathfrak{O}$ поля $\mathbb{Q}(\sqrt{d})$. Так как $\mathfrak{O}$ содержится в максимальном порядке $\widetilde{\mathfrak{O}}$ (см. § 2, п. 4), то все числа из $\mathfrak{O}$ имеют вид $x+y\omega$ с целыми рациональными x и y. Выберем среди них число с наименьшим положительным значением коэффициента y. Пусть это будет $a+f\omega$. Так как a, будучи целым рациональным числом, содержится в $\mathfrak{O}$, то $f\omega\in\mathfrak{O}$. Ясно теперь, что для всякого $x+y\omega$ из $\mathfrak{O}$ коэффициент y делится на f, а значит $\mathfrak{O}=\{1, f\omega\}$. Обратно, по лемме 3 § 2 при любом натуральном f модуль $\{1, f\omega\}$ является кольцом, а значит, и порядком поля $\mathbb{Q}(\sqrt{d})$. Так как для различных натуральных f порядки $\{1, f\omega\}$ также различны, то мы получаем следующий факт: все порядки в квадратичном поле находятся во взаимно однозначном соответствии со всеми натуральными числами.

В дальнейшем порядок $\{1, f\omega\}$ мы будем обозначать через $\mathfrak{O}_f$. Легко видеть, что число f равно индексу порядка $\mathfrak{O}_f$ в максимальном порядке $\widetilde{\mathfrak{O}}=\mathfrak{O}_1=\{1, \omega\}$. Таким образом, каждый порядок квадратичного поля вполне определяется своим индексом в максимальном порядке.

Займемся вычислением дискриминанта D_f порядка $\mathfrak{O}_f$. Предположим сначала, что $d\equiv 1 \pmod 4$. Так как $\operatorname{Sp}\sqrt{d}=0$, то

$$\operatorname{Sp}\omega=\operatorname{Sp}\left(\frac{1+\sqrt{d}}{2}\right)=1,\quad \operatorname{Sp}\omega^2=\operatorname{Sp}\left(\frac{d+1}{4}+\frac{\sqrt{d}}{2}\right)=\frac{d+1}{2}$$

и, следовательно,

$$D_f=\begin{vmatrix}\operatorname{Sp}1 & \operatorname{Sp}f\omega\\ \operatorname{Sp}f\omega & \operatorname{Sp}f^2\omega^2\end{vmatrix}=\begin{vmatrix}2 & f\\ f & f^2\dfrac{d+1}{2}\end{vmatrix}=f^2d.$$

Если теперь $d\equiv 2$ или $3 \pmod 4$, то

$$D_f=\begin{vmatrix}\operatorname{Sp}1 & \operatorname{Sp}f\sqrt{d}\\ \operatorname{Sp}f\sqrt{d} & \operatorname{Sp}f^2d\end{vmatrix}=\begin{vmatrix}2 & 0\\ 0 & 2f^2d\end{vmatrix}=f^2\cdot 4d.$$

Полученные формулы для D_f показывают нам, что каждый порядок в квадратичном поле однозначно определен своим дискриминантом.

Результаты этого пункта объединим в виде следующей теоремы.

Теорема 1. *Пусть $d \neq 1$ — свободное от квадратов целое рациональное число. В качестве базиса максимального порядка $\widetilde{\mathfrak{O}}$ квадратичного поля $\mathbb{Q}(\sqrt{d})$ можно взять числа 1 и ω, где $\omega = \frac{1+\sqrt{d}}{2}$ при $d \equiv 1 \pmod 4$ и $\omega = \sqrt{d}$ при $d \equiv 2, 3 \pmod 4$. Дискриминант D_1 порядка $\widetilde{\mathfrak{O}}$ (т. е. дискриминант поля $\mathbb{Q}(\sqrt{d})$) равен d в первом случае и $4d$ — во втором. Произвольный порядок $\mathfrak{O}$ поля $\mathbb{Q}(\sqrt{d})$ имеет вид $\mathfrak{O}_f = \{1, f\omega\}$, где f — индекс $(\widetilde{\mathfrak{O}} : \mathfrak{O})$. Дискриминант порядка $\mathfrak{O}_f$ равен $D_1 f^2$.*

3. Единицы. Так как всякое число порядка $\mathfrak{O}_f$ представляется в виде $x + yf\omega$ с целыми рациональными x и y, то по теореме 4 § 2 мы найдем все единицы в $\mathfrak{O}_f$, если решим неопределенное уравнение

$$N(x + yf\omega) = \pm 1, \tag{2}$$

т. е. уравнение

$$x^2 + fxy + f^2 \frac{1-d}{4} y^2 = \pm 1 \tag{3}$$

при $d \equiv 1 \pmod 4$ и уравнение

$$x^2 - df^2y^2 = \pm 1 \tag{4}$$

при $d \equiv 2, 3 \pmod 4$.

Для мнимого квадратичного поля $s = 0$, $t = 1$, $r = s + t - 1 = 0$, а это означает, что группа единиц в любом порядке этого поля конечна и исчерпывается корнями из 1. Этот факт согласуется также с тем, что уравнения (3) и (4) при $d < 0$ имеют лишь конечное число целочисленных решений. Именно, при $d = -1$, $f = 1$ уравнение (4) имеет четыре решения: $x = \pm 1$, $y = 0$; $x = 0$, $y = \pm 1$, что соответствует корням ± 1, $\pm i$ четвертой степени из 1. При $d = -3$, $f = 1$ уравнение (3) имеет шесть решений: $x = \pm 1$, $y = 0$; $x = 0$, $y = \pm 1$; $x = 1$, $y = -1$; $x = -1$, $y = 1$, соответствующих всем корням ± 1, $\pm\frac{1}{2} \pm \frac{i\sqrt{3}}{2}$ шестой степени из 1. Для всех остальных порядков мнимых квадратичных полей уравнения (3) или соответственно (4) имеют лишь два решения: $x = \pm 1$, $y = 0$, т. е. все их единицы исчерпываются числами ± 1.

Сложнее случай вещественного квадратичного поля $\mathbb{Q}(\sqrt{d})$, $d > 0$. Так как в этом случае $s = 2$, $t = 0$ и, следовательно, $r = 1$, то все единицы порядка $\mathfrak{O}_f$ поля $\mathbb{Q}(\sqrt{d})$ имеют вид $\pm\varepsilon^n$, где ε — так называемая основная единица порядка $\mathfrak{O}_f$. Вопрос здесь сводится, таким образом, к определению основной единицы ε. Вместе с ε числа $1/\varepsilon$, $-\varepsilon$, $-1/\varepsilon$ также являются основными единицами. Можно поэтому считать, что $\varepsilon > 1$. Ясно, что условием $\varepsilon > 1$ основная единица ε определена однозначно.

Покажем, что для единицы $\eta > 1$ из $\mathfrak{O}_f$ в ее представлении $\eta = x + yf\omega$ через базис $1, f\omega$ коэффициенты x и y положительны

(при $d=5$, $f=1$ возможно $x=0$). Для всякого $\alpha \in \mathbb{Q}(\sqrt{d})$ через α' будем обозначать сопряженное с ним число, т. е. образ α при автоморфизме $\sqrt{d} \to -\sqrt{d}$ поля $\mathbb{Q}(\sqrt{d})$. Легко видеть, что $\omega - \omega' > 0$. Так как $N(\eta) = \eta\eta' = \pm 1$, то единица η' равна либо $1/\eta$, либо $-1/\eta$; в обоих случаях $\eta - \eta' > 0$, т. е. $yf(\omega - \omega') > 0$, а значит, $y > 0$. Далее, так как $|\eta'| = |x + yf\omega'| < 1$ и $f\omega' < -1$, за исключением случая $d=5$, $f=1$, то $x > 0$ (если $d=5$, $f=1$, то $-1 < f\omega' = \frac{1-\sqrt{5}}{2} < 0$ и мы получаем $x \geqslant 0$).

Пусть $\varepsilon > 1$ — основная единица порядка $\mathfrak{O}_f$. Для единицы $\varepsilon^n = x_1 + y_1 f\omega$ с натуральным n имеем $x_1 > x$ и $y_1 > y$. Следовательно, чтобы найти основную единицу $\varepsilon > 1$, мы должны найти целочисленное решение уравнения (2) с наименьшими положительными значениями x и y. Пользуясь результатами п. 3 § 5, мы можем эти искомые значения x и y ограничить сверху некоторой константой C, после чего их нахождение сводится к конечному числу испытаний.

Мы покажем сейчас, что число проб, необходимых для вычисления основной единицы, может быть значительно сокращено, если воспользоваться одним фактом из теории непрерывных дробей. Речь идет о теореме, утверждающей, что если для вещественного $\xi > 0$ и натуральных взаимно простых x и y имеет место неравенство

$$\left|\frac{x}{y} - \xi\right| < \frac{1}{2y^2},$$

то $\frac{x}{y}$ необходимо является одной из подходящих дробей разложения числа ξ в непрерывную дробь.

В силу (2)

$$\left|\frac{x}{y} + f\omega'\right| = \frac{1}{y(x + yf\omega)}.$$

Если $d \equiv 1 \pmod 4$, то, оставив в стороне случай $d=5$, $f=1$, получаем

$$\left|\frac{x}{y} - f\frac{\sqrt{d}-1}{2}\right| = \frac{1}{y^2\left(\frac{x}{y} + f\frac{\sqrt{d}+1}{2}\right)} < \frac{1}{2y^2}$$

$\left(\text{так как } \frac{x}{y} > 0 \text{ и } f\frac{\sqrt{d}+1}{2} > 2\right)$. Если же $d \equiv 2, 3 \pmod 4$, то, поскольку $x^2 = f^2dy^2 \pm 1 \geqslant dy^2 - 1 \geqslant y^2(d-1)$ и $d \geqslant 2$, имеем

$$\left|\frac{x}{y} - f\sqrt{d}\right| = \frac{1}{y(x + yf\sqrt{d})} \leqslant \frac{1}{y^2(\sqrt{d-1} + \sqrt{d})} < \frac{1}{2y^2}.$$

Согласно упомянутой теореме несократимое отношение x/y является одной из подходящих дробей разложения иррационального числа $-f\omega'$ в непрерывную дробь. Чтобы найти наименьшее положительное решение уравнения (2), мы должны, следовательно,

испытывать лишь числители и соответствующие им знаменатели подходящих дробей для $-f\omega'$ (не превосходящие заранее вычисленной константы C). Практически вычисления целесообразно вести следующим образом. Для числа $-f\omega'$ находим последовательно неполные частные q_k $(k \geqslant 0)$ и сразу же — числители P_k и знаменатели Q_k соответствующих подходящих дробей. Вычисления продолжаем до тех пор, пока на некотором шаге выражение $N(P_k + \omega f Q_k)$ не окажется равным $+1$ или -1. Это обязательно наступит при $P_k < C$, и основная единица $\varepsilon = P_k + \omega f Q_k$ будет найдена. (Для исключенного случая $d = 5$, $f = 1$ основной единицей будет $\omega = \frac{1+\sqrt{5}}{2}$.) Проиллюстрируем сказанное двумя примерами.

Пример 1. Чтобы найти основную единицу порядка $\{1, 3\sqrt{6}\}$ поля $\mathbb{Q}(\sqrt{6})$, разложим число $-3\omega' = 3\sqrt{6}$ в непрерывную дробь:

$$\sqrt{54} = 7 + (\sqrt{54} - 7), \qquad \frac{9}{\sqrt{54}-6} = 6 + \frac{\sqrt{54}-6}{2},$$

$$\frac{1}{\sqrt{54}-7} = 2 + \frac{\sqrt{54}-3}{5}, \qquad \frac{2}{\sqrt{54}-6} = 1 + \frac{\sqrt{54}-3}{9},$$

$$\frac{5}{\sqrt{54}-3} = 1 + \frac{\sqrt{54}-6}{9}, \qquad \frac{9}{\sqrt{54}-3} = 2 + \frac{\sqrt{54}-7}{5}.$$

Одновременно заполняем таблицу:

k	0	1	2	3	4	5
q_k	7	2	1	6	1	2
P_k	7	15	22	147	169	485
Q_k	1	2	3	20	23	66
$P_k^2 - 54Q_k^2$	-5	9	-2	9	-5	1

Основная единица порядка $\{1, 3\sqrt{6}\}$ равна, следовательно, $485 + 66 \cdot 3\sqrt{6} = 485 + 198\sqrt{6}$.

Пример 2. Вычислим основную единицу поля $\mathbb{Q}(\sqrt{41})$. Имеем:

$$\frac{\sqrt{41}-1}{2} = 2 + \frac{\sqrt{41}-5}{2}, \qquad \frac{4}{\sqrt{41}-5} = 2 + \frac{\sqrt{41}-3}{4},$$

$$\frac{2}{\sqrt{41}-5} = 1 + \frac{\sqrt{41}-3}{8}, \qquad \frac{4}{\sqrt{41}-3} = 1 + \frac{\sqrt{41}-5}{8}.$$

$$\frac{8}{\sqrt{41}-3} = 2 + \frac{\sqrt{41}-5}{4},$$

h	0	1	2	3	4
q_h	2	1	2	2	1
P_h	2	3	8	19	27
Q_h	1	1	3	7	10
$P_h^2 + P_h Q_h - 10Q_h^2$	-4	2	-2	4	-1

Основная единица максимального порядка поля $\mathbb{Q}(\sqrt{41})$ равна, таким образом,

$$27 + 10\frac{\sqrt{41}+1}{2} = 32 + 5\sqrt{41}.$$

4. Модули. Перейдем к изучению полных модулей в квадратичных полях. Так как всякий модуль $\{\alpha, \beta\}$ подобен модулю $\left\{1, \frac{\beta}{\alpha}\right\}$, то мы можем ограничиться рассмотрением модулей вида $\{1, \gamma\}$.

Всякое нерациональное число γ из $\mathbb{Q}(\sqrt{d})$ является корнем некоторого многочлена at^2+bt+c с целыми рациональными коэффициентами. Если мы на a, b, c наложим условия $(a, b, c)=1$ и $a>0$, то для данного γ многочлен at^2+bt+c будет определен однозначно. Будем обозначать его в дальнейшем через $\varphi_\gamma(t)$. Ясно, что для сопряженного числа γ' имеем $\varphi_{\gamma'}(t) = \varphi_\gamma(t)$ более того, равенство $\varphi_{\gamma_1}(t) = \varphi_\gamma(t)$ имеет место тогда и только тогда, когда γ_1 равно либо γ, либо γ'.

Лемма 1. *Если для нерационального числа γ из $\mathbb{Q}(\sqrt{d})$ многочлен $\varphi_\gamma(t)$ равен at^2+bt+c, то кольцом множителей Ω модуля $M=\{1, \gamma\}$ является порядок $\{1, a\gamma\}$ с дискриминантом $D=b^2-4ac$.*

Доказательство. Рассмотрим число $\alpha = x + y\gamma$ с рациональными x и y. Так как включение $\alpha M \subset M$ равносильно тому, что $\alpha \cdot 1 = x + y\gamma \in M$ и

$$a\cdot\gamma = -\frac{cy}{a} + \left(x - \frac{by}{a}\right)\gamma \in M,$$

то α принадлежит кольцу множителей Ω тогда и только тогда, когда рациональные числа

$$x, \quad y, \quad \frac{cy}{a}, \quad \frac{by}{a}$$

все целые, т. е. когда x и y целые и, кроме того, y делится на a (последнее вытекает из того, что $(a, b, c)=1$). Этим доказано, что $\Omega = \{1, a\gamma\}$. Для завершения доказательства леммы 1

остается вычислить дискриминант порядка $\mathfrak{O}$:

$$D = \begin{vmatrix} \mathrm{Sp}\,1 & \mathrm{Sp}\,\alpha\gamma \\ \mathrm{Sp}\,\alpha\gamma & \mathrm{Sp}\,\alpha^2\gamma^2 \end{vmatrix} = \begin{vmatrix} 2 & -b \\ -b & b^2-2ac \end{vmatrix} = b^2 - 4ac.$$

Следствие. *При тех же обозначениях норма модуля* $\{1, \gamma\}$ *равна* $\frac{1}{a}$.

Действительно, матрица перехода от базиса 1, $a\gamma$ к базису 1, γ равна

$$\begin{pmatrix} 1 & 0 \\ 0 & 1/a \end{pmatrix}.$$

Лемма 2. *Для того чтобы модули* $\{1, \gamma_1\}$ *и* $\{1, \gamma\}$ *были подобны, необходимо и достаточно, чтобы числа* γ_1 *и* γ *были связаны соотношением*

$$\gamma_1 = \frac{k\gamma + l}{m\gamma + n}, \tag{5}$$

где целые рациональные k, l, m, n *таковы, что*

$$\begin{vmatrix} k & l \\ m & n \end{vmatrix} = \pm 1. \tag{6}$$

Доказательство. Так как два различных базиса в одном и том же модуле связаны между собой унимодулярным преобразованием (см. § 2, п. 1), то из равенства $\{\alpha, \alpha\gamma_1\} = \{1, \gamma\}$ следует, что

$$\alpha\gamma_1 = k\gamma + l, \qquad \alpha = m\gamma + n,$$

причем целые рациональные k, l, m, n удовлетворяют условию (6). Разделив первое из этих равенств на второе, мы и получим (5). Обратно, пусть γ_1 и γ связаны соотношением (5). Тогда

$$\{1, \gamma_1\} = \frac{1}{m\gamma + n}\{m\gamma + n, k\gamma + l\} = \frac{1}{m\gamma + n}\{1, \gamma\}$$

(равенство $\{m\gamma + n, k\gamma + l\} = \{1, \gamma\}$ имеет место в силу (6)). Доказательство леммы 2 закончено.

Рассмотрим в поле $\mathbb{Q}(\sqrt{d})$ модули, принадлежащие некоторому фиксированному порядку $\mathfrak{O}$ (т. е. для которых $\mathfrak{O}$ является кольцом множителей). Согласно теореме 3 § 6 все эти модули разбиваются на конечное число классов подобных модулей. Мы введем сейчас действие умножения классов и покажем, что относительно него все классы подобных модулей, принадлежащие данному порядку $\mathfrak{O}$, образуют группу.

Если $M = \{\alpha, \beta\}$ и $M_1 = \{\alpha_1, \beta_1\}$ — два модуля, то под их произведением MM_1 понимается модуль $\{\alpha\alpha_1, \alpha\beta_1, \beta\alpha_1, \beta\beta_1\}$ (см. задачу 7 § 2). Очевидно, что при $\lambda \neq 0$ и $\mu \neq 0$ справедлива формула

$$(\lambda M)(\mu M_1) = \lambda\mu(MM_1). \tag{7}$$

Для каждого модуля M через $[M]$ будем обозначать класс подобных модулей, содержащий M в качестве представителя. Из равенства (7) следует, что класс $[MM_1]$ зависит лишь от классов $[M]$ и $[M_1]$. Класс $[MM_1]$ называется произведением классов $[M]$ и $[M_1]$. Чтобы перемножить два класса, надо, следовательно, выбрать произвольно представители в этих классах и перемножить их. Класс подобных модулей, содержащий полученное произведение, и будет произведением данных классов.

Для каждого модуля M через M' обозначим модуль, состоящий из сопряженных чисел α' для всех α из M. Так как $\alpha+\alpha'=\mathrm{Sp}\,\alpha$ рационально, то $\alpha'\in\mathbb{Q}(\sqrt{d})$, а значит, M' вместе с M является также полным модулем поля $\mathbb{Q}(\sqrt{d})$. Легко видеть, что для любого порядка $\mathfrak{O}$ сопряженный с ним модуль $\mathfrak{O}'$ совпадает с $\mathfrak{O}$. Отсюда следует, что сопряженные модули имеют одно и то же кольцо множителей.

Докажем формулу

$$MM'=N(M)\mathfrak{O}, \tag{8}$$

в которой $\mathfrak{O}$ обозначает кольцо множителей, а $N(M)$ — норму модуля M.

Предположим сначала, что модуль M имеет вид $\{1, \gamma\}$. В этом случае, воспользовавшись обозначениями леммы 1, мы получаем

$$MM'=\{1,\gamma\}\{1,\gamma'\}=\{1,\gamma,\gamma',\gamma\gamma'\}=$$

$$=\left\{1,\gamma,-\gamma-\frac{b}{a},-\frac{c}{a}\right\}=\left\{1,\gamma,-\frac{b}{a},-\frac{c}{a}\right\}=\frac{1}{a}\{a,b,c,a\gamma\}.$$

Так как a, b и c взаимно просты, то все их целочисленные линейные комбинации совпадают с кольцом целых чисел $\mathbb{Z}$, и, следовательно,

$$MM'=\frac{1}{a}\{1,a\gamma\}=\frac{1}{a}\mathfrak{O}=N(M)\mathfrak{O}$$

(следствие леммы 1). Если теперь M — произвольный модуль, то его можно представить в виде $M=\alpha M_1$, где M_1 имеет вид $\{1, \gamma\}$. Ввиду теоремы 2 § 6 мы получаем

$$MM'=\alpha\alpha' M_1M_1'=N(\alpha)\,N(M_1)\,\mathfrak{O}=|N(\alpha)|\,N(M_1)\,\mathfrak{O}=N(M)\,\mathfrak{O},$$

и формула (8) доказана в общем случае.

Пусть теперь M и M_1 — два модуля, принадлежащие одному и тому же порядку $\mathfrak{O}$. Если $\overline{\mathfrak{O}}$ — кольцо множителей для произведения MM_1, то ввиду формулы (8)

$$MM_1(MM_1)'=N(MM_1)\overline{\mathfrak{O}}.$$

С другой стороны, так как умножение модулей, очевидно, коммутативно и ассоциативно, то, перемножив формулы $MM'=N(M)\mathfrak{O}$

и $M_1M_1' = N(M_1)\mathfrak{O}$, получим

$$MM_1(MM_1)' = N(M)N(M_1)\mathfrak{O}.$$

Сравнивая это равенство с предыдущим и замечая, что различные порядки не могут быть подобны, приходим к равенству $\mathfrak{O} = \overline{\mathfrak{O}}$. Попутно, в силу того что равенство $a\mathfrak{O} = b\mathfrak{O}$ с положительными рациональными a и b возможно только при $a = b$, мы получаем формулу

$$N(MM_1) = N(M)N(M_1).$$

Таким образом, если модули M и M_1 принадлежат порядку $\mathfrak{O}$, то их произведение MM_1 также принадлежит $\mathfrak{O}$. Так как, далее, для всякого модуля M с кольцом множителей $\mathfrak{O}$ одновременно $M\mathfrak{O} = M$ и $M\left(\frac{1}{N(M)}M'\right) = \mathfrak{O}$, то мы получаем следующий результат.

Теорема 2. *Все модули квадратичного поля, принадлежащие фиксированному порядку, относительно действия умножения модулей образуют коммутативную группу.*

Из этой теоремы и теоремы 3 § 6 очевидным образом вытекает

Теорема 3. *Все классы подобных модулей квадратичного поля с данным кольцом множителей $\mathfrak{O}$ образуют конечную коммутативную группу.*

Отметим, что теоремы 2 и 3 характерны только для модулей в квадратичных полях и перестают быть справедливыми для модулей, принадлежащих немаксимальным порядкам произвольного поля алгебраических чисел (см. задачу 18 § 2).

5. Соответствие между модулями и формами. Согласно п. 3 § 1 каждому базису α, β полного модуля $M \subset \mathbb{Q}(\sqrt{d})$ однозначно соответствует бипарная квадратичная форма $N(\alpha x + \beta y)$ с рациональными коэффициентами. Так как для различных базисов в M соответствующие им формы эквивалентны, то модулю M соответствует целый класс эквивалентных форм. Далее, если вместо M взять подобный с ним модуль γM, то все наши формы приобретут постоянный множитель $N(\gamma)$. Следовательно, рассматривая формы с точностью до постоянного множителя, можно сказать, что каждому классу подобных модулей соответствует некоторый класс эквивалентных форм. Это соответствие, однако, не будет взаимно однозначным. Действительно, сопряженные между собой модули $M = \{\alpha, \beta\}$ и $M' = \{\alpha', \beta'\}$, вообще говоря, не подобны, а соответствующие им формы совпадают. Аналогичное явление, очевидно, имеет место и для разложимых форм любых степеней. В общем случае, по-видимому, не существует естественного способа устранить это несоответствие между классами форм и классами модулей. Но для квадратичных полей, как мы сейчас увидим, можно восстановить взаимную однозначность, если только

слегка изменить определения эквивалентности форм и подобия модулей.

Определение. *Бинарная квадратичная форма* $f(x, y) = Ax^2 + Bxy + Cy^2$ *с целыми рациональными коэффициентами называется примитивной, если общий наибольший делитель ее коэффициентов равен* 1.

Целое число $B^2 - 4AC$ *называется дискриминантом примитивной формы* f.

Дискриминант примитивной формы, следовательно, отличается от ее определителя $AC - B^2/4$ постоянным множителем -4.

Легко видеть, что для примитивной формы всякая эквивалентная с ней форма будет также примитивной. При линейном преобразовании переменных с матрицей C определитель квадратичной формы приобретает множитель $(\det C)^2$, а значит, он не меняется, если только $\det C = \pm 1$. Отсюда следует, что эквивалентные примитивные формы имеют один и тот же дискриминант.

Определение. *Две примитивные формы называются собственно эквивалентными, если одна из них преобразуется в другую с помощью целочисленного линейного преобразования переменных с определителем* $+1$.

Все примитивные бинарные квадратичные формы разбиваются на классы собственно эквивалентных форм. В дальнейшем на протяжении всего настоящего пункта, говоря о классах форм, мы будем подразумевать, что речь идет о собственной эквивалентности. Часто случается все же, что две формы, эквивалентные несобственно (т. е. переводящиеся друг в друга линейным преобразованием с определителем -1), будут также и собственно эквивалентны.

Дадим теперь новое определение подобия модулей.

Определение. *Два полных модуля* M *и* M_1 *в квадратичном поле называются подобными в узком смысле, если* $M_1 = \alpha M$ *при некотором* α *с положительной нормой.*

Так как для мнимого квадратичного поля норма всякого $\alpha \neq 0$ положительна, то в этих полях понятие подобия в узком смысле ничем не отличается от обычного понятия подобия. То же самое будет иметь место и в случае вещественного квадратичного поля, если только в кольце множителей Ω рассматриваемых модулей имеется единица ε, для которой $N(\varepsilon) = -1$. Действительно, если $M_1 = \alpha M$ и $N(\alpha) < 0$, то, поскольку $\varepsilon M = M$, имеем $M_1 = (\alpha\varepsilon)M$, причем $N(\alpha\varepsilon) > 0$. Обратно, пусть подобие в узком смысле совпадает с обычным, т. е. из $M_1 = \alpha M$, $N(\alpha) < 0$ следует существование β, для которого $N(\beta) > 0$ и $M_1 = \beta M$. Полагая $\varepsilon = \alpha\beta^{-1}$, имеем $\varepsilon M = M$, а это означает (см. § 2, п. 3), что ε — единица кольца множителей Ω, причем $N(\varepsilon) = -1$.

Таким образом, понятие подобия в узком смысле отличается от обычного понятия подобия лишь для тех модулей вещественн-

ного квадратичного поля, в кольце множителей которых все единицы имеют норму $+1$. Ясно, что в этом случае каждый класс модулей, подобных в широком смысле, разбивается в точности на два класса в узком смысле.

Опишем теперь соответствие между классами модулей и классами форм.

В каждом модуле M поля $\mathbb{Q}(\sqrt{d})$ мы будем рассматривать лишь такие базисы α, β, для которых определитель

$$\Delta = \begin{vmatrix} \alpha & \beta \\ \alpha' & \beta' \end{vmatrix} \tag{9}$$

удовлетворяет условию:

$$\Delta > 0 \quad \text{при} \quad d > 0, \qquad \frac{1}{i}\Delta > 0 \quad \text{при} \quad d < 0. \tag{10}$$

(Как и ранее, α' и β' здесь обозначают числа из $\mathbb{Q}(\sqrt{d})$, сопряженные с α и β. Базисы в M, обладающие свойством (10), всегда существуют: если первый попавшийся базис α_1, α_2 им не обладает, то достаточно α_1 и α_2 поменять местами.)

Каждому базису α, β модуля M, удовлетворяющему условию (10), поставим в соответствие форму

$$f(x, y) = Ax^2 + Bxy + Cy^2 = \frac{N(\alpha x + \beta y)}{N(M)} = \frac{(\alpha x + \beta y)(\alpha' x + \beta' y)}{N(M)} \tag{11}$$

($N(M)$ — норма модуля M). Если мы для числа $\gamma = -\beta/\alpha$ введем в рассмотрение $\varphi_\gamma(t) = at^2 + bt + c$ (см. начало п. 4), то будем, очевидно, иметь

$$N(\alpha x + \beta y) = \frac{N(\alpha)}{a}(ax^2 + bxy + cy^2).$$

С другой стороны, по следствию леммы 1 и по теореме 2 § 6 норма модуля $M = \alpha\{1, \gamma\}$ равна $|N(\alpha)|/a$. Отсюда следует, что коэффициенты A, B, C отличаются от a, b, c, возможно, лишь знаком. Этим доказано, что форма (11) примитивна и ее дискриминант $B^2 - 4AC$ совпадает с дискриминантом $b^2 - 4ac$ кольца множителей модуля M (лемма 1). Таким образом, мы имеем отображение

$$\{\alpha, \beta\} \to f(x, y), \tag{12}$$

которое каждому базису α, β поля $\mathbb{Q}(\sqrt{d})$ с условием (10) сопоставляет примитивную форму $f(x, y)$ (в случае вещественного поля коэффициент A может быть отрицательным). Очевидно при этом, что в случае мнимого квадратичного поля форма (11) всегда положительно определенная, так что отрицательно определенные формы остаются вне соответствия (12).

Теорема 4. *Пусть $\mathfrak{M}$ есть совокупность всех классов подобных в узком смысле модулей квадратичного поля $\mathbb{Q}(\sqrt{d})$ и $\mathfrak{F}$ —*

совокупность всех при $d>0$ и положительно определенных при $d<0$ классов собственно эквивалентных примитивных бинарных квадратичных форм, разлагающихся в $\mathbb{Q}(\sqrt{d})$ на линейные множители. Отображение (12) *устанавливает взаимно однозначное соответствие между $\mathfrak{M}$ и $\mathfrak{F}$; при этом, если некоторый класс модулей принадлежит кольцу множителей с дискриминантом D, то соответствующие ему формы также имеют дискриминант D.*

Пусть α, β и α_1, β_1 — два базиса поля $\mathbb{Q}(\sqrt{d})$, для которых определители вида (9) удовлетворяют условию (10), и пусть этим базисам соответствуют формы f и f_1. Для доказательства теоремы 4 мы должны показать, что формы f и f_1 собственно эквивалентны тогда и только тогда, когда модули $\{\alpha, \beta\}$ и $\{\alpha_1, \beta_1\}$ подобны в узком смысле. Далее, мы должны убедиться, что для всякой неприводимой примитивной формы $g(x, y)$ (раскладывающейся на линейные множители в $\mathbb{Q}(\sqrt{d})$ и положительно определенной, если только $d<0$) существует базис α, β с условием (10), для которого форма (11) совпадает с $g(x, y)$. Ограничившись этим общим указанием, мы подробное проведение доказательства предоставляем читателю.

В п. 4 было определено произведение классов подобных модулей. Точно таким же образом мы можем определить произведение классов модулей, подобных в узком смысле. В силу взаимно однозначного соответствия $\mathfrak{M} \to \mathfrak{F}$ умножение классов модулей может быть перенесено на классы форм. Так определенное действие умножения на $\mathfrak{F}$ носит название композиции классов форм (термин исходит от Гаусса, который впервые это действие рассматривал). Так как все классы подобных в узком смысле модулей, принадлежащие фиксированному кольцу множителей, образуют, как легко видеть, группу, то, следовательно, все классы примитивных форм данного дискриминанта D (положительно определенных при $D<0$) также образуют группу.

6. Представление чисел бинарными формами и подобие модулей. В этом пункте мы покажем, что задача о нахождении представлений целых чисел бинарными квадратичными формами может быть сведена к задаче о подобии модулей в квадратичном поле.

Пусть $f(x, y)$ — примитивная бинарная квадратичная форма дискриминанта $D \neq 0$, раскладывающаяся на линейные множители в поле $\mathbb{Q}(\sqrt{d})$, и m — натуральное число. В случае $D<0$ мы предполагаем, что форма f положительно определенная. Задача состоит в нахождении всех целочисленных решений неопределенного уравнения

$$f(x, y) = m \tag{13}$$

(мы ограничиваемся положительными значениями m, так как в случае $m<0$, $D>0$ вместо f можно рассмотреть форму $-f$).

Согласно теореме 4 форму f мы можем представить в виде

$$f(x, y) = \frac{N(\alpha x + \beta x)}{N(M)}, \tag{14}$$

где базис α, β модуля M удовлетворяет условию (10). Отображение $(x, y) \to \xi = \alpha x + \beta y$ устанавливает взаимно однозначное соответствие между решениями уравнения (13) и числами $\xi \in M$ с нормой $N(\xi) = mN(M)$. Два решения уравнения (13) назовем ассоциированными, если ассоциированы соответствующие им числа из M. Легко проверить, что понятие ассоциированности решений не зависит от выбора представления (14). Обозначим через $\mathfrak{O}$ кольцо множителей модуля M и через C класс модулей в узком смысле, содержащий M в качестве представителя. Согласно теореме 4 класс C однозначно определен формой f.

Предположим, что мы имеем число $\xi \in M$ с нормой $mN(M)$. Рассмотрим модуль $A = \xi M^{-1}$. Так как $AM = \xi M^{-1}M = \xi\mathfrak{O} \subset M$, то модуль A содержится в $\mathfrak{O}$. Его норма равна $N(\xi)N(M)^{-1} = m$. Ясно также, что A содержится в обратном классе модулей C^{-1}.

Обратно, предположим, что в классе C^{-1} имеется модуль A, который содержится в кольце $\mathfrak{O}$ и имеет норму m. Тогда при некотором ξ с положительной нормой мы имеем равенство $A = \xi M^{-1}$, при этом $\xi \in MA \subset M$ и $N(\xi) = m$. Если A_1 — другой модуль из класса C^{-1}, содержащийся в $\mathfrak{O}$ и с нормой m, и если $A_1 = \xi_1 M^{-1}$, $N(\xi_1) > 0$, то $A_1 = \xi_1\xi^{-1}A$, а значит, A_1 совпадает с A тогда и только тогда, когда ξ_1 ассоциировано с ξ.

Нами доказана, таким образом, следующая теорема.

Теорема 5. *Пусть форма $f(x, y)$ соответствует классу модулей C (в узком смысле) с кольцом множителей $\mathfrak{O}$. Все классы ассоциированных решений уравнения* (13) *находятся во взаимно однозначном соответствии со всеми модулями A, которые принадлежат обратному классу C^{-1}, содержатся в кольце множителей $\mathfrak{O}$ и имеют норму m. Решения (x, y), соответствующие модулю A, определяются числами ξ, для которых $A = \xi M^{-1}$, $N(\xi) > 0$, где M — модуль из класса C.*

Для любого натурального m мы легко можем выписать все модули A с кольцом множителей $\mathfrak{O}$, которые содержатся в $\mathfrak{O}$ и имеют норму m. Пусть A — такой модуль. Обозначим через k наименьшее натуральное число, содержащееся в A. Модуль A мы можем тогда записать в виде

$$A = \{k, k\gamma\} = k\{1, \gamma\}.$$

Образующая γ определена здесь с точностью до знака и целочисленного слагаемого. Мы можем поэтому γ выбрать так, чтобы, во-первых,

$$\operatorname{Im}\gamma > 0 \quad \text{при} \quad d < 0, \qquad \operatorname{Irr}\gamma > 0 \quad \text{при} \quad d > 0 \tag{15}$$

($\operatorname{Irr}\gamma$ обозначает иррациональную часть числа γ) и, во-вто-

рых, чтобы рациональная часть γ содержалась в промежутке $(-1/2, 1/2]$. Если для числа γ мы примем обозначения леммы 1 и запишем его в виде

$$\gamma = \frac{-b+\sqrt{D}}{2a}, \tag{16}$$

то второе наше условие примет вид

$$-a \leqslant b < a. \tag{17}$$

В силу равенства $\mathfrak{O} = \{1, a\gamma\}$ (см. доказательство леммы 1) и условия $A \subset \mathfrak{O}$ мы легко получаем, что k делится на a, т. е. $k = as$ с целым s. Так как $m = N(A) = k^2 \frac{1}{a}$ (следствие к лемме 1), то

$$m = as^2. \tag{18}$$

Покажем, что найденное представление модуля A в виде

$$A = as\{1, \gamma\}, \tag{19}$$

где a, s и γ подчинены условиям (18), (15) и (17), единственно. В самом деле, если $as\{1, \gamma\} = a_1 s_1 \{1, \gamma_1\}$, где a_1, s_1 и γ_1 подчинены тем же требованиям, то $as = a_1 s_1$ и, значит, $\{1, \gamma\} = \{1, \gamma_1\}$. В силу следствия леммы 1 отсюда получаем равенство $a = a_1$ и, следовательно, $s = s_1$. Кроме того, так как образующая γ в модуле $\{1, \gamma\}$, удовлетворяющая условиям (15) и (17), определена однозначно, то $\gamma = \gamma_1$.

Предположим теперь, наоборот, что по заданному m натуральные числа a и s выбраны так, что выполнено равенство (18). Если b и c удовлетворяют условиям:

$$b^2 - 4ac = D, \qquad (a, b, c) = 1, \qquad -a \leqslant b < a, \tag{20}$$

то для числа γ вида (16) модуль $A = as\{1, \gamma\}$ будет содержаться в своем кольце множителей $\mathfrak{O} = \{1, a\gamma\}$ и его норма будет равна $a^2 s^2 \frac{1}{a} = m$.

Таким образом, мы будем иметь все нужные нам модули A, если найдем все четверки целых чисел $s > 0$, $a > 0$, b, c, удовлетворяющие условиям (18) и (20).

Если мы располагаем алгоритмом, с помощью которого можно решить вопрос о подобии в узком смысле любых двух полных модулей поля $\mathbb{Q}(\sqrt{d})$, то, выписав все модули $A \subset \mathfrak{O}$ с нормой m, мы сможем выделить из них те, которые подобны модулю M^{-1}. Согласно теореме 5 это даст нам все решения уравнения (13).

Из теоремы 5 очевидным образом вытекает следующее утверждение.

Теорема 6. *Для того чтобы натуральное число m представлялось некоторой примитивной бинарной квадратичной фор-*

мой дискриминанта D, необходимо и достаточно, чтобы в порядке $\mathfrak{O}$ дискриминанта D существовал модуль A, принадлежащий этому порядку и имеющий норму m. Последнее равносильно существованию целых $s>0$, $a>0$, b, c, удовлетворяющих условиям: $m=as^2$, $b^2-4ac=D$, $(a, b, c)=1$, $-a\leqslant b<a$.

В случае, когда D есть дискриминант максимального порядка $\widetilde{\mathfrak{O}}$, второе утверждение теоремы 6 допускает упрощение. Именно, имеет место

Теорема 7. *Пусть D — дискриминант квадратичного поля* (т. е. дискриминант максимального порядка). *Для того чтобы натуральное число $m=as^2$, где a свободно от квадратов, представлялось некоторой бинарной примитивной формой дискриминанта D, необходимо и достаточно, чтобы было разрешимо сравнение*

$$x^2\equiv D \pmod{4a}. \tag{21}$$

Доказательство теоремы 7 мы предоставляем читателю.

7. Подобие модулей в мнимом квадратичном поле. В случае мнимого квадратичного поля $\mathbb{Q}(\sqrt{d})$, $d<0$, существует особенно простой способ решения задачи о подобии модулей.

Геометрическое изображение чисел $\alpha\in\mathbb{Q}(\sqrt{d})$ точками пространства $\mathbb{R}^2$ (см. § 3, п. 1) совпадает с обычным изображением комплексных чисел на плоскости комплексной переменной. Числа полного модуля $M\subset\mathbb{Q}(\sqrt{d})$ изображаются при этом точками (или векторами) некоторой полной решетки в $\mathbb{R}^2$. В дальнейшем в этом пункте мы часто не будем различать комплексные числа и их изображения на плоскости $\mathbb{R}^2$. В связи с этим соответствующая модулю M решетка в $\mathbb{R}^2$ будет обозначаться также через M. Так как умножение всех точек решетки M на комплексное число $\xi\neq 0$ сводится к повороту решетки M (вокруг начала) на угол $\arg\xi$ и к растяжению в $|\xi|$ раз, то для подобных модулей M и ξM соответствующие им решетки подобны в элементарно геометрическом смысле. На этом очевидном свойстве и будет основано наше дальнейшее изложение.

Вопрос о подобии решеток на плоскости решается путем построения в каждой из них некоторого особого базиса, называемого приведенным. Приведенный базис α, β состоит из кратчайшего ненулевого вектора α и кратчайшего из неколлинеарных ему векторов β (подчиненных, сверх того, некоторым дополнительным условиям). Покажем, что в любой решетке M такая пара векторов α и β всегда образует базис. Действительно, если бы это было не так, то в M существовал бы вектор $\xi=u\alpha+v\beta$, у которого вещественные u и v не являются одновременно целыми. Прибавив к этому вектору надлежащую целочисленную линейную комбинацию α и β, мы можем, очевидно, добиться того, чтобы $|u|\leqslant 1/2$ и $|v|\leqslant 1/2$. Если $v\neq 0$, то по выбору β должно

быть $|\xi| \geqslant |\beta|$, что противоречит неравенству

$$|\xi| < |u\alpha| + |v\beta| \leqslant \frac{1}{2}|\alpha| + \frac{1}{2}|\beta| \leqslant |\beta|.$$

Если же $v = 0$, то $|\xi| = |u\alpha| \leqslant \frac{1}{2}|\alpha| < |\alpha|$ вопреки выбору α. Наше утверждение, таким образом, доказано.

Если α — какой-нибудь из кратчайших векторов, а β — кратчайший из неколлинеарных ему векторов, то длина проекции вектора β на вектор α не превосходит $\frac{1}{2}|\alpha|$. В самом деле, среди векторов $\beta + n\alpha$ (n целое) существует, очевидно, вектор с длиной проекции, не превосходящей $\frac{1}{2}|\alpha|$. С другой стороны, из векторов $\beta + n\alpha$ наименьшую длину имеет вектор с наименьшей проекцией.

Рассмотрим теперь для данной решетки M все отличные от нуля кратчайшие векторы и их число обозначим через w. Так как вместе с α вектор $-\alpha$ также будет кратчайшим, то число w четное. Далее, угол между двумя различными кратчайшими векторами α и α' не может быть меньше $\pi/3$, поскольку в противном случае принадлежащий решетке вектор $\alpha - \alpha'$ имел бы меньшую длину. Следовательно, $w \leqslant 6$, а значит, для числа кратчайших векторов возможны лишь следующие значения: $w = 2$, $w = 4$, $w = 6$.

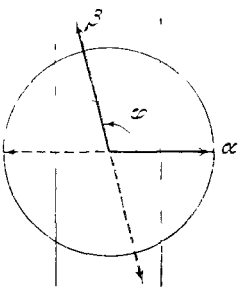

Рис. 1.

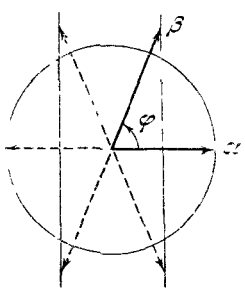

Рис. 2.

Приступим к построению в решетке M *приведенного базиса*. Если $w = 2$, то в качестве α берем любой из двух кратчайших векторов. Среди векторов, неколлинеарных с α, наименьшую длину могут иметь два или четыре вектора (см. рис. 1 и 2). В качестве β мы выбираем тот из них, для которого угол φ, отсчитываемый от α к β в положительном направлении (против часовой стрелки), наименьший. Если же $w = 4$ или $w = 6$, то в качестве приведенного базиса выбираем пару различных крат-

чайших векторов α и β так, чтобы угол φ, отсчитываемый от α к β в положительном направлении, был наименьшим.

Легко видеть, что приведенный базис определяется решеткой однозначно с точностью до поворота, переводящего решетку в себя. Именно в случаях, когда $w=2$ или когда $w=4$, но $\pi/3<\varphi<\pi/2$ (см. рис. 3), имеется два приведенных базиса и они

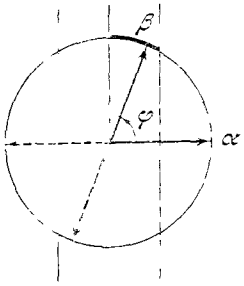

Рис. 3.

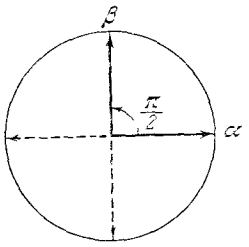

Рис. 4.

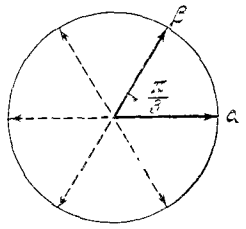

Рис. 5.

переходят друг в друга при повороте на угол, кратный π. При $w=4$, $\varphi=\pi/2$ (рис. 4) мы имеем дело с квадратной решеткой, которая имеет четыре приведенных базиса, переходящих друг в друга при поворотах на углы, кратные $\pi/2$. Наконец, при $w=6$ мы имеем шесть приведенных базисов, которые переходят друг в друга при поворотах на углы, кратные $\pi/3$ (рис. 5; окружность делится на 6 равных частей, так как углы между кратчайшими векторами не могут быть меньше $\pi/3$).

Пользуясь понятием приведенного базиса, теперь уже легко решить вопрос о подобии решеток на плоскости.

Теорема 8. *Решетки M и M_1 в $\mathbb{R}^2$ подобны тогда и только тогда, когда подобны их приведенные базисы* (т. е. переходят друг в друга при повороте и равномерном растяжении).

Доказательство. Пусть α, β и α_1, β_1 — приведенные базисы решеток M и M_1. Если $\xi M=M_1$, то $\xi\alpha$, $\xi\beta$ будет, очевидно, приведенным базисом M_1. Этот базис, как мы видели, при повороте на некоторый угол должен перейти в базис α_1, β_1; поэтому существует такое число η (являющееся корнем степени 1, 2, 4 или 6 из единицы), что $\eta\xi\alpha=\alpha_1$, $\eta\xi\beta=\beta_1$. Таким образом, базис α_1, β_1 получается из базиса α, β поворотом на угол $\arg(\eta\xi)$ и растяжением в $|\eta\xi|$ раз, что и означает подобие этих базисов. Обратное утверждение теоремы очевидно.

Перейдем к описанию классов подобных модулей мнимого квадратичного поля. Пусть M — произвольный модуль в $\mathbb{Q}(\sqrt{d})$, $d<0$, и α, β — какой-нибудь приведенный базис в M. Перейдем к подобному модулю $\frac{1}{\alpha}M=\{1,\gamma\}$, где $\gamma=\beta/\alpha$. Базис 1, γ здесь

также приведенный. Из определения приведенного базиса легко следует, что число γ удовлетворяет условиям:

$$\operatorname{Im}\gamma > 0, \tag{22}$$

$$-1/2 < \operatorname{Re}\gamma \leqslant 1/2, \tag{23}$$

$$\begin{aligned} &|\gamma| > 1, \quad \text{если} \quad -1/2 < \operatorname{Re}\gamma < 0, \\ &|\gamma| \geqslant 1, \quad \text{если} \quad 0 \leqslant \operatorname{Re}\gamma \leqslant 1/2. \end{aligned} \tag{24}$$

Определение. *Число γ из мнимого квадратичного поля называется приведенным, если оно удовлетворяет условиям* (22), (23) *и* (24). *Вместе с γ модуль $\{1, \gamma\}$ также называется приведенным.*

Геометрически условие приведенности числа γ означает, что его изображение на комплексной плоскости принадлежит области Г, указанной на рис. 6 (выделенная часть границы, включая точку i, причисляется к Г, остальная часть — нет).

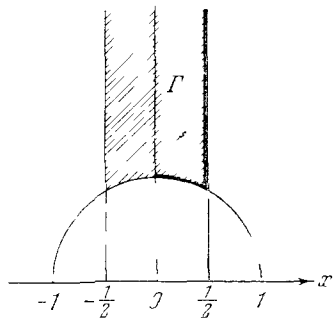

Рис. 6.

Теорема 9. *В каждом классе подобных модулей мнимого квадратичного поля $\mathbb{Q}(\sqrt{d}), d < 0$, содержится один и только один приведенный модуль.*

Доказательство. Тот факт, что в каждом классе имеется приведенный модуль, уже доказан. Остается только проверить, что различные приведенные модули не могут быть подобны. Для этого докажем сначала, что для любого приведенного $\gamma = x + yi$ числа 1, γ образуют приведенный базис решетки $\{1, \gamma\}$. Нам надо убедиться, что γ есть кратчайший из векторов решетки $\{1, \gamma\}$, не лежащих на вещественной прямой, т. е. что $|k + l\gamma| \geqslant |\gamma|$ при любых целых k и $l \neq 0$. Так как $|x| \leqslant 1/2$, то

$$|k \pm \gamma|^2 = (k \pm x)^2 + y^2 \geqslant x^2 + y^2 = |\gamma|^2.$$

Если же $|l| \geqslant 2$, то

$$|k + l\gamma|^2 \geqslant l^2 y^2 > 2y^2 > x^2 + y^2 = |\gamma|^2,$$

что и доказывает наше утверждение. Пусть теперь γ и γ_1 — два приведенных числа. Если модули $\{1, \gamma\}$ и $\{1, \gamma_1\}$ подобны, то по теореме 8 базисы 1, γ и 1, γ_1 подобны. Но это, как легко сообразить, возможно только при $\gamma = \gamma_1$. Теорема 9 этим доказана полностью.

Для полного решения вопроса о подобии модулей в мнимом квадратичном поле нам надо еще иметь алгоритм для нахождения приведенного модуля, подобного заданному. Такой алгоритм

сформулирован в задаче 24. Чтобы узнать, подобны модули M_1 и M_2 или нет, мы находим подобные с ними приведенные модули: исходные модули M_1 и M_2 подобны между собой тогда и только тогда, когда соответствующие им приведенные модули совпадают.

Замечание. В доказательстве теоремы 9 мы фактически нигде не использовали того, что рассматриваемые модули содержатся в некотором мнимом квадратичном поле. Утверждение этой теоремы справедливо, следовательно, для произвольных плоских решеток: *всякая решетка на комплексной плоскости подобна одной и только одной решетке вида* $\{1, \gamma\}$, *где* γ — *некоторое число из области* Г, *указанной на* рис. 6. Согласно лемме 2 (которая без каких бы то ни было изменений применима и к произвольным плоским решеткам) две решетки вида $\{1, \lambda\}$ и $\{1, \gamma\}$ подобны тогда и только тогда, когда числа λ и γ связаны соотношением

$$\lambda = \frac{k\gamma + l}{m\gamma + n}, \qquad kn - ml = \pm 1,$$

с целыми рациональными k, l, m, n. Такая пара невещественных комплексных чисел называется *модулярно эквивалентной*. Полученный нами результат означает, таким образом, что каждое невещественное комплексное число модулярно эквивалентно одному и только одному числу из области Г. Саму область Г часто называют *модулярной фигурой*. Согласно сказанному выше ее точки взаимно однозначно соответствуют классам подобных решеток на плоскости. Задача о подобии плоских решеток встречается в связи с многими вопросами, в особенности в теории эллиптических функций. Каждое поле эллиптических функций задается своей решеткой периодов, причем два поля эллиптических функций изоморфны тогда и только тогда, когда соответствующие им решетки периодов подобны (см., например, [21]). Таким образом, точки модулярной фигуры Г взаимно однозначно соответствуют типам неизоморфных полей эллиптических функций.

Множество всех классов подобных решеток может быть параметризовано также с помощью всех комплексных чисел. Чтобы такую параметризацию указать, достаточно определить взаимно однозначное соответствие между всеми точками модулярной фигуры Г и всеми точками комплексной плоскости. Это можно сделать при помощи модулярных функций, т. е. мероморфных функций $f(z)$, заданных на верхней комплексной полуплоскости $\operatorname{Im} z > 0$ и принимающих равные значения для модулярно эквивалентных точек (при надлежащем уточнении мероморфности в бесконечно удаленной точке). Среди модулярных функций имеется одна особенно важная функция $f(z)$, которая однозначно определяется условиями:

1) область значений $f(z)$ совпадает с множеством всех комплексных чисел;

2) если $f(z)=f(z')$, то z и z' модулярно эквивалентны (т. е. $z'=(kz+l)/(mz+n)$, $kn-ml=1$, с целыми рациональными k, l, m, n) и

3) $$f\left(-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)=1, \quad f(i)=0.$$

Модулярная функция, определенная этими условиями, называется *абсолютным инвариантом* и обозначается через $j(z)$. Функция $j(z)$ дает нам взаимно однозначное соответствие между всеми точками модулярной фигуры Γ и всеми комплексными числами. Следовательно, все значения абсолютного инварианта $j(z)$ описывают также все классы подобных друг другу решеток, и тем самым дают нам параметризацию всех типов неизоморфных полей эллиптических функций.

Модулярная функция $j(z)$ имеет много различных теоретико-числовых приложений. Бо́льшая часть их связана с так называемой теорией комплексного умножения. Согласно этой теории, если точка z верхней полуплоскости соответствует решетке, подобной модулю M с кольцом множителей $\mathfrak{O}$ в некотором квадратичном поле $K=\mathbb{Q}(\sqrt{d})$, $d<0$, то значение $j(z)$ является целым алгебраическим числом, причем степень $(\mathbb{Q}(j(z)):\mathbb{Q})$ равна числу h классов подобных модулей, имеющих порядок $\mathfrak{O}$ своим кольцом множителей (см. [1], [19]).

Рассмотрим теперь классы подобных модулей, принадлежащих некоторому фиксированному порядку $\mathfrak{O}$ с дискриминантом $D<0$. Пусть модуль $\{1, \gamma\}$, $\gamma\in\Gamma$, принадлежит порядку $\mathfrak{O}$. Если для числа γ мы воспользуемся обозначениями леммы 1 и запишем его в виде

$$\gamma=\frac{-b+i\sqrt{|D|}}{2a},$$

то условия (23) и (24) дадут

$$-a\leqslant b<a, \quad c\geqslant a \text{ при } b\leqslant 0, \qquad c>a \text{ при } b>0. \tag{25}$$

Таким образом, чтобы получить полную систему приведенных модулей мнимого квадратичного поля, принадлежащих порядку с дискриминантом D, надо найти все тройки целых чисел $a>0$, b, c, удовлетворяющих неравенствам (25), а также условиям

$$D=b^2-4ac, \quad (a, b, c)=1. \tag{26}$$

Согласно теореме 3 § 6 число таких троек конечно, что, впрочем, ясно и непосредственно, так как в силу неравенств

$$|D|=4ac-b^2\geqslant 4a^2-a^2=3a^2, \qquad |b|\leqslant a<\sqrt{|D|/3},$$

при заданном D для a и b, а значит и для c, мы имеем лишь конечное число возможностей.

Пример 1. Найдем число классов модулей, принадлежащих максимальному порядку поля $\mathbb{Q}(\sqrt{-47})$. Так как здесь $D = -47$, то $|b| \leqslant a < \sqrt{\frac{47}{3}}$. Принимая во внимание, что при нечетном D число b также нечетно, имеем следующие возможности: $b = \pm 1$, $b = \pm 3$. Во втором случае мы должны были бы иметь: $b^2 - D = 56 = 4ac$, $ac = 14$, $3 \leqslant a \leqslant c$, что, однако, невозможно. Если же $b = \pm 1$, то $b^2 - D = 48 = 4ac$, откуда

$$a = 1, \quad c = 12; \quad a = 2, \quad c = 6; \quad a = 3, \quad c = 4.$$

Поскольку случай $b = 1 = a$ должен быть исключен, то получаем, что для максимального порядка поля $\mathbb{Q}(\sqrt{-47})$ имеется 5 классов подобных модулей. Представителями в этих классах являются приведенные модули $\{1, \gamma\}$, где γ равно одному из чисел:

$$\frac{1 + i\sqrt{47}}{2}, \qquad \frac{\pm 1 + i\sqrt{47}}{4}, \qquad \frac{\pm 1 + i\sqrt{47}}{6}.$$

В предшествующем пункте было отмечено, что наличие алгоритма для решения вопроса о подобии модулей в квадратичном поле дает возможность решать уравнения вида (13).

Пример 2. Найдем в модуле $M = \{13, 1 + 5i\}$ все числа с нормой 650. Кольцом множителей здесь является порядок $\mathfrak{O} = \{1, 5i\}$ с дискриминантом $D = -100$. Так как $N(M) = 13$, то мы должны прежде всего выписать модули $A \subset \mathfrak{O}$, принадлежащие порядку $\mathfrak{O}$ и имеющие норму $m = 650/13 = 50$. Условия (18) и (20) дают нам следующие возможности:

1) $s = 5, \quad a = 2, \quad b = -2, \quad c = 13;$
2) $s = 1, \quad a = 50, \quad b = 10, \quad c = 1;$
3) $s = 1, \quad a = 50, \quad b = -10, \quad c = 1;$
4) $s = 1, \quad a = 50, \quad b = -50, \quad c = 13.$

Для каждого из этих четырех случаев составляем модуль A вида (19) и находим подобный с ним приведенный модуль:

$$10\left\{1, \frac{1 + 5i}{2}\right\}, \quad 50\left\{1, \frac{-1 + i}{10}\right\} = (-5 + 5i)\{1, 5i\},$$

$$50\left\{1, \frac{1 + i}{10}\right\} = (5 + 5i)\{1, 5i\}, \quad 50\left\{1, \frac{5 + i}{10}\right\} = 10i\left\{1, \frac{1 + 5i}{2}\right\}.$$

Находим также приведенный модуль для M^{-1}:

$$M^{-1} = \left\{1, \frac{1 - 5i}{13}\right\} = \frac{1 - 5i}{13}\left\{1, \frac{1 + 5i}{2}\right\}.$$

Модули A в случаях 2) и 3) отбрасываются, так как они не подобны M^{-1}. Для оставшихся случаев 1) и 4) равенство $A = \xi M^{-1}$ выполняется при $\xi = 5 + 25i$ и $\xi = -25 + 5i$. Так как в $\mathfrak{O}$

имеется только две единицы: ± 1, то получаем окончательно, что в модуле M имеется четыре числа: $\pm(5+25i)$ и $\pm(-25+5i)$ с нормой 650.

В рассмотренном примере нами установлено также, что уравнение $13x^2+2xy+2y^2=50$ имеет четыре целочисленных решения:

$$x=0,\quad y=5;\qquad x=0,\qquad y=-5;$$
$$x=2,\quad y=-1;\quad x=-2,\quad y=1.$$

Пример 3. Какие натуральные числа представляются формой x^2+y^2?

Дискриминант формы равен $D=-4$. Для порядка $\mathfrak{O}=\{1, i\}$ поля $\mathbb{Q}(\sqrt{-1})$ (дискриминант -4) имеется только один приведенный модуль, так как условия (25) и (26) выполняются лишь при $a=c=1$, $b=0$. Это значит, что все модули, принадлежащие порядку $\mathfrak{O}$, подобны между собой и, следовательно, все бинарные формы дискриминанта -4 эквивалентны форме x^2+y^2. Но эквивалентные формы представляют одни и те же числа, поэтому согласно теореме 6 форма x^2+y^2 представляет число m тогда и только тогда, когда существует модуль $A\subset\mathfrak{O}$, принадлежащий порядку $\mathfrak{O}$ и имеющий норму m. Если такой модуль существует, то при некоторых s, a, b, c справедливы равенства:

$$m=as^2,\quad D=-4=b^2-4ac,\qquad (a, b, c)=1.$$

Число b здесь необходимо четное, $b=2z$, причем z удовлетворяет сравнению

$$z^2\equiv -1 \pmod a. \tag{27}$$

Обратно, если последнее сравнение при некотором $a=m/s^2$ разрешимо, т. е. $z^2=-1+ac$, то, как легко видеть, $(a, 2z, c)=1$, а значит, существует модуль $A\subset\mathfrak{O}$, принадлежащий порядку $\mathfrak{O}$, с нормой m, т. е. m представляется формой x^2+y^2.

Сравнение (27), как известно, разрешимо тогда и только тогда, когда a не делится на 4 и не делится на простое число вида $4k+3$. Так как a содержит все простые множители, входящие в m в нечетной степени, то получаем окончательно, что m представляется формой x^2+y^2 тогда и только тогда, когда простые числа вида $4k+3$ входят в m только в четной степени.

Задачи

1. Найти основные единицы в полях $\mathbb{Q}(\sqrt{19})$ и $\mathbb{Q}(\sqrt{37})$.

2. Доказать, что если $d\equiv 1 \pmod 8$ (и свободно от квадратов), то основная единица порядка $\{1, \sqrt{d}\}$ является также основной единицей и максимального порядка поля $\mathbb{Q}(\sqrt{d})$, $d>0$.

3. Доказать, что если дискриминант некоторого порядка $\mathfrak{O}$ в квадратичном поле делится хоть на одно простое число вида $4n+3$, то норма всякой единицы из $\mathfrak{O}$ равна $+1$.

4. Пусть целое рациональное $m > 1$ не является полным квадратом. Показать, что при разложении $\sqrt{m}$ в непрерывную дробь последовательность неполных частных имеет вид

$$q_0, q_1, \ldots, q_s, 2q_0, q_1, \ldots, q_s, 2q_0, q_1, \ldots$$

(при этом $q_{t+1} = q_{s-t}$, $t = 0, 1, \ldots, s-1$).

5. В тех же обозначениях показать, что если P_s/Q_s — подходящая дробь, соответствующая предпоследнему члену наименьшего периода, то $P_s + Q_s\sqrt{m}$ является основной единицей порядка $\{1, \sqrt{m}\}$ (в поле $\mathbb{Q}(\sqrt{m})$).

6. Пусть для модулей M_1 и M_2 квадратичного поля кольцами множителей являются порядки $\mathfrak{O}_{f_1}$ и $\mathfrak{O}_{f_2}$ соответственно (относительно обозначений см. конец п. 2). Показать, что для произведения M_1M_2 кольцом множителей является порядок $\mathfrak{O}_f$, где f — общий наибольший делитель f_1 и f_2.

7. Для всякого натурального f через $\mathfrak{G}_f$ обозначим группу модулей данного квадратичного поля, принадлежащих порядку $\mathfrak{O}_f$ (см. конец п. 4). Показать, что если d есть делитель f, то отображение $M \to M\mathfrak{O}_d$ ($M \in \mathfrak{G}_f$ является гомоморфизмом группы $\mathfrak{G}_f$ на группу $\mathfrak{G}_d$).

8. Пусть ξ — число из максимального порядка $\widetilde{\mathfrak{O}} = \{1, \omega\}$ квадратичного поля, взаимно простое с натуральным f. Показать, что кольцом множителей для модуля $M = \{f, f\omega, \xi\}$ является $\mathfrak{O}_f$, а также что $M\widetilde{\mathfrak{O}} = \widetilde{\mathfrak{O}}$. Показать, далее, что, и обратно, всякий модуль M, принадлежащий порядку $\mathfrak{O}_f$ и обладающий свойством $M\widetilde{\mathfrak{O}} = \widetilde{\mathfrak{O}}$, имеет вид $M = \{f, f\omega, \xi\}$ при некотором $\xi \in \widetilde{\mathfrak{O}}$, взаимно простом с f.

9. Пусть ξ_1 и ξ_2 — два числа из $\widetilde{\mathfrak{O}}$, взаимно простые с f. Доказать, что равенство $\{f, f\omega, \xi_1\} = \{f, f\omega, \xi_2\}$ имеет место тогда и только тогда, когда $s\xi_1 \equiv \xi_2 \pmod f$ при некотором целом рациональном s.

10. Доказать, что для произвольных полных модулей M_1 и M_2 квадратичного поля (не обязательно принадлежащих одному и тому же порядку) справедлива формула

$$N(M_1M_2) = N(M_1)N(M_2).$$

11. Доказать, что число классов h подобных модулей, принадлежащих максимальному порядку $\widetilde{\mathfrak{O}}$ квадратичного поля, и число классов h_f подобных модулей, принадлежащих порядку $\mathfrak{O}_f$ (индекса f), связаны между собой соотношением

$$h_f = h\frac{\Phi(f)}{e_f\varphi(f)},$$

где $\Phi(f)$ — число классов вычетов в $\widetilde{\mathfrak{O}}$ по модулю f, состоящих из чисел, взаимно простых с f (аналог функции Эйлера $\varphi(f)$), а e_f — индекс группы единиц порядка $\mathfrak{O}_f$ в группе единиц максимального порядка $\widetilde{\mathfrak{O}}$.

12. Число γ вещественного квадратичного поля называется *приведенным*, если оно само удовлетворяет условию $0 < \gamma < 1$, а для сопряженного с ним числа γ' справедливо неравенство $\gamma' < -1$. Вместе с γ модуль $\{1, \gamma\}$ также называется приведенным. Доказать, что в обозначениях леммы 1 приведенность числа γ равносильна выполнению неравенств

$$0 < b < \sqrt{D}, \quad -b + \sqrt{D} < 2a < b + \sqrt{D}.$$

Вывести отсюда, что число приведенных модулей, принадлежащих фиксированному порядку вещественного квадратичного поля, конечно.

13. Пусть γ — иррациональное число вещественного квадратичного поля, удовлетворяющее условию $0 < \gamma < 1$, $\operatorname{Irr}\gamma > 0$. Положим

$$\gamma_1 = -(\operatorname{sgn}\gamma')\frac{1}{\gamma} - n,$$

где целое рациональное число n выбрано так, что $0 < \gamma_1 < 1$. Доказать, что в результате конечного числа преобразований $\{1, \gamma\} \to \{1, \gamma_1\}$ модуль $\{1, \gamma\}$ перейдет в подобный с ним приведенный модуль. Таким образом, в каждом классе подобных модулей (в обычном смысле) вещественного квадратичного поля имеется приведенный модуль.

14. Пусть γ — приведенное число вещественного квадратичного поля. Так как $\operatorname{sgn}\gamma' = -1$, то преобразование $\gamma \to \gamma_1$ предшествующей задачи для приведенного γ имеет вид

$$\gamma_1 = \frac{1}{\gamma} - n, \qquad n = \left[\frac{1}{\gamma}\right].$$

Доказать, что вместе с γ число γ_1 также приведенное. Оно называется соседним справа к числу γ. Исходное число γ называется при этом соседним слева для γ_1. Проверить, что для любого приведенного числа γ_1 всегда существует, и притом только одно, соседнее слева к нему приведенное число γ.

15. Отправляясь от приведенного числа γ_0 вещественного квадратичного поля, построим последовательность приведенных чисел $\gamma_0, \gamma_1, \gamma_2, \ldots$, в которой каждое последующее число является соседним справа для предыдущего. При некотором натуральном m имеет место равенство $\gamma_m = \gamma_0$, т. е. наша последовательность приведенных чисел периодическая. Если m выбрано наименьшим, то числа $\gamma_0, \gamma_1, \ldots, \gamma_{m-1}$ различны. Такая конечная последовательность приведенных чисел называется периодом. Доказать, что два приведенных модуля $\{1, \gamma\}$ и $\{1, \gamma^*\}$ подобны (в обычном смысле) тогда и только тогда, когда приведенные числа γ и γ^* принадлежат одному и тому же периоду.

16. Найти число классов подобных модулей, принадлежащих максимальному порядку поля $\mathbb{Q}(\sqrt{10})$.

17. Показать, что все целочисленные решения уравнения

$$17x^2 + 32xy + 14y^2 = 9$$

определяются равенствами

$$\pm(15 + 6\sqrt{2})(3 + 2\sqrt{2})^n = \pm[17x_n + (16 + 3\sqrt{2})y_n]$$

(при всех целых n).

18. Какие из модулей

$$\{1, \sqrt{15}\}, \quad \{2, 1 + \sqrt{15}\}, \quad \{3, \sqrt{15}\}, \quad \{35, 20 + \sqrt{15}\}$$

поля $\mathbb{Q}(\sqrt{15})$ подобны между собой?

19. Найти полную систему представителей в классах собственно эквивалентных примитивных форм с дискриминантом 252.

20. Сколько существует классов собственно эквивалентных примитивных форм с дискриминантом 360?

21. Какие простые числа представляются формами $x^2 + 5y^2$, $2x^2 + 2xy + 3y^2$?

22. Решить в целых числах уравнения:

1) $5x^2 + 2xy + 2y^2 = 26$;
2) $5x^2 - 2y^2 = 3$;
3) $80x^2 - y^2 = 16$.

23. Показать, что уравнения:

1) $13x^2 + 34xy + 22y^2 = 23$;
2) $5x^2 + 16xy + 13y^2 = 23$

не имеют целочисленных решений.

24. Пусть число γ из мнимого квадратичного поля удовлетворяет условиям $\operatorname{Im}\gamma > 0$, $-1/2 < \operatorname{Re}\gamma \leqslant 1/2$, но не является приведенным. Положим

$\gamma_1 = -\frac{1}{\gamma} + n$, где целое рациональное n выбрано так, что $-1/2 < \operatorname{Re}\gamma_1 \leqslant 1/2$. Если γ_1 не приведенное, то аналогично полагаем $\gamma_2 = -\frac{1}{\gamma_1} + n_1$ и т. д. Доказать, что в результате конечного числа таких преобразований модуль $\{1, \gamma\}$ перейдет в подобный с ним приведенный модуль $\{1, \gamma_s\}$.

25. Найти число классов подобных модулей, принадлежащих максимальному порядку поля $\mathbb{Q}(\sqrt{-47})$.

26. Найти в модуле $\{13, 1+5i\}$ все числа с нормой 650.

27. Определить кольца множителей для модулей

$$\{11, 6+2i\sqrt{2}\}, \quad \{2, 1+i\sqrt{2}\}, \quad \{4, i\sqrt{2}\}, \quad \{2, i\sqrt{2}\}.$$

Какие из этих модулей подобны между собой?

28. Показать, что в поле $\mathbb{Q}(\sqrt{-43})$ все модули с максимальным порядком в качестве кольца множителей подобны между собой.

Глава III

ТЕОРИЯ ДЕЛИМОСТИ

В предшествующей главе мы видели пример того, как решение теоретико-числовой задачи приводит к рассмотрению глубоких вопросов теории алгебраических чисел: нахождение целочисленных представлений рациональных чисел полными разложимыми формами оказалось тесно связанным с теорией единиц в порядках полей алгебраических чисел.

Еще большее количество задач теории чисел приводит к другому важному вопросу арифметики полей алгебраических чисел — к вопросу о разложении алгебраических чисел на простые множители.

В настоящей главе мы построим общую теорию разложения алгебраических чисел на множители и дадим ее приложения к некоторым задачам теории чисел. Необходимые здесь сведения из теории колец изложены в § 4 Дополнения. Эти сведения вместе с теми свойствами конечных расширений полей, которыми мы уже пользовались во второй главе, составят алгебраический аппарат этой главы.

С разложением алгебраических чисел на множители особенно тесно связана теорема Ферма. Исторически именно занятия теоремой Ферма привели Куммера к его работам по арифметике алгебраических чисел, содержащим ряд основных для этой области идей.

Мы начнем поэтому с изложения первого результата Куммера по теореме Ферма как с теоретико-числового введения в общую теорию разложения алгебраических чисел на простые множители.

§ 1. Некоторые частные случаи теоремы Ферма

1. Связь теоремы Ферма с разложением на множители. Предположение, высказанное Ферма, заключается в том, что уравнение

$$x^n + y^n = z^n$$

при $n > 2$ не имеет решений в отличных от нуля целых рациональных числах x, y, z.

Очевидно, что если теорема Ферма доказана для некоторого показателя n, то тем самым она доказана и для всех показателей, кратных n. Так как всякое целое $n > 2$ делится или на 4, или на нечетное простое число, то можно поэтому ограничиться случая-

ми, когда показатель равен либо 4, либо нечетному простому числу. Для $n=4$ элементарное доказательство теоремы Ферма дано самим Ферма. Мы ограничимся в дальнейшем изучением уравнения

$$x^l+y^l=z^l, \tag{1}$$

в котором показатель l есть нечетное простое число. Очевидно, что в уравнении (1) числа x, y, z можно считать попарно взаимно простыми.

Для тех значений l, для которых доказательство теоремы Ферма найдено, оно обычно разбивается на два случая: во-первых, доказывается, что уравнение (1) не имеет решений в целых x, y, z, не делящихся на l, и, во-вторых, что оно не имеет решений в целых x, y, z, среди которых одно (и только одно) делится на l. Эти два случая называются соответственно *первым и вторым случаями* теоремы Ферма. Из имеющихся в настоящее время доказательств различных частных случаев можно, по-видимому, сделать вывод, что принципиальные трудности в первом и втором случаях теоремы Ферма приблизительно одинаковы, хотя технически первый случай рассматривается проще. Мы займемся здесь лишь первым случаем теоремы Ферма.

Связь теоремы Ферма с задачей о разложении алгебраических чисел на простые множители выясняется из следующих простых соображений. Если через ζ мы обозначим первообразный корень l-й степени из 1, то уравнение (1) можно будет переписать в виде

$$\prod_{k=0}^{l-1}(x+\zeta^k y)=z^l. \tag{2}$$

Для целых рациональных чисел из того, что произведение нескольких взаимно простых множителей является l-й степенью, следует в силу однозначности разложения на простые множители, что каждый сомножитель в отдельности также есть l-я степень. Множители в левой части равенства (2) принадлежат полю алгебраических чисел $\mathbb{Q}(\zeta)$ степени $l-1$ над $\mathbb{Q}$ (легко показать, что многочлен $t^{l-1}+t^{l-2}+\ldots+t+1$ при простом l неприводим над полем рациональных чисел; см., например, задачу 6 или теорему 1 § 2 гл. V). Рассмотрим в поле $\mathbb{Q}(\zeta)$ порядок $\mathfrak{O}=\{1, \zeta, \ldots, \zeta^{l-2}\}$ (согласно теореме 1 § 5 гл. V $\mathfrak{O}$ является максимальным порядком поля $\mathbb{Q}(\zeta)$). Предположим, что в кольце $\mathfrak{O}$ разложение чисел на простые множители однозначно. Тогда для любого $\alpha\in\mathfrak{O}$, $\alpha\neq 0$, в разложении $\alpha=\varepsilon\pi_1^{a_1}\ldots\pi_r^{a_r}$, где ε — единица кольца $\mathfrak{O}$, а простые числа $\pi_1, \ldots, \pi_r$ попарно не ассоциированы, показатели $a_1, \ldots, a_r$ определены однозначно (см. § 2, п. 2). Ясно, что каждое простое число π, входящее в разложение числа z^l, входит в это разложение с показателем, кратным l. С другой стороны, ниже будет доказано, что, когда мы имеем дело с первым случаем теоремы Ферма, числа $x+\zeta^k y$ ($k=0, 1, \ldots$

..., $l-1$) попарно взаимно просты. Следовательно, если мы $x+\zeta^k y$ представим в виде произведения степеней простых множителей, то каждое простое число из этого разложения будет входить в него с показателем, также кратным l. Это значит, что каждое $x+\zeta^k y$ с точностью до множителя, являющегося единицей, будет l-й степенью. В частности,

$$x+\zeta y=\varepsilon\alpha^l, \tag{3}$$

где ε — единица кольца $\mathfrak{O}$ и $\alpha\in\mathfrak{O}$.

Так как равенство $x^l+y^l=z^l$ ввиду нечетности l может быть записано также в виде $x^l+(-z)^l=(-y)^l$, то аналогичным образом мы получим

$$x-\zeta z=\varepsilon_1\alpha_1^l. \tag{3'}$$

Равенства (3) и (3'), оказывается, уже сравнительно легко могут быть приведены к противоречию. Если это будет сделано, то тем самым будет доказана неразрешимость уравнения (1) в целых x, y, z, не делящихся на l (при сделанном предположении относительно кольца $\mathfrak{O}$).

После этих вводных замечаний установим несколько вспомогательных фактов, относящихся к свойствам кольца $\mathfrak{O}$.

2. Кольцо $\mathbb{Z}[\zeta]$. Лемма 1. *В кольце $\mathfrak{O}=\mathbb{Z}[\zeta]$ число $1-\zeta$ является простым, и для l имеем разложение*

$$l=\varepsilon^*(1-\zeta)^{l-1}, \tag{4}$$

где ε^* — единица в $\mathfrak{O}$.

Доказательство. Полагая в разложении

$$t^{l-1}+t^{l-2}+\ldots+t+1=(t-\zeta)(t-\zeta^2)\ldots(t-\zeta^{l-1})$$

t равным 1, получим

$$l=(1-\zeta)(1-\zeta^2)\ldots(1-\zeta^{l-1}). \tag{5}$$

Если $\alpha=r(\zeta)$ — произвольное число поля $\mathbb{Q}(\zeta)$ (здесь $r(t)$ — многочлен с рациональными коэффициентами), то числа

$$\sigma_k(\alpha)=r(\zeta^k), \quad 1\leqslant k\leqslant l-1 \tag{6}$$

мы можем рассматривать как образы α при изоморфизмах $\mathbb{Q}(\zeta)$ в поле всех комплексных чисел. Другими словами, числа (6) согласно терминологии п. 3 § 2 Дополнения являются сопряженными для α, а значит, $N(\alpha)=\prod_{k=1}^{l-1} r(\zeta^k)$. В частности, при $s\not\equiv 0 \pmod l$ мы имеем

$$N(1-\zeta^s)=\prod_{k=1}^{l-1}(1-\zeta^{ks})=\prod_{k=1}^{l-1}(1-\zeta^k)=l.$$

Отсюда следует, что $1-\zeta$, $1-\zeta^2$, ..., $1-\zeta^{l-1}$ являются простыми числами в кольце $\mathfrak{O}$. Действительно, если $1-\zeta^s=\alpha\beta$, то $N(\alpha)N(\beta)=l$, а потому либо $N(\alpha)=1$, либо $N(\beta)=1$, т. е. один из сомножителей необходимо является единицей (теорема 4 § 2 гл. II). Переходя в равенстве

$$(1-\zeta^s)=(1-\zeta)(1+\zeta+\ldots+\zeta^{s-1})=(1-\zeta)\varepsilon_s \qquad (7)$$

к нормам, получаем, что $N(\varepsilon_s)=1$, а значит, ε_s — единица в $\mathfrak{O}$. Таким образом, все числа $1-\zeta^s$ при $s\not\equiv 0 \pmod{l}$ ассоциированы с $1-\zeta$. Разложение (4) вытекает теперь из (5) и (7).

Лемма 2. *Если целое рациональное число a делится на $1-\zeta$ (в кольце $\mathfrak{O}$), то оно делится и на l.*

Доказательство. Пусть $a=(1-\zeta)\alpha$, где $\alpha\in\mathfrak{O}$. Переходя в этом равенстве к нормам, получим $a^{l-1}=lN(\alpha)$, где $N(\alpha)$ целое рациональное. Так как l простое, то a делится на l.

Лемма 3. *Все корни из 1, содержащиеся в поле $\mathbb{Q}(\zeta)$, исчерпываются корнями степени $2l$ из 1.*

Доказательство. Все корни из 1, содержащиеся в $\mathbb{Q}(\zeta)$, принадлежат, очевидно, максимальному порядку. Согласно теореме 2 § 3 гл. II все они образуют конечную циклическую группу. Обозначим через m порядок этой группы и через η какой-нибудь первообразный корень степени m из 1. Так как $-\zeta$ принадлежит $\mathbb{Q}(\zeta)$ и является первообразным корнем степени $2l$ из 1, то m делится на $2l$. В § 2 гл. V (следствие теоремы 1) нами будет доказано, что степень поля $\mathbb{Q}(\eta)$ над $\mathbb{Q}$ равна $\varphi(m)$, где $\varphi(m)$ — теоретико-числовая функция Эйлера. Положим

$$m=l^r m_0, \quad (m_0, l)=1, \quad r\geqslant 1, \quad m_0\geqslant 2.$$

Так как $\mathbb{Q}(\eta)$ содержится в $\mathbb{Q}(\zeta)$, а степень последнего поля равна $l-1$, то $\varphi(m)=l^{r-1}(l-1)\varphi(m_0)\leqslant l-1$. Из этого неравенства следует, что $r=1$ и $\varphi(m_0)=1$. Так как условия $\varphi(m_0)=1$ и $m_0\geqslant 2$ возможны лишь при $m_0=2$, то $m=2l$, и лемма 3 доказана.

Лемма 4 (лемма Куммера). *Всякая единица кольца $\mathfrak{O}$ является произведением степени ζ на вещественную единицу.*

Доказательство. Пусть

$$\varepsilon=a_0+a_1\zeta+\ldots+a_{l-2}\zeta^{l-2}=r(\zeta), \qquad a_i\in\mathbb{Z}$$

— произвольная единица кольца $\mathfrak{O}$. Очевидно, что комплексно сопряженное число $\bar{\varepsilon}=r(\zeta^{-1})=r(\zeta^{l-1})$ также будет единицей кольца $\mathfrak{O}$. Рассмотрим единицу $\mu=\varepsilon/\bar{\varepsilon}\in\mathfrak{O}$. В силу (6) числа, сопряженные с μ, имеют вид

$$\sigma_k(\mu)=r(\zeta^k)/r(\zeta^{(l-1)k})=r(\zeta^k)/r(\zeta^{-k}).$$

Так как $r(\zeta^k)$ и $r(\zeta^{-k})$ комплексно сопряжены между собой, то $|\sigma_k(\mu)|=1$ (при всех $k=1, \ldots, l-1$). По теореме 2 § 3 гл. II μ

есть корень из 1, а значит, в силу леммы 3

$$\mu = \pm\zeta^a.$$

Покажем, что в правой части этого равенства стоит знак плюс. Действительно, в противном случае мы имели бы равенство

$$\varepsilon = -\zeta^a\bar{\varepsilon}.$$

Рассмотрим его как сравнение в кольце $\mathfrak{O}$ по модулю $\lambda = 1-\zeta$. Так как $\zeta \equiv 1 \pmod{\lambda}$, то все степени ζ также сравнимы с 1 по модулю λ, и мы получаем

$$\varepsilon \equiv \bar{\varepsilon} \equiv a_0 + a_1 + \ldots + a_{l-2} = M \pmod{\lambda},$$

а значит, $M \equiv -M \pmod{\lambda}$, или $2M \equiv 0 \pmod{\lambda}$. В силу леммы 2 отсюда следует, что

$$2M \equiv 0 \pmod{l}, \quad M \equiv 0 \pmod{l}, \quad M \equiv 0 \pmod{\lambda},$$

откуда $\varepsilon \equiv 0 \pmod{\lambda}$, а это противоречит тому, что ε — единица кольца $\mathfrak{O}$. Таким образом, $\varepsilon = \zeta^a\bar{\varepsilon}$.

Найдем теперь такое целое число s, что $2s \equiv a \pmod{l}$. Тогда $\zeta^a = \zeta^{2s}$ и равенство $\varepsilon = \zeta^{2s}\bar{\varepsilon}$ можно переписать в виде

$$\varepsilon/\zeta^s = \zeta^s\bar{\varepsilon} = \bar{\varepsilon}/\zeta^{-s} = \overline{(\varepsilon/\zeta^s)}.$$

Полученное равенство означает, что единица $\eta = \varepsilon/\zeta^s$ вещественна. Таким образом, ε представляется в виде произведения ζ^s на вещественную единицу η, что и требовалось доказать.

Лемма 5. *Пусть x и y — целые рациональные числа. Для того чтобы $x+\zeta^m y$ и $x+\zeta^n y$ при $m \not\equiv n \pmod{l}$ были взаимно просты* (т. е. чтобы единицы были их единственными общими делителями), *необходимо и достаточно, чтобы, во-первых, x и y были взаимно просты и, во-вторых, чтобы $x+y$ не делилось на l.*

Доказательство. Если x и y имеют общий делитель $d > 1$, то $x+\zeta^m y$ и $x+\zeta^n y$, очевидно, делятся на d. Если же $x+y$ делится на l, то $x+\zeta^m y$ и $x+\zeta^n y$ имеют общий делитель $1-\zeta$ (не являющийся единицей). В самом деле,

$$x+\zeta^m y = x+y+(\zeta^m-1)y = (x+y)-(1-\zeta)\varepsilon_m y \equiv 0 \pmod{1-\zeta}.$$

Таким образом, необходимость обоих условий доказана. Для доказательства достаточности мы покажем, что в кольце $\mathfrak{O}$ существуют такие ξ_0 и η_0, что

$$(x+\zeta^m y)\xi_0 + (x+\zeta^n y)\eta_0 = 1.$$

Рассмотрим совокупность A всех чисел вида

$$(x+\zeta^m y)\xi + (x+\zeta^n y)\eta,$$

где ξ и η независимо друг от друга пробегают все числа из $\mathfrak{O}$. Очевидно, что если α и β принадлежат A, то и любая их линей-

ная комбинация $\alpha\xi' + \beta\eta'$ с коэффициентами ξ', η' из $\mathfrak{O}$ также принадлежат A. Нам надо доказать, что число 1 принадлежит A.

Из равенств

$$(x + \zeta^m y) - (x + \zeta^n y) = \zeta^m(1 - \zeta^{n-m})y = \zeta^m \varepsilon_{n-m}(1 - \zeta)y,$$

$$(x + \zeta^m y)\zeta^n - (x + \zeta^n y)\zeta^m = -\zeta^m(1 - \zeta^{n-m})x = -\zeta^m \varepsilon_{n-m}(1 - \zeta)x$$

заключаем, что $(1-\zeta)y \in A$ и $(1-\zeta)x \in A$ (так как $\zeta^m \varepsilon_{n-m}$ — единица кольца $\mathfrak{O}$). В силу взаимной простоты x и y существуют такие целые рациональные a и b, что $ax + by = 1$, поэтому

$$(1-\zeta)xa + (1-\zeta)yb = 1 - \zeta \in A.$$

Далее,

$$x + y = (x + \zeta^m y) + (1 - \zeta^m)y = (x + \zeta^m y) + (1 - \zeta)\varepsilon_m y,$$

а значит, $x + y \in A$. Так как l делится на $1 - \zeta$, то $l \in A$. Согласно второму условию леммы числа $x + y$ и l взаимно просты. Следовательно, при некоторых целых рациональных u и v имеем $(x + y)u + lv = 1$, откуда и следует, что $1 \in A$. Лемма 5, таким образом, доказана.

3. Теорема Ферма в случае однозначности разложения на множители. Теорема 1. *Пусть l — простое нечетное число и ζ — первообразный корень степени l из 1. Если в порядке $\mathfrak{O} = \mathbb{Z}[\zeta] = \{1, \zeta, \ldots, \zeta^{l-2}\}$ поля $\mathbb{Q}(\zeta)$ разложение на простые множители однозначно, то для показателя l справедлив первый случай теоремы Ферма, т. е. уравнение*

$$x^l + y^l = z^l$$

не имеет решений в целых рациональных числах x, y, z, не делящихся на l.

Доказательство. Простое число 3 будет играть в нашем доказательстве особую роль, поэтому случай $l = 3$ рассмотрим отдельно. Покажем, что не только уравнение $x^3 + y^3 = z^3$, но и сравнение $x^3 + y^3 \equiv z^3 \pmod 9$ не имеет решений в числах, не делящихся на 3. В самом деле, допустим, что последнее сравнение имеет место. Тогда из сравнения $x^3 + y^3 \equiv z^3 \pmod 3$ будет следовать (в силу малой теоремы Ферма) $x + y \equiv z \pmod 3$, т. е. $z = x + y + 3u$, а значит,

$$x^3 + y^3 \equiv (x + y + 3u)^3 \equiv x^3 + y^3 + 3x^2y + 3xy^2 \pmod 9,$$

откуда $0 \equiv x^2y + xy^2 = xy(x + y) \equiv xyz \pmod 3$.

Таким образом, одно из чисел x, y, z должно делиться на 3, и наше утверждение доказано.

Пусть теперь $l \geqslant 5$. Доказывая теорему от противного, предположим, что для некоторых целых рациональных x, y, z, попарно взаимно простых и не делящихся на l, имеет место равенство $x^l + y^l = z^l$, которое мы можем записать также в виде (2). Так как $x + y \equiv x^l + y^l \equiv z \not\equiv 0 \pmod l$ и, кроме того, x и y взаимно

просты, то по лемме 5 все числа $x+\zeta^k y$ $(k=0, 1, \ldots, l-1)$ попарно взаимно просты. А тогда, как уже было показано в п. 1, ввиду однозначности разложения на простые множители из (2) следуют равенства

$$x+\zeta y=\varepsilon\alpha^l, \tag{3}$$

$$x-\zeta z=\varepsilon_1\alpha_1^l, \tag{3'}$$

в которых ε и ε_1 — единицы кольца $\mathfrak{O}$. Мы уже отмечали, что наличие равенств (3) и (3′) ведет к противоречию. Более того, мы покажем сейчас, что противоречивыми оказываются даже соответствующие сравнения в кольце $\mathfrak{O}$ по модулю l.

Пусть $\alpha=a_0+a_1\zeta+\ldots+a_{l-2}\zeta^{l-2}$ с целыми рациональными a_0, $a_1, \ldots, a_{l-2}$. Тогда

$$\alpha^l\equiv a_0^l+a_1^l\zeta^l+\ldots+a_{l-2}^l\zeta^{l(l-2)}\equiv M \pmod l,$$

где $M=a_0+a_1+\ldots+a_{l-2}$. В силу леммы Куммера единица ε может быть представлена в виде $\varepsilon=\zeta^s\eta$, где η — вещественная единица. Следовательно, из равенства (3) получаем сравнение

$$x+\zeta y\equiv\zeta^s\eta M=\zeta^s\xi \pmod l$$

с вещественным числом $\xi\in\mathfrak{O}$. Это сравнение мы можем также переписать в виде

$$\zeta^{-s}(x+\zeta y)\equiv\xi \pmod l. \tag{8}$$

Заметим теперь, что для любого $\alpha\in\mathfrak{O}$ комплексно сопряженное число $\bar{\alpha}$ также принадлежит $\mathfrak{O}$. Если мы имеем сравнение $\alpha\equiv\beta \pmod l$, то $\alpha-\beta=l\gamma$, откуда $\bar{\alpha}-\bar{\beta}=l\bar{\gamma}$ и, следовательно, $\bar{\alpha}\equiv\bar{\beta} \pmod l$. Переходя в сравнении (8) к комплексно сопряженным числам, получим

$$\zeta^s(x+\zeta^{-1}y)\equiv\bar{\xi} \pmod l. \tag{9}$$

Но $\bar{\xi}=\xi$, поэтому из (8) и (9) следует, что

$$\zeta^{-s}(x+\zeta y)\equiv\zeta^s(x+\zeta^{-1}y) \pmod l,$$

или

$$x\zeta^s+y\zeta^{s-1}-x\zeta^{-s}-y\zeta^{1-s}\equiv 0 \pmod l. \tag{10}$$

Очевидно, что произвольное число из $\mathfrak{O}$, представленное в каноническом виде $a_0+a_1\zeta+\ldots+a_{l-2}\zeta^{l-2}$, делится на l тогда и только тогда, когда все коэффициенты $a_0, \ldots, a_{l-2}$ делятся на l. Если показатели

$$s,\quad s-1,\quad -s,\quad 1-s \tag{11}$$

попарно не сравнимы между собой и не сравнимы с $l-1$ по модулю l, то число, стоящее в левой части сравнения (10), будет иметь канонический вид, а тогда из этого сравнения должно следовать, что все коэффициенты делятся на l. Таким образом, в этом

случае $x \equiv 0 \pmod{l}$ и $y \equiv 0 \pmod{l}$, что, однако, невозможно, так как x и y взаимно просты (и не делятся на l).

Рассмотрим теперь те случаи, когда левая часть сравнения (10) не является каноническим представлением, т. е. когда среди чисел (11) имеются сравнимые с $l-1$ или сравнимые между собой по модулю l. Один из показателей (11) будет сравним с $l-1$ по модулю l лишь при следующих значениях (по модулю l) этих показателей:

s	$s-1$	$-s$	$1-s$
$l-1$	$l-2$	1	2
0	$l-1$	0	1
1	0	$l-1$	0
2	1	$l-2$	$l-1$

Мы видим, что в каждом из этих случаев имеется только один показатель, сравнимый с $l-1$ (ибо $l \geqslant 5$). Для того чтобы левую часть сравнения (10) записать в канонической форме, надо воспользоваться равенством

$$\zeta^{l-1} = -1 - \zeta - \ldots - \zeta^{l-2}.$$

Подставляя это выражение в тот член левой части (10), в котором показатель сравним с $l-1$ по модулю l, мы получим вместо этого члена сумму одночленов $1, \zeta, \ldots, \zeta^{l-2}$ с коэффициентами $\pm x$ или $\pm y$. Так как число этих одночленов равно $l-1 \geqslant 4$ (ибо $l \geqslant 5$), то при приведении подобных членов хоть один из них не сократится с оставшимися тремя членами левой части сравнения (10). Но тогда из сравнения (10), левая часть которого уже записана в каноническом виде, будет следовать $\pm x \equiv 0 \pmod{l}$ или $\pm y \equiv 0 \pmod{l}$, что опять невозможно, так как x и y, по предположению, не делятся на l.

Остается рассмотреть еще случай, когда среди показателей (11) имеются сравнимые между собой по модулю l. Сравнения $s \equiv s-1 \pmod{l}$ и $-s \equiv 1-s \pmod{l}$, очевидно, вообще невозможны. Если $s \equiv -s \pmod{l}$ или $s-1 \equiv 1-s \pmod{l}$, то имеем соответственно $s \equiv 0 \pmod{l}$ и $s \equiv 1 \pmod{l}$, что отвечает уже разобранным случаям $s-1 \equiv l-1 \pmod{l}$ и $-s \equiv l-1 \pmod{l}$. Из двух оставшихся возможностей $s \equiv 1-s \pmod{l}$ и $s-1 \equiv -s \pmod{l}$ следует, что $s \equiv (l+1)/2 \pmod{l}$. В этом случае сравнение (10) принимает вид

$$(x-y)\zeta^{(l+1)/2} + (y-x)\zeta^{(l-1)/2} \equiv 0 \pmod{l}.$$

Так как левая часть этого сравнения записана в каноническом виде (показатели $(l+1)/2$ и $(l-1)/2$ не сравнимы между собой и

не сравнимы с $l-1$), то из него следует, что

$$x \equiv y \pmod{l}.$$

Аналогичным образом из (3′) мы получим

$$x \equiv -z \pmod{l}.$$

Из сравнения $x+y \equiv x^l+y^l=z^l \equiv z \pmod{l}$ следует теперь, что $2x \equiv -x \pmod{l}$ или $3x \equiv 0 \pmod{l}$. Так как $l \neq 3$, то $x \equiv 0 \pmod{l}$, и мы снова пришли к противоречию. Этим доказательство теоремы 1 закончено.

Применяя более тонкие свойства целых чисел поля $\mathbb{Q}(\zeta)$, Куммер доказал, что если простое число l удовлетворяет условию теоремы 1, то для показателя l справедлив и второй случай теоремы Ферма.

Обобщение теоремы 1 на более широкий класс показателей l будет приведено в п. 3 § 7 настоящей главы. Для тех же показателей l второй случай теоремы Ферма будет доказан в п. 1 § 7 гл. V.

Сделаем к теореме 1 несколько замечаний.

Замечание 1. Основной частью доказательства теоремы является доказательство неразрешимости некоторых сравнений по модулю l. Из этого, конечно, не следует, что мы доказываем неразрешимость сравнения $x^l+y^l \equiv z^l \pmod{l}$. Так как это сравнение равносильно сравнению $x+y \equiv z \pmod{l}$, то оно всегда имеет решение, состоящее из чисел, не делящихся на l. Более того, можно показать, что, например, при $l \equiv 7$ уравнение $x^7+y^7=z^7$, будучи рассмотрено как сравнение по модулю 7^m при любом $m \geqslant 1$ имеет решение в числах x, y, z, не делящихся на 7 (см. задачу 3 § 5 гл. I).

Таким образом, доказательство неразрешимости уравнения (1) основывается на сведении его к уравнениям (3) и (3′) при помощи теории разложения на множители в кольце $\mathbb{Z}[\zeta]$ и на применении теории сравнений к полученным уравнениям.

Замечание 2. Ясно, что соображения, которые мы применили в этом параграфе к теореме Ферма, могут быть применены и к другим аналогичным задачам, но при этом вместо кругового поля $\mathbb{Q}(\zeta)$ надо будет использовать другие поля алгебраических чисел (задача 2).

Замечание 3. Если мы захотим применить доказанную теорему к какому-либо конкретному l, то обнаружим, что не можем этого сделать, так как не располагаем способом, который давал бы возможность определить, однозначно ли разложение целых чисел поля $\mathbb{Q}(\zeta)$ на простые множители.

В связи с этим мы приходим к следующим двум основным вопросам теории алгебраических чисел:

1. В каких полях алгебраических чисел K разложение целых чисел на простые множители однозначно?

2. Как видоизменяются арифметические закономерности в тех полях K, в которых разложение целых чисел на простые множители неоднозначно?

Замечание 4. В настоящее время известно [106], что в кольце $\mathbb{Z}[\zeta]$, где ζ — первообразный корень степени l из 1, однозначность разложения на простые множители имеет место только для первых семи нечетных простых чисел. Это значит, что теорема 1 фактически применима лишь для $l = 3, 5, 7, 11, 13, 17, 19$. Однако в п. 3 § 7 мы увидим, что утверждение теоремы 1 справедливо для значительно более широкого класса показателей l. Именно, там будет доказано, что первый случай теоремы Ферма справедлив для всех регулярных показателей (определение регулярности простого числа приведено в том же п. 3 § 7).

Задачи

1. Доказать, что сравнение $x^5 + y^5 \equiv z^5 \pmod{5^2}$ не имеет решений в целых рациональных числах x, y, z, не делящихся на 5.

2. Пусть ω — первообразный корень 3-й степени из 1. Считая известным, что в поле $\mathbb{Q}(\omega)$ разложение целых чисел на простые множители однозначно, доказать, что уравнение $x^3 + y^3 = 5z^3$ не имеет решений в целых рациональных x, y, z, не делящихся на 3.

3. Пусть l — простое число, ζ — первообразный корень l-й степени из 1, x и y — целые рациональные числа, d — общий наибольший делитель x и y. Положим $\delta = d$, если $x + y \not\equiv 0 \pmod{l}$, и $\delta = d(1-\zeta)$, если $x + y \equiv 0 \pmod{l}$. Доказать, что δ есть общий делитель чисел $x + \zeta^m y$ и $x + \zeta^n y$ ($m \not\equiv n \pmod{l}$), делящийся на все прочие общие делители этих чисел.

4. Доказать, что в порядке $\{1, \zeta, \ldots, \zeta^{l-2}\}$ поля $\mathbb{Q}(\zeta)$ произведение $\alpha\beta$ делится на $1-\zeta$ тогда и только тогда, когда хоть один из сомножителей α или β делится на $1-\zeta$.

5. Используя понятие сравнимости целочисленных многочленов, показать, что $t^{l-1} + \ldots + t + 1 \equiv (t-1)^{l-1} \pmod{l}$.

6. Доказать неприводимость многочлена $t^{l-1} + \ldots + t + 1$ над полем рациональных чисел, рассматривая сравнения для целочисленных многочленов по модулю l^2.

§ 2. Разложение на множители

1. Простые множители. В предшествующем параграфе мы видели пример того, как задачи теории чисел приводят нас к вопросу о разложении на простые множители в порядках полей алгебраических чисел. С другими примерами такого рода мы познакомимся позже. Сейчас мы займемся исследованием с общей точки зрения вопроса о разложении на простые множители.

Для того чтобы говорить о разложении на простые множители, нам необходимо фиксировать кольцо $\mathfrak{O}$, элементы которого мы будем раскладывать на множители. Мы начнем с того, что сформулируем нашу задачу в самом общем виде и ввиду этого не будем накладывать на это кольцо никаких условий, кроме того, что оно коммутативно, не имеет делителей нуля и содержит единицу.

В дальнейшем эти условия постоянно будут предполагаться выполненными без специальных оговорок.

Определение. *Элемент π кольца $\mathfrak{O}$, отличный от нуля и не являющийся единицей, называется простым, если он не может быть разложен на множители $\pi = \alpha\beta$, ни один из которых не является единицей в $\mathfrak{O}$.*

Простота элемента означает, таким образом, что он делится только на единицы и на ассоциированные с ним элементы.

Не во всяком кольце простые элементы существуют, и, следовательно, не всегда элементы кольца могут быть представлены в виде произведения простых элементов. Возьмем, например, в качестве $\mathfrak{O}$ кольцо всех целых алгебраических чисел. Для всякого $\alpha \neq 0$ из $\mathfrak{O}$, не являющегося единицей, имеем разложение $\alpha = \sqrt{\alpha}\sqrt{\alpha}$, в котором множители принадлежат кольцу $\mathfrak{O}$ и также не являются единицами. Таким образом, все неединицы в $\mathfrak{O}$ допускают разложения на нетривиальные множители, а это и означает, что в $\mathfrak{O}$ простых элементов нет.

Примерами колец, в которых разложение на простые множители возможно, могут служить порядки в полях алгебраических чисел (именно эти кольца нас больше всего интересуют). Простые элементы в порядках мы будем называть также простыми числами.

Теорема 1. *В произвольном порядке $\mathfrak{O}$ поля алгебраических чисел K каждое отличное от нуля и не являющееся единицей число может быть представлено в виде произведения простых чисел.*

Доказательство. Согласно теореме 4 § 2 гл. II единицы ε порядка $\mathfrak{O}$ характеризуются тем, что их нормы $N(\varepsilon)$ равны ± 1. Будем доказывать теорему индукцией по абсолютной величине нормы $|N(\alpha)|$ числа $\alpha \in \mathfrak{O}$. Если число α само простое, то доказывать нечего. Если же $\alpha = \beta\gamma$, где β и γ — числа из $\mathfrak{O}$, не являющиеся единицами, то

$$1 < |N(\beta)| < |N(\alpha)|, \quad 1 < |N(\gamma)| < |N(\alpha)|.$$

По индуктивному предположению β и γ являются произведениями простых чисел кольца $\mathfrak{O}$. Но тогда ввиду равенства $\alpha = \beta\gamma$ и число α является произведением простых чисел. Теорема 1, таким образом, доказана.

2. Однозначность разложения. Предполагая теперь, что в некотором кольце $\mathfrak{O}$ разложение на простые множители возможно, займемся выяснением вопроса об однозначности такого разложения (конечно, с точностью до ассоциированности).

Определение. *Будем говорить, что в кольце $\mathfrak{O}$ разложение на простые множители однозначно, если для двух разложений $\alpha = \pi_1 \dots \pi_r$, $\alpha = \pi'_1 \dots \pi'_s$ число сомножителей всегда одинако-*

во $(r=s)$ *и при надлежащей нумерации простые элементы* π_i *и* π_i' *ассоциированы между собой.*

В разложении $\alpha=\pi_1\dots\pi_r$ ассоциированные простые элементы можно превратить в равные умножением на надлежащие единицы. Объединяя затем равные сомножители в степень, мы придем к разложению вида $\alpha=\varepsilon\pi_1^{k_1}\dots\pi_m^{k_m}$, в котором простые элементы $\pi_1, \dots, \pi_m$ попарно не ассоциированы, а ε — единица кольца $\mathfrak{O}$. В случае однозначного разложения на множители простые элементы $\pi_1, \dots, \pi_m$ с точностью до ассоциированности и показатели $k_1, \dots, k_m$ определены единственным образом.

Классическим примером кольца с однозначным разложением на множители является кольцо целых рациональных чисел. В общем же случае далеко не для всех колец, в которых разложение на простые множители возможно, будет иметь место однозначность разложения. Так, результат задачи 1 показывает, что из всех порядков в полях алгебраических чисел только для максимальных порядков можно рассчитывать на однозначность разложения.

Однозначность разложения на простые множители в кольце целых рациональных чисел $\mathbb{Z}$ вытекает из теоремы о делении с остатком, утверждающей, что для любых a и $b\neq 0$ из $\mathbb{Z}$ существуют такие целые q и r, что $a=bq+r$ и $|r|<|b|$. Если поэтому для произвольного кольца $\mathfrak{O}$ будет иметь место надлежащий аналог этого деления с остатком, то в $\mathfrak{O}$, совершенно так же как и в $\mathbb{Z}$, можно будет доказать однозначность разложения на простые множители.

Определение. *Мы говорим, что в кольце* $\mathfrak{O}$ *имеет место алгоритм деления с остатком, если на отличных от нуля элементах* $\alpha\in\mathfrak{O}$ *определена функция* $\|\alpha\|$, *принимающая целые неотрицательные значения, так, что удовлетворяются следующие условия:*

1) *если* $\alpha\neq 0$ *делится на* β, *то* $\|\alpha\|\geqslant\|\beta\|$;

2) *для любых элементов* α *и* $\beta\neq 0$ *в* $\mathfrak{O}$ *существуют такие* γ *и* ρ, *что* $\alpha=\beta\gamma+\rho$, *причем либо* $\rho=0$, *либо* $\|\rho\|<\|\beta\|$. *Само кольцо* $\mathfrak{O}$ *называется при этом евклидовым.*

Вспомним доказательства однозначности разложения целых рациональных чисел на простые множители и разложения многочленов на неприводимые множители. В них, помимо общих свойств колец, используется только теорема о делении с остатком. Поэтому, дословно повторяя эти доказательства, приходим к следующему результату.

Теорема 2. *В каждом евклидовом кольце разложение элементов на простые множители возможно и однозначно.*

Рассмотрим в качестве примера максимальный порядок $\mathfrak{O}$ квадратичного поля $\mathbb{Q}(\sqrt{-1})$ и покажем, что в $\mathfrak{O}$ имеет место алгоритм деления с остатком относительно функции $\|\alpha\|=N(\alpha)$.

Пусть α и $\beta \neq 0$ — произвольные числа из $\mathfrak{O}$. Для рациональных чисел u и v, определенных равенством

$$\frac{\alpha}{\beta} = u + v\sqrt{-1},$$

выберем ближайшие к ним целые рациональные числа x и y:

$$|u - x| \leqslant 1/2, \quad |v - y| \leqslant 1/2.$$

Если мы положим теперь $\gamma = x + y\sqrt{-1}$, $\rho = \alpha - \beta\gamma$, то ввиду неравенства

$$N\left(\frac{\alpha}{\beta} - \gamma\right) = (u - x)^2 + (v - y)^2 \leqslant \frac{1}{4} + \frac{1}{4} < 1$$

будем иметь $N(\rho) = N\left(\frac{\alpha}{\beta} - \gamma\right) N(\beta) < N(\beta)$, а это и доказывает наше утверждение.

В силу теоремы 2 мы получаем, следовательно, что в максимальном порядке поля $\mathbb{Q}(\sqrt{-1})$ разложение на простые множители однозначно.

Таким же образом можно доказать однозначность разложения и для ряда других колец (см. задачи 3, 4 и 7). Следует отметить, однако, что существуют кольца, которые не являются евклидовыми, но в которых тем не менее разложение на простые множители однозначно. Простейшим примером такого кольца может служить максимальный порядок поля $\mathbb{Q}(\sqrt{-19})$. Отсутствие в этом кольце алгоритма деления с остатком следует из задачи 6. То, что в нем разложение на простые множители однозначно, следует из задачи 11 § 7 этой главы.

Среди максимальных порядков вещественных квадратичных полей $\mathbb{Q}(\sqrt{d})$ алгоритмом деления с остатком по норме обладают те и только те, для которых d равно одному из следующих шестнадцати значений:

$$2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

3. Примеры неоднозначного разложения. Совсем нетрудно построить примеры противоположного характера, показывающие, что в максимальных порядках полей алгебраических чисел разложение на простые множители может быть неоднозначным. Возьмем, например, поле $\mathbb{Q}(\sqrt{-5})$. Как показано в п. 2 § 7 гл. II, числа из максимального порядка $\mathfrak{O}$ этого поля имеют вид $\alpha = x + y\sqrt{-5}$ с целыми рациональными x и y, при этом $N(\alpha) = x^2 + 5y^2$. Для числа 21 в кольце $\mathfrak{O}$ имеем разложения

$$21 = 3 \cdot 7, \tag{1}$$

$$21 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}). \tag{2}$$

Утверждаем, что в кольце $\mathfrak{O}$ все сомножители, стоящие справа,

простые. Действительно, если бы, например, $3=\alpha\beta$, где α и β не единицы, то из равенства $9=N(\alpha\beta)=N(\alpha)N(\beta)$ следовало бы $N(\alpha)=3$. Этого, однако, не может быть, так как равенство $x^2+5y^2=3$ с целыми рациональными x и y невозможно. Точно так же доказывается, что числа 7, $1+2\sqrt{-5}$, $1-2\sqrt{-5}$ тоже простые. Так как отношения

$$\frac{1\pm 2\sqrt{-5}}{3}, \quad \frac{1\pm 2\sqrt{-5}}{7}$$

не принадлежат кольцу $\mathfrak{O}$, то числа 3 и 7 не ассоциированы с $1+2\sqrt{-5}$ и $1-2\sqrt{-5}$. Мы видим, таким образом, что в $\mathfrak{O}$ существуют числа, допускающие существенно различные разложения на простые множители.

Приведенный пример поля $\mathbb{Q}(\sqrt{-5})$, для максимального порядка которого разложение на простые множители неоднозначно, не представляет собой особенно редкого исключения. Таких примеров можно привести довольно много (см. задачи 10 и 11).

Казалось бы, обнаруженное нами явление неоднозначности разложения на простые множители в полях алгебраических чисел делает невозможным построение законченной арифметики алгебраических чисел, а тем самым лишает нас надежды на возможность более глубоких применений алгебраических чисел к задачам теории чисел. Однако на самом деле это не так. В середине прошлого века Куммер показал, что, хотя арифметика алгебраических чисел радикально отличается от арифметики рациональных чисел, она может быть развита настолько далеко, чтобы давать исключительно сильные приложения к теоретико-числовым вопросам.

Основная идея Куммера заключалась в том, что если в максимальном порядке $\mathfrak{O}$ некоторого поля алгебраических чисел разложение на простые множители неоднозначно, то отличные от нуля числа из $\mathfrak{O}$ можно отобразить в некоторое новое множество, в котором определено умножение и в котором разложение на простые множители уже однозначно. Тогда для всякого числа $\alpha\neq 0$ из $\mathfrak{O}$ его образ (α) при этом отображении можно будет однозначно представить в виде произведения простых множителей, но эти простые множители будут принадлежать не нашему кольцу, а некоторому новому множеству. Однозначность разложения, по мысли Куммера, должна восстановиться в силу того, что некоторые простые числа из $\mathfrak{O}$ (а может быть, и все) отобразятся на непростые элементы нового множества и потому их образы будут иметь разложения на нетривиальные множители. Так, в примере максимального порядка поля $\mathbb{Q}(\sqrt{-5})$ для восстановления однозначности в разложениях (1) и (2) должны существовать такие объекты $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$, что

$$3=\mathfrak{p}_1\mathfrak{p}_2, \quad 7=\mathfrak{p}_3\mathfrak{p}_4, \quad 1+2\sqrt{-5}=\mathfrak{p}_1\mathfrak{p}_3, \quad 1-2\sqrt{-5}=\mathfrak{p}_2\mathfrak{p}_4$$

(в этих равенствах мы не различали числа и сопоставляемые им новые объекты). Разложения (1) и (2) сводятся теперь к разложениям $21 = \mathfrak{p}_1\mathfrak{p}_2 \cdot \mathfrak{p}_3\mathfrak{p}_4 = \mathfrak{p}_1\mathfrak{p}_3 \cdot \mathfrak{p}_2\mathfrak{p}_4$, которые отличаются лишь порядком сомножителей.

Сам Куммер называл эти новые объекты идеальными числами. Теперь их называют дивизорами. Систематическое изложение теории дивизоров составит содержание следующих параграфов.

Задачи

1. Доказать, что если в некотором порядке $\mathfrak{O}$ поля алгебраических чисел K разложение на простые множители однозначно, то этот порядок максимальный. И вообще: если в кольце $\mathfrak{O}$ разложение на простые множители возможно и однозначно, то кольцо $\mathfrak{O}$ целозамкнуто в своем поле отношений.

2. Доказать, что если в евклидовом кольце элемент $\alpha \neq 0$ делится на β, причем α не ассоциировано с β, то $\|\alpha\| > \|\beta\|$.

3. Пусть $\mathfrak{M}$ есть решетка на плоскости комплексной переменной, точки которой изображают числа максимального порядка $\mathfrak{O}$ мнимого квадратичного поля. Доказать что в $\mathfrak{O}$ алгоритм деления с остатком по норме $N(\alpha)$ имеет место тогда и только тогда, когда сдвиги единичного круга (без границы) на все векторы решетки $\mathfrak{M}$ покрывают всю плоскость.

4. Показать, что в максимальном порядке мнимого квадратичного поля $\mathbb{Q}(\sqrt{d})$ алгоритм деления с остатком по норме имеет место тогда и только тогда, когда d равно одному из значений: -1, -2, -3, -7, -11.

5. Доказать, что в мнимом квадратичном поле $\mathbb{Q}(\sqrt{d})$, где свободное от квадратов целое $d < 0$ отлично от -1, -2, -3, -7, -11, норма всякого целого числа, не равного 0 и ± 1, больше трех.

6. Доказать, что, кроме пяти полей, указанных в задаче 4, для всех прочих мнимых квадратичных полей максимальные порядки не являются евклидовыми кольцами.

Указание. Доказательство провести от противного. Предположим, что на элементах α максимального порядка $\mathfrak{O}$ существует функция $\|\alpha\|$, удовлетворяющая условиям определения п. 2. Среди чисел кольца $\mathfrak{O}$, не являющихся единицами, выберем число γ с наименьшим значением $\|\gamma\|$. Тогда всякое $\alpha \in \mathfrak{O}$ по модулю γ будет сравнимо с одним из трех чисел: 0, 1, -1.

7. Доказать существование алгоритма деления с остатком для максимального порядка поля $\mathbb{Q}(\sqrt{2})$.

8. Доказать, что в максимальном порядке поля $\mathbb{Q}(\sqrt{-1})$ каждое нечетное простое рациональное число p остается простым, если оно имеет вид $4k+3$, и раскладывается в произведение $p = \pi\pi'$ двух неассоциированных простых множителей, если $p = 4k+1$. Найти, далее, разложение числа 2 на простые множители.

9. Пусть в кольце $\mathfrak{O}$ имеет место однозначность разложения на простые множители. Доказать, что тогда для любых α и β из $\mathfrak{O}$ (не равных одновременно нулю) существует такой их общий делитель δ, который делится на все прочие общие делители α и β (δ называется общим наибольшим делителем α и β).

10. Показать, что в максимальном порядке поля $\mathbb{Q}(\sqrt{-6})$ имеем существенно различные разложения на простые множители:

$$55 = 5 \cdot 11 = (7+\sqrt{-6})(7-\sqrt{-6}), \qquad 6 = 2 \cdot 3 = -(\sqrt{-6})^2.$$

11. Проверить, что в максимальном порядке поля $\mathbb{Q}(\sqrt{-23})$ имеем разложения на простые множители:

$$6 = 2 \cdot 3 = \frac{1+\sqrt{-23}}{2} \cdot \frac{1-\sqrt{-23}}{2}, \quad 27 = 3 \cdot 3 \cdot 3 = (2+\sqrt{-23})(2-\sqrt{-23}).$$

Найти в том же кольце различные разложения числа 8 на простые множители.

12. Доказать, что если в кольце $\mathfrak{O}$ все идеалы главные, то $\mathfrak{O}$ — кольцо с однозначным разложением на простые множители.

§ 3. Дивизоры

1. Аксиоматическое описание дивизоров. Рассмотрим произвольное коммутативное кольцо $\mathfrak{O}$ (с единицей и без делителей нуля) и постараемся выяснить, какой смысл можно вложить в изложенную в п. 3 § 2 идею отображения отличных от нуля элементов кольца $\mathfrak{O}$ в некоторую новую область, в которой разложение на простые множители однозначно.

Наша теория должна, очевидно, состоять из двух частей: из построения некоторой совокупности $\mathfrak{D}$ новых объектов, в которой разложение на простые множители однозначно, и из сопоставления ненулевым элементам кольца $\mathfrak{O}$ элементов совокупности $\mathfrak{D}$. Начнем с первой части. Для того чтобы в $\mathfrak{D}$ можно было говорить о разложении на множители, там должна быть определена операция умножения, сопоставляющая любым двум элементам из $\mathfrak{D}$ некоторый третий элемент — их произведение. Эту операцию мы будем предполагать ассоциативной и коммутативной. Множества с такой операцией называются коммутативными полугруппами. Для наших целей необходимо, далее, потребовать, чтобы в $\mathfrak{D}$ была единица, т. е. такой элемент e, что $ea = a$ для всех $a \in \mathfrak{D}$.

В коммутативной полугруппе $\mathfrak{D}$ с единицей e можно говорить о делимости элементов: элемент $a \in \mathfrak{D}$ делится на $b \in \mathfrak{D}$, если существует такой элемент $c \in \mathfrak{D}$, что $a = bc$ (говорят также, что b есть делитель a, или a кратно b). Элемент $p \in \mathfrak{D}$, отличный от e, называется *простым*, если он делится только на себя и на единицу e. Говорят, далее, что в полугруппе $\mathfrak{D}$ имеет место однозначность разложения на простые множители, если каждый элемент $a \in \mathfrak{D}$ может быть представлен в виде произведения простых элементов

$$a = p_1 \dots p_r, \qquad r \geqslant 0,$$

и такое разложение единственно с точностью до порядка сомножителей (при $r = 0$ произведение считается равным единице e). Однозначность разложения предполагает, таким образом, что в полугруппе $\mathfrak{D}$, кроме e, нет других обратимых элементов (делителей e). Ясно, что полугруппа с однозначным разложением на множители вполне определяется множеством своих простых элементов (их мощностью). Простой пример полугруппы с однозначным разложением на простые множители дает нам совокупность всех натуральных чисел относительно действия умножения.

В полугруппе $\mathfrak{D}$ с однозначным разложением на простые множители для любых двух элементов существует, очевидно, их об-

щий наибольший делитель (т. е. такой общий делитель, который делится на все другие общие делители данных элементов), а также общее наименьшее кратное. Два элемента из $\mathfrak{D}$ называются взаимно простыми, если их общий наибольший делитель равен ϵ. Отметим несколько элементарных свойств делимости в $\mathfrak{D}$: если произведение ab делится на c и a взаимно просто с c, то b делится на c; если c делится на взаимно простые элементы a и b, то c делится и на произведение ab; если произведение ab делится на простой элемент p, то хоть один из сомножителей делится на p.

Перейдем теперь к выявлению условий, которым должна удовлетворять вторая часть нашей теории — сопоставление элементам кольца $\mathfrak{D}$ элементов полугруппы $\mathfrak{D}$.

Обозначим через $\mathfrak{D}^*$ совокупность всех отличных от нуля элементов кольца $\mathfrak{D}$. Так как кольцо $\mathfrak{D}$ по предположению не имеет делителей нуля, то множество $\mathfrak{D}^*$ является полугруппой относительно действия умножения.

Пусть задано отображение полугруппы $\mathfrak{D}^*$ в полугруппу $\mathfrak{D}$ с однозначным разложением на простые множители. Образ элемента $\alpha \in \mathfrak{D}^*$ при этом отображении будем обозначать через (α). Ясно, что изучение мультипликативной структуры кольца $\mathfrak{D}$ при помощи полугруппы $\mathfrak{D}$ будет возможно лишь в том случае, если при отображении $\alpha \to (\alpha)$ произведению элементов в $\mathfrak{D}^*$ будет соответствовать произведение их образов в $\mathfrak{D}$, т. е. если $(\alpha\beta) = (\alpha)(\beta)$ при всех α и β из $\mathfrak{D}^*$. Мы должны, следовательно, потребовать, чтобы отображение $\alpha \to (\alpha)$ было гомоморфизмом полугруппы $\mathfrak{D}^*$ в полугруппу $\mathfrak{D}$. Из делимости α на β в кольце $\mathfrak{D}$ будет тогда следовать, что (α) делится на (β) в полугруппе $\mathfrak{D}$. Чтобы отношение делимости в $\mathfrak{D}$ в точности соответствовало делимости в $\mathfrak{D}$, надо потребовать, чтобы и, обратно, из делимости (α) на (β) в полугруппе $\mathfrak{D}$ вытекала делимость α на β в кольце $\mathfrak{D}$.

Мы будем дальше говорить, что элемент $\alpha \neq 0$ из $\mathfrak{D}$ делится на элемент $\mathfrak{a} \in \mathfrak{D}$, и писать $\mathfrak{a} | \alpha$, если (α) делится на $\mathfrak{a}$ в смысле делимости в полугруппе $\mathfrak{D}$. Будем также считать, что 0 делится на все элементы из $\mathfrak{D}$.

Совокупность всех элементов кольца $\mathfrak{D}$, делящихся на $\alpha \in \mathfrak{D}^*$, замкнута относительно действий сложения и вычитания. Естественно потребовать, чтобы это свойство сохранилось и для новых делителей $\mathfrak{a}$ из полугруппы $\mathfrak{D}$.

Последним нашим условием будет требование отсутствия в $\mathfrak{D}$ «лишних» элементов. Под этим мы понимаем то, что два различных элемента из $\mathfrak{D}$ должны отличаться друг от друга своими свойствами делимости по отношению к элементам из $\mathfrak{D}$.

Мы приходим к следующему определению.

Определение. *Под теорией дивизоров кольца $\mathfrak{D}$ будем понимать задание некоторой полугруппы $\mathfrak{D}$ с однозначным разложением на простые множители и гомоморфизма $\alpha \to (\alpha)$ полугруппы $\mathfrak{D}^*$ в $\mathfrak{D}$, для которых выполнены условия:*

1°. *В кольце* $\mathfrak{O}$ *элемент* $\alpha \in \mathfrak{O}^*$ *делится на* $\beta \in \mathfrak{O}^*$ *тогда и только тогда, когда* (α) *делится на* (β) *в полугруппе* $\mathfrak{D}$.

2°. *Если* α *и* β *из* $\mathfrak{O}$ *делятся на элемент* $\mathfrak{a} \in \mathfrak{D}$, *то* $\alpha \pm \beta$ *также делится на* $\mathfrak{a}$.

3°. *Если* $\mathfrak{a}$ *и* $\mathfrak{b}$ *— два элемента из* $\mathfrak{D}$ *и если совокупность всех элементов* $\alpha \in \mathfrak{O}$, *делящихся на* $\mathfrak{a}$, *совпадает с совокупностью всех элементов* $\beta \in \mathfrak{O}$, *делящихся на* $\mathfrak{b}$, *то* $\mathfrak{a} = \mathfrak{b}$.

Элементы полугруппы $\mathfrak{D}$ называются при этом *дивизорами* кольца $\mathfrak{O}$, дивизоры вида (α), $\alpha \in \mathfrak{O}^*$,— *главными дивизорами*. Единичный элемент $\mathfrak{e}$ полугруппы $\mathfrak{D}$ называется *единичным дивизором*, а простой элемент $\mathfrak{p}$ — *простым дивизором*.

Из условия 1° определения теории дивизоров очевидным образом вытекает следующее важное утверждение.

Равенство $(\alpha) = (\beta)$ *имеет место тогда и только тогда, когда* α *и* β *ассоциированы в кольце* $\mathfrak{O}$. *В частности, все единицы* ε *кольца* $\mathfrak{O}$ *характеризуются равенством* $(\varepsilon) = \mathfrak{e}$.

Теорию дивизоров для кольца $\mathfrak{O}$ будем обозначать в дальнейшем через $\mathfrak{O}^* \to \mathfrak{D}$.

Данное нами определение теории дивизоров фиксирует только, что именно мы будем подразумевать под этим понятием. Оно ни в какой мере не гарантирует ни существования гомоморфизма $\mathfrak{O}^* \to \mathfrak{D}$, ни его *единственности*.

В следующем пункте мы рассмотрим вопрос о единственности теории дивизоров, предполагая, что она существует, а в п. 3 укажем одно важное необходимое (но не достаточное) условие ее существования.

Существование теории дивизоров для интересующих нас максимальных порядков в полях алгебраических чисел будет доказано нами в § 5 (что касается немаксимальных порядков, то в них ввиду теоремы 3 теория дивизоров построена быть не может).

Замечание. Условие 2° в определении теории дивизоров можно опустить: это условие, как легко показать (см. задачи 11—13), является следствием условий 1° и 3° [132].

2. Единственность. Теорема 1. *Если для кольца* $\mathfrak{O}$ *существует теория дивизоров, то только одна. Точнее, это означает, что для любых двух гомоморфизмов* $\mathfrak{O}^* \to \mathfrak{D}$ *и* $\mathfrak{O}^* \to \mathfrak{D}'$, *удовлетворяющих определению п.* 1, *существует изоморфизм* $\mathfrak{D} \approx \mathfrak{D}'$, *при котором главные дивизоры, сопоставляемые одному и тому же элементу* $\alpha \in \mathfrak{O}^*$ *в* $\mathfrak{D}$ *и в* $\mathfrak{D}'$, *соответствуют друг другу.*

Доказательство. Пусть $\mathfrak{O}^* \to \mathfrak{D}$ и $\mathfrak{O}^* \to \mathfrak{D}'$ — две теории дивизоров кольца $\mathfrak{O}$. Для простых дивизоров $\mathfrak{p} \in \mathfrak{D}$ и $\mathfrak{p}' \in \mathfrak{D}'$ через $\overline{\mathfrak{p}}$ и $\overline{\mathfrak{p}'}$ обозначим совокупности элементов кольца $\mathfrak{O}$, делящихся на $\mathfrak{p}$ и на $\mathfrak{p}'$ соответственно (делимость на $\mathfrak{p}$ здесь понимается, конечно, относительно теории $\mathfrak{O}^* \to \mathfrak{D}$, а на $\mathfrak{p}'$ — относительно теории $\mathfrak{O}^* \to \mathfrak{D}'$). Докажем, что для всякого простого дивизора $\mathfrak{p}' \in \mathfrak{D}'$ существует простой дивизор $\mathfrak{p} \in \mathfrak{D}$ такой, что

$\bar{\mathfrak{p}} \subset \bar{\mathfrak{p}}'$. Допустим, что это не так, т. е. что $\bar{\mathfrak{p}} \not\subset \bar{\mathfrak{p}}'$ для всех простых дивизоров $\mathfrak{p} \in \mathfrak{D}$. Из условия 3° легко следует, что для всякого дивизора совокупность всех делящихся на него элементов кольца $\mathfrak{O}$ не может состоять только из нуля. Выберем в $\mathfrak{O}$ элемент $\beta \neq 0$, делящийся на $\mathfrak{p}'$, и разложим главный дивизор $(\beta) \in \mathfrak{D}$ на простые множители:

$$(\beta) = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r}$$

($\mathfrak{p}_1, \dots, \mathfrak{p}_r$ — простые дивизоры полугруппы $\mathfrak{D}$). Так как по нашему допущению $\bar{\mathfrak{p}}_i \not\subset \bar{\mathfrak{p}}'$, то для каждого $i = 1, \dots, r$ найдется элемент $\gamma_i \in \mathfrak{O}$, делящийся на $\mathfrak{p}_i$, но не делящийся на $\mathfrak{p}'$. Произведение $\gamma = \gamma_1^{k_1} \dots \gamma_r^{k_r}$ будет делиться, очевидно, на $\mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r}$, а значит, в силу условия 1° γ будет делиться на β в кольце $\mathfrak{O}$. Но в таком случае γ должно делиться и на $\mathfrak{p}'$. Мы получили противоречие, так как произведение $\gamma_1^{k_1} \dots \gamma_r^{k_r}$ не может делиться на $\mathfrak{p}'$ ввиду простоты $\mathfrak{p}'$ и ввиду того, что все сомножители γ_i не делятся на $\mathfrak{p}'$.

Итак, для всякого простого дивизора $\mathfrak{p}' \in \mathfrak{D}'$ найдется такой простой дивизор $\mathfrak{p} \in \mathfrak{D}$, что $\bar{\mathfrak{p}} \subset \bar{\mathfrak{p}}'$. Аналогичным образом в силу симметрии существует простой дивизор $\mathfrak{q}' \in \mathfrak{D}'$, для которого $\bar{\mathfrak{q}}' \subset \bar{\mathfrak{p}}$. Покажем, что $\mathfrak{q}' = \mathfrak{p}'$ и, следовательно, $\bar{\mathfrak{q}}' = \bar{\mathfrak{p}} = \bar{\mathfrak{p}}'$. Действительно, по условию 3° в кольце $\mathfrak{O}$ существует элемент ξ, делящийся на $\mathfrak{q}'$ и не делящийся на $\mathfrak{q}'\mathfrak{p}'$. Если предположить, что $\mathfrak{q}' \neq \mathfrak{p}'$, то этот элемент ξ не будет делиться на $\mathfrak{p}'$, и мы вступаем в противоречие с включением $\bar{\mathfrak{q}}' \subset \bar{\mathfrak{p}}'$.

Так как равенством $\bar{\mathfrak{p}} = \bar{\mathfrak{p}}'$ простой дивизор $\mathfrak{p} \in \mathfrak{D}$ (при данном $\mathfrak{p}' \in \mathfrak{D}'$) определен однозначно (условие 3°), то мы получаем взаимно однозначное соответствие $\mathfrak{p} \leftrightarrow \mathfrak{p}'$ между всеми простыми дивизорами из $\mathfrak{D}$ и простыми дивизорами из $\mathfrak{D}'$. Это соответствие можно, очевидно, продолжить (единственным образом) до изоморфизма $\mathfrak{D} \approx \mathfrak{D}'$. Именно, если $\mathfrak{p}_1 \leftrightarrow \mathfrak{p}_1', \dots, \mathfrak{p}_r \leftrightarrow \mathfrak{p}_r'$, то

$$\mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r} \leftrightarrow \mathfrak{p}_1'^{k_1} \dots \mathfrak{p}_r'^{k_r}.$$

Нам остается теперь доказать, что при этом изоморфизме главные дивизоры $(\alpha) \in \mathfrak{D}$ и $(\alpha)' \in \mathfrak{D}'$ для любого $\alpha \in \mathfrak{D}^*$ соответствуют друг другу. Пусть $\mathfrak{p} \in \mathfrak{D}$ и $\mathfrak{p}' \in \mathfrak{D}'$ — соответствующие друг другу простые дивизоры, и пусть они входят в разложения (α) и $(\alpha)'$ с показателями k и l соответственно. По условию 3° в кольце $\mathfrak{O}$ существует элемент π, делящийся на $\mathfrak{p}$ и не делящийся на $\mathfrak{p}^2$. Ввиду равенства $\bar{\mathfrak{p}} = \bar{\mathfrak{p}}'$ элемент π делится также и на $\mathfrak{p}'$. Главный дивизор (π) имеет, очевидно, вид $(\pi) = \mathfrak{p}\mathfrak{b}$, где $\mathfrak{b}$ не делится на $\mathfrak{p}$. Выберем в $\mathfrak{O}$ элемент ω, делящийся на $\mathfrak{b}^k$ и не делящийся на $\mathfrak{b}^k\mathfrak{p}$. Так как $\mathfrak{p}$ не входит в $\mathfrak{b}^k$, то ω не будет делиться также и на $\mathfrak{p}$, а значит, и на $\mathfrak{p}'$. Рассмотрим произведение $\alpha\omega$. По-

сколько α делится на $\mathfrak{p}^k$, а ω делится на $\mathfrak{p}^k$, то $\alpha\omega$ будет делиться на $\mathfrak{p}^k\mathfrak{p}^k = (\pi^k)$, откуда ввиду условия 1° получаем, что $\alpha\omega = \pi^k\eta$, $\eta \in \mathfrak{O}$. Но $\mathfrak{p}' | \pi$, поэтому $\alpha\omega$ делится на $\mathfrak{p}'^k$, а так как $\mathfrak{p}' \nmid \omega$, то $\mathfrak{p}'^k | \alpha$. Это показывает, что в дивизор $(\alpha)' \in \mathfrak{D}'$ простой дивизор $\mathfrak{p}'$ входит с показателем не меньшим, чем k, т. е. что $l \geqslant k$. В силу симметрии также и $k \geqslant l$, а значит, $l = k$.

Мы доказали, таким образом, что если $(\alpha) = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r}$ и $\mathfrak{p}_1 \leftrightarrow \mathfrak{p}_1', \dots, \mathfrak{p}_r \leftrightarrow \mathfrak{p}_r'$, то $(\alpha)' = \mathfrak{p}_1'^{k_1} \dots \mathfrak{p}_r'^{k_r}$, а это и означает, что при изоморфизме $\mathfrak{D} \approx \mathfrak{D}'$ главные дивизоры $(\alpha) \in \mathfrak{D}$ и $(\alpha)' \in \mathfrak{D}'$ соответствуют друг другу. Теорема 1 доказана.

Если в кольце $\mathfrak{O}$ имеет место однозначность разложения на простые множители, то для него мы легко можем построить теорию дивизоров $\mathfrak{O}^* \to \mathfrak{D}$, и в этой теории все дивизоры из $\mathfrak{D}$ будут главными. Действительно, разобьем все отличные от нуля элементы кольца $\mathfrak{O}$ на классы ассоциированных между собой элементов и рассмотрим множество $\mathfrak{D}$ всех таких классов. Для каждого $\alpha \in \mathfrak{O}^*$ через (α) обозначим класс ассоциированных с α элементов. Легко видеть, что относительно умножения $(\alpha)(\beta) = (\alpha\beta)$ множество $\mathfrak{D}$ является полугруппой с однозначным разложением на простые множители, а также что отображение $\alpha \to (\alpha)$, $\alpha \in \mathfrak{O}^*$ определяет теорию дивизоров кольца $\mathfrak{O}$. (Простыми дивизорами здесь будут классы (π), определяемые простыми элементами $\pi \in \mathfrak{O}$.) Согласно теореме 1 всякая теория дивизоров кольца $\mathfrak{O}$ должна в этом случае совпадать с только что построенной.

Предположим теперь, что, наоборот, для некоторого кольца $\mathfrak{O}$ мы имеем теорию дивизоров $\mathfrak{O}^* \to \mathfrak{D}$, в которой все дивизоры из $\mathfrak{D}$ главные. Докажем, что тогда элемент $\pi \neq 0$ кольца $\mathfrak{O}$ будет простым тогда и только тогда, когда соответствующий ему дивизор (π) простой. В самом деле, если $(\pi) = \mathfrak{p}$ — простой дивизор и γ — произвольный делитель π в кольце $\mathfrak{O}$, то дивизор (γ) должен быть делителем $\mathfrak{p}$ (в полугруппе $\mathfrak{D}$) и поэтому, ввиду простоты $\mathfrak{p}$, должен совпадать либо с $\mathfrak{p}$, либо с единичным дивизором $\mathfrak{e}$. В первом случае γ ассоциировано с π, во втором — γ есть единица кольца $\mathfrak{O}$, а это и означает, что π — простой элемент кольца $\mathfrak{O}$. Пусть теперь дивизор (α) отличен от $\mathfrak{e}$ и не является простым. Так как (α) делится на некоторый простой дивизор $\mathfrak{p} = (\pi)$ и не совпадает с ним, то α делится на простой элемент π и не ассоциировано с π. Элемент α не может, следовательно, быть простым.

Таким образом, действительно, если все дивизоры главные, то простота дивизора (π) эквивалентна простоте элемента π.

Пусть теперь α — произвольный элемент из $\mathfrak{O}^*$. Если в $\mathfrak{D}$ имеет место разложение

$$(\alpha) = \mathfrak{p}_1 \dots \mathfrak{p}_r \tag{1}$$

(простые дивизоры $\mathfrak{p}_i$ не обязательно различны) и если $\mathfrak{p}_1 = (\pi_1)$, ..., $\mathfrak{p}_r = (\pi_r)$, то в кольце $\mathfrak{O}$ мы будем иметь разложение

$$\alpha = \varepsilon\pi_1 \dots \pi_r, \tag{2}$$

где ε — единица кольца $\mathfrak{O}$. Так как всякое разложение вида (2) при переходе к дивизорам должно давать разложение (1), то отсюда следует, что в $\mathfrak{O}$ имеет место однозначность разложения на простые множители.

Мы получили следующий результат.

Теорема 2. *Для того чтобы в кольце $\mathfrak{O}$ разложение на простые множители было возможно и однозначно, необходимо и достаточно, чтобы в $\mathfrak{O}$ существовала теория дивизоров $\mathfrak{O}^* \to \mathfrak{D}$ и чтобы в этой теории все дивизоры из $\mathfrak{D}$ были главными.*

3. **Целозамкнутость колец с теорией дивизоров.** Мы уже говорили, что теория дивизоров существует не для всякого кольца. Наличие гомоморфизма $\alpha \to (\alpha)$, удовлетворяющего условиям определения теории дивизоров, накладывает на кольцо сильные ограничения. Одно из таких ограничений дается следующей теоремой.

Теорема 3. *Если для кольца $\mathfrak{O}$ существует теория дивизоров, то это кольцо целозамкнуто в своем поле отношений K.*

Доказательство. Предположим, что элемент ξ из поля отношений K кольца $\mathfrak{O}$, удовлетворяющий соотношению

$$\xi^n + a_1\xi^{n-1} + \ldots + a_{n-1}\xi + a_n = 0, \quad a_1, \ldots, a_n \in \mathfrak{O},$$

не принадлежит $\mathfrak{O}$. Представим его в виде $\xi = \alpha/\beta$, где $\alpha \in \mathfrak{O}$ и $\beta \in \mathfrak{O}$, и разложим главные дивизоры (α) и (β) в произведение степеней простых дивизоров. Поскольку α не делится на β в кольце $\mathfrak{O}$ (по нашему предположению $\xi \notin \mathfrak{O}$), то (α) не делится на (β) в смысле делимости дивизоров (по условию 1°). Это значит, что некоторый простой дивизор $\mathfrak{p} \in \mathfrak{D}$ входит в (β) в большей степени, чем в (α). Пусть $\mathfrak{p}$ входит в (α) с показателем $k \geqslant 0$. Так как β делится на $\mathfrak{p}^{k+1}$, то в силу условия 2° правая часть равенства

$$\alpha^n = -a_1\beta\alpha^{n-1} - \ldots - a_n\beta^n$$

делится на $\mathfrak{p}^{kn+1}$. В то же время $\mathfrak{p}$ входит в дивизор $(\alpha^n) = (\alpha)^n$ с показателем kn, и поэтому α^n не может делиться на $\mathfrak{p}^{kn+1}$. Полученное противоречие показывает, что $\xi \in \mathfrak{O}$, и теорема 3 доказана.

Другое необходимое условие существования теории дивизоров указано в задаче 1.

Так как среди порядков в полях алгебраических чисел свойством целозамкнутости обладают лишь максимальные порядки, то согласно теореме 3 только для них можно рассчитывать на построение теории дивизоров.

4. Связь теории дивизоров с показателями. Займемся теперь вопросом о фактическом построении теории дивизоров. Мы предположим сначала, что для кольца $\mathfrak{O}$ теория дивизоров $\mathfrak{O}^* \to \mathfrak{D}$ существует, и постараемся выяснить, какой конструкцией эта теория определяется.

Выбрав произвольно простой дивизор $\mathfrak{p}$, мы можем сопоставить ему некоторую функцию $\nu_{\mathfrak{p}}(\alpha)$, подобно тому как в гл. I простому числу p мы сопоставляли p-адический показатель. Именно,

для каждого $\alpha \neq 0$ из $\mathfrak{O}$ через $\nu_{\mathfrak{p}}(\alpha)$ обозначим показатель степени, с которым $\mathfrak{p}$ входит в разложение главного дивизора (α) на простые множители. Очевидно, что $\nu_{\mathfrak{p}}(\alpha)$ характеризуется также тем, что

$$\mathfrak{p}^{\nu_{\mathfrak{p}}(\alpha)} \mid \alpha \quad \text{и} \quad \mathfrak{p}^{\nu_{\mathfrak{p}}(\alpha)+1} \nmid \alpha.$$

Так как нуль делится на сколь угодно большую степень $\mathfrak{p}$, то естественно положить $\nu_{\mathfrak{p}}(0) = \infty$.

Из определения легко следуют следующие свойства функции $\nu_{\mathfrak{p}}(\alpha)$:

$$\nu_{\mathfrak{p}}(\alpha\beta) = \nu_{\mathfrak{p}}(\alpha) + \nu_{\mathfrak{p}}(\beta), \tag{3}$$

$$\nu_{\mathfrak{p}}(\alpha + \beta) \geqslant \min\left(\nu_{\mathfrak{p}}(\alpha), \nu_{\mathfrak{p}}(\beta)\right) \tag{4}$$

(при доказательстве свойства (4) следует воспользоваться условием 2°).

Функцию $\nu_{\mathfrak{p}}(\alpha)$ мы можем распространить на поле отношений K кольца $\mathfrak{O}$ с сохранением свойств (3) и (4). Именно, для произвольного $\xi = \alpha/\beta \in K$ $(\alpha, \beta \in \mathfrak{O})$ положим

$$\nu_{\mathfrak{p}}(\xi) = \nu_{\mathfrak{p}}(\alpha) - \nu_{\mathfrak{p}}(\beta).$$

Значение $\nu_{\mathfrak{p}}(\xi)$, очевидно, не зависит от способа представления ξ в виде $\xi = \alpha/\beta$. Легко проверяется также, что свойства (3) и (4) выполняются и для расширенной функции $\nu_{\mathfrak{p}}$.

Выясним теперь, какие значения принимает функция $\nu_{\mathfrak{p}}(\alpha)$, когда α пробегает все элементы поля K. Так как дивизоры $\mathfrak{p}$ и $\mathfrak{p}^2$ различны, то по условию 3° существует элемент $\gamma \in \mathfrak{O}$, делящийся на $\mathfrak{p}$ и не делящийся на $\mathfrak{p}^2$. Для этого элемента имеем: $\nu_{\mathfrak{p}}(\gamma) = 1$. Но тогда $\nu_{\mathfrak{p}}(\gamma^k) = k$ при любом целом k. Этим доказано, что функция $\nu_{\mathfrak{p}}(\alpha)$ при отличных от нуля α принимает все целые рациональные значения.

Определение. *Пусть K — произвольное поле. Функция $\nu(\alpha)$, определенная на элементах $\alpha \in K$, называется показателем поля K, если она удовлетворяет условиям:*

1. *$\nu(\alpha)$ принимает все целые рациональные значения, когда α пробегает все отличные от нуля элементы из K; $\nu(0) = \infty$.*

2. $$\nu(\alpha\beta) = \nu(\alpha) + \nu(\beta).$$

3. $$\nu(\alpha + \beta) \geqslant \min(\nu(\alpha), \nu(\beta)).$$

Мы можем теперь сказать, что каждый простой дивизор $\mathfrak{p}$ кольца $\mathfrak{O}$ определяет некоторый показатель $\nu_{\mathfrak{p}}(\alpha)$ поля отношений K. Легко видеть, что для различных простых дивизоров $\mathfrak{p}$ и $\mathfrak{q}$ соответствующие им показатели $\nu_{\mathfrak{p}}$ и $\nu_{\mathfrak{q}}$ также различны. В самом деле, по условию 3° в кольце $\mathfrak{O}$ существует элемент γ, деля-

щийся на $\mathfrak{p}$ и не делящийся на $\mathfrak{q}$. Но тогда $\nu_{\mathfrak{p}}(\gamma) \geqslant 1$ и $\nu_{\mathfrak{q}}(\gamma) = 0$, а значит, $\nu_{\mathfrak{p}} \neq \nu_{\mathfrak{q}}$.

Все показатели поля K вида $\nu_{\mathfrak{p}}$ обладают, очевидно, свойством:

$$\nu_{\mathfrak{p}}(\alpha) \geqslant 0 \text{ при всех } \alpha \in \mathfrak{O}. \tag{5}$$

В терминах показателей $\nu_{\mathfrak{p}}$ очень просто записывается разложение главного дивизора (α), соответствующего элементу $\alpha \in \mathfrak{O}^*$, на простые множители. Простые дивизоры $\mathfrak{p}_i$, входящие в это разложение, характеризуются условием $\nu_{\mathfrak{p}_i}(\alpha) > 0$. Само же разложение имеет вид

$$(\alpha) = \prod_i \mathfrak{p}_i^{\nu_{\mathfrak{p}_i}(\alpha)}, \tag{6}$$

где $\mathfrak{p}_i$ пробегает все простые дивизоры с условием $\nu_{\mathfrak{p}_i}(\alpha) > 0$.

Мы видим, таким образом, что полугруппа дивизоров $\mathfrak{D}$ и гомоморфизм $\mathfrak{O}^* \to \mathfrak{D}$ вполне определяются заданием множества всех показателей $\nu_{\mathfrak{p}}$ поля K, соответствующих простым дивизорам $\mathfrak{p}$. Действительно, множество всех дивизоров и закон их умножения однозначно определяются заданием простых дивизоров (каждый дивизор есть произведение степеней простых дивизоров с неотрицательными показателями, а при умножении дивизоров соответствующие показатели складываются). Что касается простых дивизоров, то это — некоторые объекты $\mathfrak{p}$, взаимно однозначно соответствующие показателям $\nu_{\mathfrak{p}}$. Наконец, и это самое важное, равенство (6) определяет гомоморфизм $\mathfrak{O}^* \to \mathfrak{D}$.

Это показывает, что в основу построения теории дивизоров может быть положено понятие показателя $\nu(\alpha)$. На этой мысли и будет основано дальнейшее изложение.

Прежде всего нам надо выяснить следующий важный вопрос: чем характеризуется множество $\mathfrak{N}$ всех тех показателей ν поля K, которые можно взять для построения теории дивизоров кольца $\mathfrak{O}$?

Так как произведение (6) должно содержать только конечное число множителей с ненулевыми показателями $\nu_{\mathfrak{p}_i}(\alpha)$, то, следовательно, множество показателей $\mathfrak{N}$ должно удовлетворять условию $\nu(\alpha) = 0$ почти для всех $\nu \in \mathfrak{N}$ при любом фиксированном $\alpha \in \mathfrak{O}^*$ (выражение «почти для всех» означает: для всех, за исключением конечного числа).

Далее, в силу (5) для всех $\nu \in \mathfrak{N}$ мы должны иметь $\nu(\alpha) \geqslant 0$, если только $\alpha \in \mathfrak{O}$. Обратно, предположим, что для некоторого $\xi \neq 0$ из K выполнены неравенства $\nu(\xi) \geqslant 0$ при всех $\nu \in \mathfrak{N}$. Если мы представим ξ в виде $\xi = \alpha/\beta$ $(\alpha, \beta \in \mathfrak{O})$, то наши условия запишутся в виде $\nu(\alpha) \geqslant \nu(\beta)$ при всех $\nu \in \mathfrak{N}$. Но это, очевидно, эквивалентно тому, что главный дивизор (α) делится на главный

дивизор (β). В силу условия 1° получаем отсюда, что α делится на β в кольце $\mathfrak{O}$, т. е. что $\xi \in \mathfrak{O}$. Мы получили, таким образом, второе необходимое условие: множество показателей $\mathfrak{N}$ должно быть таким, чтобы неравенства $\nu(\alpha) \geqslant 0$ при всех $\nu \in \mathfrak{N}$ были справедливы для элементов кольца $\mathfrak{O}$, и только для них.

Чтобы выявить еще одно свойство множества $\mathfrak{N}$, выберем в нем произвольно конечное число показателей $\nu_1, \ldots, \nu_m$, соответствующих простым дивизорам $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Фиксировав, далее, неотрицательные целые числа $k_1, \ldots, k_m$, рассмотрим дивизор $\mathfrak{a} = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_m^{k_m}$. В силу условия 3° в кольце $\mathfrak{O}$ существует элемент α_i, делящийся на $\mathfrak{a}_i = \mathfrak{a}\mathfrak{p}_1 \ldots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \ldots \mathfrak{p}_m$ и не делящийся на $\mathfrak{a}_i\mathfrak{p}_i$ $(1 \leqslant i \leqslant m)$. Рассмотрим сумму

$$\alpha = \alpha_1 + \ldots + \alpha_m.$$

Пользуясь условием 2°, легко получим, что элемент α делится на $\mathfrak{p}_i^{k_i}$ и не делится на $\mathfrak{p}_i^{k_i+1}$. Этим доказано, что множество $\mathfrak{N}$ удовлетворяет также следующему необходимому условию: для произвольных показателей $\nu_1, \ldots, \nu_m$ из $\mathfrak{N}$ и произвольных неотрицательных целых чисел $k_1, \ldots, k_m$ в кольце $\mathfrak{O}$ существует элемент α, для которого $\nu_i(\alpha) = k_i$ $(1 \leqslant i \leqslant m)$.

Найденные нами необходимые условия оказываются также и достаточными для того, чтобы с помощью показателей из $\mathfrak{N}$ можно было построить теорию дивизоров кольца $\mathfrak{O}$. Для доказательства рассмотрим полугруппу $\mathfrak{D}$ с однозначным разложением на простые множители, простые элементы которой находятся во взаимно однозначном соответствии с показателями из $\mathfrak{N}$. Показатель $\nu \in \mathfrak{N}$, соответствующий простому элементу $\mathfrak{p} \in \mathfrak{D}$, будем обозначать также через $\nu_\mathfrak{p}$. В силу первого и второго условий для любого $\alpha \in \mathfrak{O}^*$ произведение (6) будет иметь смысл (показатели $\nu_{\mathfrak{p}_i}(\alpha)$ неотрицательны, причем только конечное число из них отлично от нуля). Ввиду свойства $\nu(\alpha\beta) = \nu(\alpha) + \nu(\beta)$ отображение $\alpha \to (\alpha)$ будет гомоморфизмом $\mathfrak{O}^*$ в $\mathfrak{D}$. Из второго условия легко вытекает, что делимость α на β в кольце $\mathfrak{O}$ эквивалентна неравенствам $\nu(\alpha) \geqslant \nu(\beta)$ для всех $\nu \in \mathfrak{N}$. Это обеспечивает выполнение условия 1°. Условие 2° непосредственно следует из неравенства $\nu(\alpha \pm \beta) \geqslant \min(\nu(\alpha), \nu(\beta))$. Если $\mathfrak{a}$ и $\mathfrak{b}$ — два различных элемента из $\mathfrak{D}$, то некоторый простой элемент $\mathfrak{p}$ входит в их разложения на простые множители с различными показателями, скажем, k и l соответственно. Пусть $k < l$. Согласно третьему условию в $\mathfrak{O}$ существует элемент α, делящийся на $\mathfrak{a}$, для которого $\nu_\mathfrak{p}(\alpha) = k$. Этот элемент α не будет делиться на $\mathfrak{b}$. Этим мы доказали, что условие 3° также выполнено. Гомоморфизм $\mathfrak{O}^* \to \mathfrak{D}$ дает нам, следовательно, теорию дивизоров для кольца $\mathfrak{O}$.

Сформулируем полученный нами результат.

Теорема 4. *Пусть $\mathfrak{O}$ — кольцо, K — его поле отношений и $\mathfrak{N}$ — некоторое множество показателей поля K. Для того чтобы*

показатели из $\mathfrak{N}$ определяли теорию дивизоров для кольца $\mathfrak{O}$, необходимо и достаточно, чтобы выполнялись условия:

1) *для всякого $\alpha \neq 0$ из $\mathfrak{O}$ существует только конечное число показателей $\nu \in \mathfrak{N}$, для которых $\nu(\alpha) \neq 0$;*

2) *элемент α из K принадлежит $\mathfrak{O}$ тогда и только тогда, когда $\nu(\alpha) \geqslant 0$ при всех $\nu \in \mathfrak{N}$;*

3) *для произвольной конечной системы различных показателей $\nu_1, \ldots, \nu_m$ из $\mathfrak{N}$ и произвольных неотрицательных целых чисел $k_1, \ldots, k_m$ в кольце $\mathfrak{O}$ существует элемент α, для которого*

$$\nu_1(\alpha) = k_1, \ \ldots, \ \nu_m(\alpha) = k_m.$$

Построение теории дивизоров для данного кольца $\mathfrak{O}$ сводится, таким образом, к построению в его поле отношений K соответствующего множества показателей $\mathfrak{N}$.

Мы не будем вдаваться в анализ целозамкнутых колец, для которых возможно построение теории дивизоров (см. замечание в конце пункта). В следующем параграфе мы докажем, что если для кольца $\mathfrak{o}$ с полем отношений k теория дивизоров существует, то она существует и в целом замыкании $\mathfrak{O}$ кольца $\mathfrak{o}$ в произвольном конечном расширении K поля k. Так как для кольца $\mathbb{Z}$ целых рациональных чисел теория дивизоров хорошо известна (здесь имеет место однозначность разложения на простые множители), то этим будет доказано также существование теории дивизоров и для максимальных порядков в полях алгебраических чисел.

Набор показателей ν поля K, которые надо взять для построения теории дивизоров, существенным образом зависит, конечно, от кольца $\mathfrak{O}$, и, вообще говоря, этот набор не будет исчерпывать все показатели поля K (задача 6). Может даже случиться (задача 7), что для всех показателей поля K условие 1) теоремы 4 не будет выполняться. Покажем, однако, что в случае кольца целых рациональных чисел $\mathbb{Z}$ соответствующий набор показателей исчерпывает все показатели поля рациональных чисел $\mathbb{Q}$ (в дальнейшем мы увидим, что аналогичный факт справедлив и для максимальных порядков в произвольных полях алгебраических чисел).

Каждому простому числу $p \in \mathbb{Z}$ (т. е. простому дивизору кольца $\mathbb{Z}$) соответствует показатель ν_p поля $\mathbb{Q}$, значения которого для отличного от нуля рационального числа

$$x = p^m a/b \tag{7}$$

(a и b целые, не делящиеся на p) определяются равенством

$$\nu_p(x) = m. \tag{8}$$

Этот показатель ν_p называется *p-адическим показателем* поля $\mathbb{Q}$ (очевидно, что значения показателя (8) совпадают со значениями p-адического показателя на поле p-адических чисел $\mathbb{Q}_p$; см. гл. I, § 3, п. 2).

Теорема 5. *Все показатели поля рациональных чисел исчерпываются p-адическими показателями ν_p (для всех простых p).*

Доказательство. Пусть ν — произвольный показатель поля $\mathbf{Q}$. Так как

$$\nu(1+\ldots+1) \geqslant \min(\nu(1), \ldots, \nu(1)) = 0,$$

то $\nu(n) \geqslant 0$ при всех натуральных n. Если бы $\nu(p) = 0$ для всех простых p, то мы имели бы также $\nu(a) = 0$ для всех $a \neq 0$ из $\mathbf{Q}$, что невозможно по условию 1 определения показателя. Следовательно, для некоторого простого p мы должны иметь $\nu(p) = e > 0$. Пусть для простого $q \neq p$ имеем также $\nu(q) > 0$; тогда из равенства $pu + qv = 1$ с целыми u и v будет следовать

$$0 = \nu(pu + qv) \geqslant \min(\nu(pu), \nu(qv)) \geqslant \min(\nu(p), \nu(q)) > 0.$$

Полученное противоречие показывает, что $\nu(q) = 0$ для всех простых чисел q, отличных от p, а значит, $\nu(a) = 0$ для всех целых a, не делящихся на p. Для рационального числа (7) имеем, таким образом,

$$\nu(x) = m\nu(p) + \nu(a) - \nu(b) = me = e\nu_p(x).$$

Так как значения показателя ν должны охватить все целые числа, то $e = 1$ и, следовательно, $\nu = \nu_p$. Теорема 5 доказана.

Заметим, что теорему 5 можно было бы легко вывести из теоремы 3 § 4 гл. I, вторая часть доказательства которой совпадает, по существу, с только что проведенным доказательством.

Рассмотрим в заключение еще один частный случай.

Предположим, что для некоторого кольца $\mathfrak{O}$ мы имеем теорию дивизоров $\mathfrak{O}^* \to \mathfrak{D}$ с конечным числом простых дивизоров $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Обозначим через $\nu_1, \ldots, \nu_m$ соответствующие показатели поля отношений K. Согласно условию 3) теоремы 4 для произвольного дивизора $\mathfrak{a} = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_m^{k_m} \in \mathfrak{D}\ (k_i \geqslant 0)$ в кольце $\mathfrak{O}$ существует элемент α, для которого $\nu_1(\alpha) = k_1, \ldots, \nu_m(\alpha) = k_m$. Но это значит, что дивизор $\mathfrak{a}$ совпадает с главным дивизором (α). Таким образом, все дивизоры из $\mathfrak{D}$ главные, и, значит, в кольце $\mathfrak{O}$ имеет место однозначность разложения на простые множители (теорема 2). Если $\mathfrak{p}_1 = (\pi_1), \ldots, \mathfrak{p}_m = (\pi_m)$, то элементы $\pi_1, \ldots, \pi_m$ составляют полную систему попарно не ассоциированных простых элементов кольца $\mathfrak{O}$ и каждый элемент $\alpha \in \mathfrak{O}^*$ однозначно представляется в виде

$$\alpha = \varepsilon \pi_1^{k_1} \ldots \pi_m^{k_m},$$

где ε — единица в $\mathfrak{O}$. Простые элементы $\pi_1, \ldots, \pi_m$ характеризуются, очевидно, также условиями:

$$\nu_i(\pi_i) = 1, \quad \nu_j(\pi_i) = 0 \quad \text{при} \quad j \neq i.$$

Нами доказан следующий результат.

Теорема 6. *Если для некоторого кольца $\mathfrak{O}$ мы имеем теорию дивизоров с конечным числом простых дивизоров, то в $\mathfrak{O}$ имеет место однозначность разложения на простые множители.*

Замечание. Согласно задаче 15 кольцо $\mathfrak{O}$ с теорией дивизоров вполне целозамкнуто. Далее, из задачи 16 § 6 легко следует, что в кольце с теорией дивизоров для каждого целого d-идеала A существует лишь конечное число целых d-идеалов, содержащих этот идеал A (поскольку для целого дивизора существует лишь конечное число целых делителей). Эти два необходимых условия, оказывается, и достаточны для того, чтобы для кольца $\mathfrak{O}$ существовала теория дивизоров. Другими словами, кольцо $\mathfrak{O}$ допускает теорию дивизоров тогда и только тогда, когда оно вполне целозамкнуто и для целых d-идеалов в $\mathfrak{O}$ выполнено условие максимальности (т. е. в каждом непустом семействе целых d-идеалов имеется d-идеал, не содержащийся ни в каком другом d-идеале этого семейства). Кольца, удовлетворяющие двум последним условиям, носят название колец Крулля. Кольца с теорией дивизоров совпадают, таким образом, с кольцами Крулля (см. [4], гл. VII). Кольца Крулля могут быть охарактеризованы также как пересечения $\bigcap_{\nu \in \mathfrak{N}} \mathfrak{O}_\nu$ колец показателей $\mathfrak{O}_\nu$ для показателей ν из семейств $\mathfrak{N}$, удовлетворяющих условию: для каждого $\alpha \neq 0$ из K существует лишь конечное число показателей $\nu \in \mathfrak{N}$, для которых $\nu(\alpha) \neq 0$. Согласно задаче 6 § 4 Дополнения всякое целозамкнутое нётерово кольцо вполне целозамкнуто. Поэтому нётерово кольцо допускает теорию дивизоров тогда и только тогда, когда оно целозамкнуто (см. [5], § 140).

Задачи

1. Доказать, что если для кольца $\mathfrak{O}$ существует теория дивизоров, то каждый элемент из $\mathfrak{O}$ имеет лишь конечное число не ассоциированных между собой делителей.

2. Доказать, что в произвольной теории дивизоров всякий дивизор является общим наибольшим делителем двух главных дивизоров.

3. Пусть $K = k(x)$ — поле рациональных функций над произвольным полем k и φ — некоторый неприводимый многочлен из кольца $k[x]$. Каждую рациональную функцию $u \neq 0$ из K можно представить в виде $u = \varphi^m f/g$, где f и g — многочлены из $k[x]$, не делящиеся на φ. Показать, что функция ν_φ, определенная равенством $\nu_\varphi(u) = m$, является показателем поля K.

4. Если отличные от нуля многочлены f и g из кольца $k[x]$ имеют соответственно степени n и m, то для рациональной функции $u = f/g \in k(x)$ положим $\nu^*(u) = m - n$. Доказать, что функция ν^* является показателем поля $K = k(x)$.

5. Доказать, что показатели ν_Φ (для всех неприводимых многочленов φ кольца $k[x]$) и показатель ν^* (задачи 3 и 4) исчерпывают собой все показатели ν поля $k(x)$, для которых $\nu(a) = 0$ при всех $a \neq 0$ из k.

6. Определить множество показателей $\mathfrak{N}$ поля $K = k(x)$, удовлетворяющих условиям теоремы 4, если в качестве $\mathfrak{O}$ взять кольцо $k[x]$. Определить, далее, множество $\mathfrak{N}$ для кольца $\mathfrak{O}' = k[1/x]$.

7. Пусть $K = k(x, y)$ — поле рациональных функций от x и y над полем k. Для произвольного натурального n положим

$$x_n = \frac{x}{y^n}.$$

Отличную от нуля рациональную функцию $u = u(x, y) \in K$ представим в виде

$$u = u\left(x_n y^n, y\right) = y^m \frac{f(x_n, y)}{g(x_n, y)},$$

где многочлены f и g не делятся на y. Показать, что функция ν_n, определенная равенством $\nu_n(u) = m$, является показателем поля K. Показать далее, что все показатели ν_n $(n \geqslant 1)$ различны и для всех них $\nu_n(x) > 0$.

8. Известный признак неприводимости Эйзенштейна для целочисленных многочленов сформулировать и доказать для многочленов с коэффициентами из произвольного кольца $\mathfrak{O}$ с теорией дивизоров.

9. Доказать, что если для кольца $\mathfrak{O}$ существует теория дивизоров, то для его поля отношений K существуют алгебраические расширения произвольной степени.

10. Для многочлена $f \neq 0$ из кольца многочленов $\mathfrak{O} = k[x, y]$ от двух переменных над полем k через $\bar{\nu}(f)$ обозначим наименьшую степень одночленов, входящих в f с ненулевым коэффициентом. Показать, что функция $\bar{\nu}$ может быть продолжена до показателя поля рациональных функций $k(x, y)$. Обозначим через $\mathfrak{R}$ множество показателей поля $k(x, y)$, соответствующих неприводимым многочленам кольца $\mathfrak{O}$. Какое из условий теоремы 4 не выполняется для кольца $\mathfrak{O}$ и множества показателей $\mathfrak{R}_1$, получающегося из $\mathfrak{R}$ присоединением показателя $\bar{\nu}$?

11. Доказать, что условие 3° в определении теории дивизоров эквивалентно условию: каждый элемент $\mathfrak{a} \in \mathfrak{O}$ является общим наибольшим делителем элементов вида $(\alpha_1), \ldots, (\alpha_n)$, где $\alpha_i \in \mathfrak{O}^*$ $(1 \leqslant i \leqslant n)$.

12. Пусть для гомоморфизма $\mathfrak{O}^* \to \mathfrak{D}$ выполнено условие 3° определения теории дивизоров. Показать, что для любого $\mathfrak{a} \in \mathfrak{D}$ в полугруппе $\mathfrak{O}^*$ существуют такие элементы $\alpha, \alpha_1, \ldots \alpha_n$, что произведение $(\alpha)\mathfrak{a}$ есть общее *наименьшее кратное элементов* $(\alpha_1), \ldots, (\alpha_n)$.

Указание. Выберем элементы $\beta \in \mathfrak{O}^*$ и $\mathfrak{b} \in \mathfrak{D}$ так, чтобы $(\beta) = \mathfrak{a}\mathfrak{b}$. Согласно задаче 11 $\mathfrak{b}$ есть общий наибольший делитель элементов вида $(\beta_1), \ldots, (\beta_n)$, где $\beta_i \in \mathfrak{O}^*$. Положим $\alpha = \beta_1 \ldots \beta_n$ и $\alpha_i = \alpha\beta/\beta_i$ $(1 \leqslant i \leqslant n)$.

13. Основываясь на предыдущей задаче, показать, что условие 2° в определении теории дивизоров является следствием условий 1° и 3°.

14. Пусть $\mathfrak{O}$ — кольцо с теорией дивизоров. Доказать, что кольцо многочленов $\mathfrak{O}[x_1, \ldots, x_n]$ является также кольцом с теорией дивизоров.

15. Доказать, что всякое кольцо с теорией дивизоров вполне целозамкнуто (см. задачу 5 § 4 Дополнения).

§ 4. Показатели

Согласно теореме 4 § 3 построение теории дивизоров в целозамкнутом кольце $\mathfrak{O}$ сводится к построению в его поле отношений K показателей, обладающих указанными в этой теореме свойствами. Займемся поэтому систематическим изучением свойств показателей.

1. Простейшие свойства показателей. Из определения показателя ν в произвольном поле K (§ 3, п. 4) непосредственно

вытекают следующие его свойства:

$$\nu(\pm 1)=0; \qquad \nu(-\alpha)=\nu(\alpha);$$
$$\nu(\alpha/\beta)=\nu(\alpha)-\nu(\beta), \quad \beta\neq 0; \qquad \nu(\alpha^n)=n\nu(\alpha), \quad n\in\mathbb{Z};$$
$$\nu(\alpha_1+\ldots+\alpha_n)\geqslant \min(\nu(\alpha_1), \ldots, \nu(\alpha_n)).$$

Предположим, что $\nu(\alpha)\neq\nu(\beta)$. Если $\nu(\alpha)>\nu(\beta)$, то $\nu(\alpha+\beta)\geqslant \nu(\beta)$. С другой стороны, из равенства $\beta=(\alpha+\beta)-\alpha$ получаем $\nu(\beta)\geqslant\min(\nu(\alpha+\beta), \nu(\alpha))$, откуда $\nu(\beta)\geqslant\nu(\alpha+\beta)$. Таким образом,

$$\nu(\alpha+\beta)=\min(\nu(\alpha), \nu(\beta)), \qquad \text{если} \qquad \nu(\alpha)\neq\nu(\beta). \tag{1}$$

Индукцией по числу слагаемых отсюда легко получаем, что

$$\nu(\alpha_1+\ldots+\alpha_n)=\min(\nu(\alpha_1), \ldots, \nu(\alpha_n)),$$

если только среди значений $\nu(\alpha_1), \ldots, \nu(\alpha_n)$ имеется только одно наименьшее.

Определение. *Пусть на поле K задан показатель ν. Подкольцо $\mathfrak{O}_\nu$ поля K, состоящее из тех элементов $\alpha\in K$, для которых $\nu(\alpha)\geqslant 0$, называется кольцом показателя ν. Элементы из $\mathfrak{O}_\nu$ называются целыми относительно показателя ν.*

Очевидно, что для кольца $\mathfrak{O}_\nu$ и множества $\mathfrak{N}$, состоящего только из одного показателя ν, выполнены все три условия теоремы 4 § 3. Для кольца $\mathfrak{O}_\nu$ существует, следовательно, теория дивизоров с единственным простым дивизором. Теоремы 3 и 6 § 3 дают нам поэтому следующие результаты:

Теорема 1. *Кольцо $\mathfrak{O}_\nu$ показателя ν поля K целозамкнуто в K.*

Теорема 2. *С точностью до ассоциированности в кольце $\mathfrak{O}_\nu$ имеется только один простой элемент π, и всякий элемент $\alpha\neq 0$ из $\mathfrak{O}_\nu$ однозначно (при фиксированном π) представляется в виде $\alpha=\varepsilon\pi^m$, где ε — единица в $\mathfrak{O}_\nu$ $(m\geqslant 0)$.*

Простой элемент π кольца показателя ν характеризуется, очевидно, равенством $\nu(\pi)=1$.

В кольце $\mathfrak{O}_\nu$, как и во всяком кольце, можно рассматривать сравнения по модулю элемента (см. Дополнение, § 4, п. 1). Так как сравнения по модулю ассоциированных элементов равносильны, то кольцо классов вычетов кольца $\mathfrak{O}_\nu$ по модулю простого элемента π не зависит от выбора π и, следовательно, вполне определено самим кольцом $\mathfrak{O}_\nu$. Обозначим это кольцо классов вычетов через Σ_ν и покажем, что оно в данном случае является полем. Действительно, если $\alpha\in\mathfrak{O}_\nu$ и $\alpha\not\equiv 0 (\mathrm{mod}\,\pi)$, то $\nu(\alpha)=0$ и, значит, α является единицей в $\mathfrak{O}_\nu$. Но в таком случае не только сравнение $\alpha\xi\equiv 1 (\mathrm{mod}\,\pi)$, но и уравнение $\alpha\xi=1$ разрешимо относительно элемента $\xi\in\mathfrak{O}_\nu$.

Поле Σ_ν называется *полем вычетов показателя ν*.

2. Независимость показателей. Пусть для кольца $\mathfrak{O}$ мы имеем теорию дивизоров $\mathfrak{D}^*\to\mathfrak{D}$, и пусть $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ — различные простые дивизоры из $\mathfrak{D}$. Согласно теореме 4 § 3 соответствующие этим

простым дивизорам показатели $\nu_1, \ldots, \nu_m$ поля отношений K обладают свойством независимости, выражающимся в том, что в K^* существуют элементы ξ, на которых эти показатели принимают любые наперед заданные значения $k_1, \ldots, k_m$. Действительно, если для каждого $i = 1, \ldots, m$ мы положим $k_i' = \max(0, k_i)$, $k_i'' = \min(0, k_i)$, то согласно условию 3) упомянутой теоремы в $\mathfrak{O}$ найдутся элементы α и β с условиями $\nu_i(\alpha) = k_i'$, $\nu_i(\beta) = -k_i''$, а тогда для их отношения $\xi = \alpha/\beta$ будем иметь

$$\nu_i(\xi) = k_i, \quad 1 \leqslant i \leqslant m.$$

Мы докажем, что это свойство независимости не связано с тем обстоятельством, что показатели ν_i соответствуют простым дивизорам в некоторой теории дивизоров, а имеет место для любой конечной системы показателей.

Теорема 3. *Если $\nu_1, \ldots, \nu_m$ — попарно различные показатели поля K, то для любых целых рациональных чисел $k_1, \ldots, k_m$ существует элемент $\xi \in K$, для которого*

$$\nu_1(\xi) = k_1, \ldots, \nu_m(\xi) = k_m.$$

Эта теорема о независимости конечной системы показателей будет получена нами как простое следствие более сильной теоремы 4. Сформулируем одно следствие теоремы 3.

Обозначим через $\mathfrak{O}_1, \ldots, \mathfrak{O}_m$ кольца показателей $\nu_1, \ldots, \nu_m$ и через $\mathfrak{O}$ пересечение $\bigcap_{i=1}^{m} \mathfrak{O}_i$. Для кольца $\mathfrak{O}$ и для множества показателей $\mathfrak{N}$, состоящего из $\nu_1, \ldots, \nu_m$, условия 1) и 2) теоремы 4 § 3 выполняются очевидным образом. Сформулированная теорема 3 показывает, что условие 3) также выполнено, а значит, для кольца $\mathfrak{O}$ мы имеем теорию дивизоров с конечным числом простых дивизоров. Теорема 3 означает, таким образом, что любая конечная система показателей $\nu_1, \ldots, \nu_m$ поля K определяет теорию дивизоров в кольце $\mathfrak{O} = \bigcap_{i=1}^{m} \mathfrak{O}_i$. Ввиду теоремы 6 § 3 это дает нам следующий результат.

Следствие. *Если $\mathfrak{O}_1, \ldots, \mathfrak{O}_m$ — кольца попарно различных показателей $\nu_1, \ldots, \nu_m$ поля K, то пересечение $\mathfrak{O} = \bigcap_{i=1}^{m} \mathfrak{O}_i$ является кольцом с однозначным разложением на простые множители. Именно, каждый элемент $\alpha \neq 0$ из $\mathfrak{O}$ однозначно представляется в виде $\alpha = \varepsilon \pi_1^{k_1} \ldots \pi_m^{k_m}$, где ε — единица в $\mathfrak{O}$, а $\pi_1, \ldots, \pi_m$ — фиксированные простые элементы, характеризуемые условиями*

$$\nu_i(\pi_i) = 1, \qquad \nu_j(\pi_i) = 0, \qquad j \neq i.$$

Теорема 4 (об аппроксимации). *Если $\nu_1, \ldots, \nu_m$ — попарно различные показатели поля K, то для любых элементов $\xi_1, \ldots$*

..., ξ_m из K и любого целого N в поле K найдется элемент ξ, для которого

$$v_1(\xi-\xi_1)\geqslant N,\ \ldots,\ v_m(\xi-\xi_m)\geqslant N.$$

Доказательство. 1°. Докажем сначала, что если для колец $\mathfrak{O}_1$ и $\mathfrak{O}_2$ показателей v_1 и v_2 поля K имеет место включение $\mathfrak{O}_1\subset\mathfrak{O}_2$, то $v_1=v_2$. Действительно, всякая единица ε кольца $\mathfrak{O}_1$ является также единицей и в кольце $\mathfrak{O}_2$, и поэтому $v_2(\varepsilon)=0$. Если теперь π — простой элемент кольца $\mathfrak{O}_1$, то произвольный элемент $\xi\in K^*$ представляется в виде $\xi=\pi^{v_1(\xi)}\varepsilon$ (ε — единица кольца $\mathfrak{O}_1$), а значит,

$$v_2(\xi)=v_1(\xi)l, \tag{2}$$

где $l=v_2(\pi)\geqslant 0$. Ясно, что равенство (2) возможно только при $l=1$, и, следовательно, $v_2=v_1$.

2°. Покажем теперь, что если показатели $v_1,\ \ldots,\ v_m$ ($m\geqslant 2$) попарно различны, то в поле K существует такой элемент α, что

$$v_1(\alpha)>0,\qquad v_j(\alpha)<0,\qquad j=2,\ \ldots,\ m. \tag{3}$$

Будем доказывать это утверждение индукцией по m. Пусть $m=2$. По доказанному выше включения $\mathfrak{O}_1\subset\mathfrak{O}_2$ и $\mathfrak{O}_2\subset\mathfrak{O}_1$ невозможны, поэтому в K^* найдутся такие элементы β и γ, что

$$v_1(\beta)\geqslant 0,\ \ v_2(\beta)<0;\qquad v_1(\gamma)<0,\ \ v_2(\gamma)\geqslant 0.$$

Но тогда для $\alpha=\beta/\gamma$ имеем

$$v_1(\alpha)>0,\qquad v_2(\alpha)<0.$$

Пусть $m\geqslant 3$, и пусть для случая $m-1$ показателей наше утверждение уже доказано. Выберем тогда в K^* элементы α_0 и δ так, чтобы

$$v_1(\alpha_0)>0,\qquad v_j(\alpha_0)<0,\qquad j=2,\ \ldots,\ m-1,$$
$$v_1(\delta)>0,\qquad v_m(\delta)<0,$$

и положим

$$\alpha=\alpha_0+\delta^r, \tag{4}$$

где натуральное r выберем с соблюдением условий: $v_j(\delta^r)\neq v_j(\alpha_0)$ при $j=2,\ \ldots,\ m$. Тогда

$$v_1(\alpha)\geqslant\min\left(v_1(\alpha_0),\ \gamma_1(\delta^r)\right)>0$$

и ввиду (1)

$$v_j(\alpha)=\min\left(v_j(\alpha_0),\ v_j(\delta^r)\right)<0$$

при всех $j=2,\ \ldots,\ m$. Таким образом, элемент (4) при надлежащем r удовлетворяет требованиям (3).

3°. Для доказательства утверждения теоремы 4 выберем в K элементы $\alpha_1,\ \ldots,\ \alpha_m$ так, чтобы

$$v_i(\alpha_i)>0,\qquad v_j(\alpha_i)<0,\qquad j\neq i,$$

и положим

$$\xi = \frac{1}{1+\alpha_1^r}\xi_1 + \ldots + \frac{1}{1+\alpha_m^r}\xi_m. \qquad (5)$$

Так как $v_j(\alpha_i^r) \neq 0 = v_j(1)$ при натуральном r, то по свойству (1) значение $v_j(1+\alpha_i^r)$ равно 0 при $i=j$ и равно $rv_j(\alpha_i) \leqslant -r$ при $i \neq j$. Следовательно,

$$v_j\left(\frac{1}{1+\alpha_i^r}\right) \geqslant r \quad \text{при} \quad i \neq j \quad \text{и} \quad v_j\left(\frac{-\alpha_j^r}{1+\alpha_j^r}\right) \geqslant r,$$

а значит, $v_j(\xi - \xi_j) \geqslant \min\limits_i (r + v_j(\xi_i))$. Ясно теперь, что элемент (5) будет удовлетворять неравенствам теоремы 4, если только

$$r \geqslant N - \min_{i,j} v_j(\xi_i).$$

Замечание. Каждый показатель поля K определяет на K некоторую метрику (см. начало § 1 гл. IV). Пусть $\varphi_1, \ldots, \varphi_m$ — метрики поля K, соответствующие попарно различным показателям $v_1, \ldots, v_m$. В терминах понятия метрики теорема 4 означает, что в поле K для любой системы элементов $\xi_1, \ldots, \xi_m$ можно найти элемент ξ, который будет сколь угодно близок к каждому из элементов ξ_i, если понимать близость каждый раз в смысле соответствующей метрики φ_i. Более точно это можно выразить также следующим образом. Пусть $K_i (1 \leqslant i \leqslant m)$ — метризованное поле, совпадающее как поле с K и наделенное метрикой φ_i (см. п. 1 § 4 гл. I). Поскольку метрика φ_i определяет на K_i топологию, то декартово произведение $\prod\limits_i K_i$ является топологическим пространством (топологическим кольцом). Утверждение теоремы 4 равносильно тому, что образ поля K при «диагональном» отображении $\xi \to (\xi, \ldots, \xi) \in \prod\limits_i K_i$, $\xi \in K$ является всюду плотным подмножеством в $\prod\limits_i K_i$.

Доказательство теоремы 3. Пусть $k_1, \ldots, k_m$ — произвольные целые числа. Для каждого $i = 1, \ldots, m$ в поле K существует такой элемент ξ_i, что $v_i(\xi_i) = k_i$. Положим $N = 1 + \max(k_1, \ldots, k_m)$. Согласно теореме 4 в K можно найти элемент ξ, для которого $v_i(\xi - \xi_i) \geqslant N$. Для этого элемента ξ имеем

$$v_i(\xi) = \min(v_i(\xi_i), v_i(\xi - \xi_i)) = k_i,$$

и теорема 3 доказана.

3. Продолжение показателей. Пусть k — произвольное поле, K/k — конечное расширение и v — некоторый показатель поля K. Рассматривая v лишь на элементах из k, мы получим функцию, которая будет, очевидно, также удовлетворять условиям 2 и 3 определения показателя (§ 3, п. 4). Что касается первого

условия, то оно для этой функции может и не выполняться, т. е. значения ν на элементах из k^* не обязательно исчерпают группу всех целых чисел $\mathbb{Z}$. Все эти значения не могут состоять, однако, только из нуля. В самом деле, если бы это было так, то поле k целиком содержалось бы в кольце показателя ν, а тогда в силу целозамкнутости этого кольца (теорема 1) в нем содержалось бы и поле K, что невозможно. Таким образом, среди значений $\nu(a)$, $a \in k^*$, имеются отличные от нуля, а значит, имеются и положительные (если $\nu(a) < 0$, то $\nu(a^{-1}) > 0$).

Обозначим через p какой-нибудь элемент из k, для которого $\nu(p) = e$ есть наименьшее положительное значение показателя ν на элементах поля k. Тогда для любого $a \in k^*$ значение $\nu(a) = m$ делится на e. Действительно, если $m = es + r$, $0 \leqslant r < e$, то $\nu(ap^{-s}) = m - se = r$, откуда в силу минимальности e следует, что $r = 0$. Полагая теперь

$$\nu_0(a) = \nu(a)/e, \quad a \in k^*, \quad \nu_0(0) = \infty, \tag{6}$$

мы получаем на k функцию ν_0, которая принимает уже все целые значения и которая является, следовательно, показателем поля k.

Определение. *Пусть K — конечное расширение поля k. Если показатель ν_0 поля k связан с показателем ν поля K соотношением* (6), *то говорят, что ν_0 индуцируется на k показателем ν, а ν является продолжением ν_0 на поле K. Однозначно определенное соотношением* (6) *натуральное число e называется при этом индексом ветвления ν относительно ν_0 (или относительно подполя k).*

В этом определении следует обратить внимание на то обстоятельство, что при $e > 1$ термин «продолжение показателя» не совпадает с обычным пониманием продолжения функции на более широкую область задания.

Согласно доказанному выше каждый показатель ν на K индуцирует некоторый (единственный) показатель ν_0 на k. Справедливо и обратное утверждение.

Теорема 5. *Для всякого показателя ν_0 поля k существует его продолжение на конечное расширение K поля k.*

Доказательство теоремы 5 мы проведем в следующем пункте. Сейчас же мы рассмотрим некоторые свойства продолжений данного ν_0, предполагая, что эти продолжения существуют.

Пусть $k \subset K \subset K'$ — цепочка конечных расширений и ν_0, ν, ν' — показатели полей k, K, K' соответственно. Очевидно, что если ν является продолжением ν_0 с индексом ветвления e, а ν' — продолжением ν с индексом ветвления e', то ν' будет продолжением ν_0 на поле K', причем индекс ветвления ν' относительно ν_0 будет равен ee'. Легко видеть также, что если ν_0 и ν индуцируются показателем ν' на подполях k и K, то ν является продолжением ν_0.

Лемма 1. *Если K — конечное расширение поля k степени n, то для произвольного показателя v_0 поля k существует не более n его продолжений на K.*

Доказательство. Пусть $v_1, \ldots, v_m$ — различные показатели поля K, являющиеся продолжениями v_0. По теореме 3 в поле K мы можем найти элементы $\xi_1, \ldots, \xi_m$, для которых $v_i(\xi_i) = 0$ и $v_j(\xi_i) = 1$ при $j \neq i$. Покажем, что эти элементы линейно независимы над k. Рассмотрим линейную комбинацию

$$\gamma = a_1\xi_1 + \ldots + a_m\xi_m$$

с коэффициентами a_j из k, не равными нулю одновременно. Пусть $r = \min(v_0(a_1), \ldots, v_0(a_m))$, и пусть индекс i_0 таков, что $v_0(a_{i_0}) = r$. Обозначая через e индекс ветвления показателя v_{i_0} относительно k, имеем

$$v_{i_0}(a_{i_0}\xi_{i_0}) = ev_0(a_{i_0}) + v_{i_0}(\xi_{i_0}) = er,$$

$$v_{i_0}(a_j\xi_j) = ev_0(a_j) + v_{i_0}(\xi_j) \geqslant er + 1, \qquad j \neq i_0,$$

поэтому

$$v_{i_0}(\gamma) = \min(v_{i_0}(a_1\xi_1), \ldots, v_{i_0}(a_m\xi_m)) = er,$$

а значит, $\gamma \neq 0$, что и доказывает наше утверждение. Из линейной независимости элементов $\xi_1, \ldots, \xi_m$ над полем k следует, что $m \leqslant (K : k)$, а это и значит, что число продолжений v_i не может быть больше n. Лемма 1 доказана.

Теорема 6. *Пусть v_0 — показатель поля k, $\mathfrak{o}$ — его кольцо и $\mathfrak{O}$ — целое замыкание кольца $\mathfrak{o}$ в конечном расширении K поля k. Если $v_1, \ldots, v_m$ — все продолжения показателя v_0 на поле K и $\mathfrak{O}_1, \ldots, \mathfrak{O}_m$ — их кольца, то* $\mathfrak{O} = \bigcap_{i=1}^{m} \mathfrak{O}_i$.

Доказательство. Так как $\mathfrak{o} \subset \mathfrak{O}_i$, а кольцо $\mathfrak{O}_i$ целозамкнуто в K, то $\mathfrak{O} \subset \mathfrak{O}_i$ при любом $i = 1, \ldots, m$, а значит,

$$\mathfrak{O} \subset \mathfrak{O}' = \bigcap_{i=1}^{m} \mathfrak{O}_i.$$

Доказательство обратного включения мы проведем в несколько этапов.

1) Предположим сначала, что K/k — конечное расширение Галуа и G — его группа Галуа. Для показателя v_i и автоморфизма $\sigma \in G$ рассмотрим функцию v_i^{σ}, определенную формулой

$$v_i^{\sigma}(\xi) = v_i(\sigma(\xi)), \qquad \xi \in K.$$

Ясно, что v_i^{σ} — показатель поля K. Легко видеть также, что v_i^{σ} — продолжение показателя v_0. В самом деле, если e_i — индекс ветвления v_i относительно k, то при $a \in k$ имеем

$$v_i^{\sigma}(a) = v_i(\sigma(a)) = v_i(a) = e_iv_0(a).$$

Так как $\nu_1, \ldots, \nu_m$ — это все продолжения ν_0 на поле K, то каждый показатель ν_i^{σ} совпадает с некоторым ν_j,

Пусть теперь ξ — произвольный элемент из $\mathfrak{O}'$. Так как

$$\nu_i(\sigma(\xi)) = \nu_i^{\sigma}(\xi) = \nu_j(\xi) \geqslant 0,$$

то вместе с ξ элементы $\sigma(\xi)$ $(\sigma \in G)$ также содержатся в $\mathfrak{O}'$. Согласно теореме 11 § 2 Дополнения характеристический многочлен $f(t) \in k[t]$ элемента ξ относительно расширения K/k в поле K имеет разложение

$$f(t) = t^n + a_1 t^{n-1} + \ldots + a_n = \prod_{\sigma \in G} (t - \sigma(\xi)).$$

Отсюда следует, что все коэффициенты a_s $(1 \leqslant s \leqslant n)$ содержатся в $\mathfrak{O}'$. Но, с другой стороны, $a_s \in k$, поэтому $a_s \in \mathfrak{O}' \cap k \subset \mathfrak{O}_v \cap k = \mathfrak{o}$. Таким образом, элемент ξ целый относительно $\mathfrak{o}$, т. е. $\xi \in \mathfrak{O}$. Равенство $\mathfrak{O} = \mathfrak{O}'$ для случая расширения Галуа доказано.

2) Пусть K — чисто несепарабельное расширение поля k характеристики p. Если $\xi \in K$, то $\xi^{p^n} = a \in k$ при некотором $n \geqslant 0$, и для продолжения ν показателя ν_0 на поле K с индексом ветвления e мы имеем

$$\nu(\xi) = \frac{1}{p^n}\nu(a) = \frac{e}{p^n}\nu_0(a).$$

Полученное равенство говорит о том, что для ν_0 имеется только одно продолжение на поле K, и $\mathfrak{O}'$ совпадает с кольцом $\mathfrak{O}_\nu$ показателя ν. Если теперь $\xi \in \mathfrak{O}' = \mathfrak{O}_\nu$, то $\nu(\xi) \geqslant 0$, $\nu_0(a) \geqslant 0$, $a \in \mathfrak{o}$ и $\xi \in \mathfrak{O}$, а значит, и в этом случае $\mathfrak{O} = \mathfrak{O}'$.

3) Пусть K/k — произвольное нормальное расширение. Если это расширение не является расширением Галуа, то согласно теореме 14 § 2 Дополнения существует такое промежуточное поле K_0, что K/K_0 — расширение Галуа и K_0/k — чисто несепарабельное расширение. По только что доказанному для ν_0 существует только одно продолжение $\bar{\nu}_0$ на поле K_0 и его кольцо $\mathfrak{O}_0$ совпадает с целым замыканием $\mathfrak{o}$ в K_0. Так как показатели $\nu_1, \ldots, \nu_m$ являются, очевидно, продолжениями и $\bar{\nu}_0$, то ввиду 1) для доказательства равенства $\mathfrak{O} = \mathfrak{O}'$ достаточно лишь заметить, что целое замыкание кольца $\mathfrak{O}_0$ в поле K совпадает с $\mathfrak{O}$ (задача 2 § 4 Дополнения).

4) Теперь мы можем рассмотреть случай произвольного конечного расширения K/k. Согласно теореме 12 § 2 Дополнения поле K можно погрузить в конечное нормальное расширение $\bar{K}/k$. Пусть ν_{ij} — все продолжения показателя ν_i на поле $\bar{K}$ и $\mathfrak{O}_{ij}$ — их кольца. Если $\bar{\mathfrak{O}}$ — целое замыкание $\mathfrak{o}$ в $\bar{K}$, то по доказанному

$\bar{\mathfrak{O}} = \bigcap_{i,j} \mathfrak{O}_{ij}$, откуда

$$\mathfrak{O} = \bar{\mathfrak{O}} \cap K = \bigcap_{i,j} (\mathfrak{O}_{ij} \cap K) = \bigcap_{i=1}^{m} \mathfrak{O}_i,$$

и теорема 6 доказана полностью.

Теорема 7. *В кольце* $\mathfrak{O}$ (*при обозначениях предыдущей теоремы*) *имеет место однозначность разложения на простые множители; при этом набор показателей поля* K, *соответствующих простым элементам в* $\mathfrak{O}$, *совпадает со всеми продолжениями* $\nu_1, \ldots, \nu_m$ *показателя* ν_0 *на поле* K. *Если* $\pi_1, \ldots, \pi_m$ — *простые элементы в* $\mathfrak{O}$, *занумерованные так, что* $\nu_i(\pi_i) = 1$, *и если для простого элемента* $p \in \mathfrak{o}$ *в кольце* $\mathfrak{O}$ *мы имеем разложение*

$$p = \varepsilon \pi_1^{e_1} \ldots \pi_m^{e_m} \qquad (\varepsilon \text{ — единица в } \mathfrak{O}), \tag{7}$$

то e_i *является индексом ветвления* ν_i *относительно* ν_0 (*и, следовательно,* $e_i > 0$).

Доказательство. Первое утверждение теоремы непосредственно вытекает из теоремы 6 и следствия теоремы 3. Докажем второе равенство. Пусть a — произвольный элемент из k^*. Если $\nu_0(a) = s$, то $a = p^s u$, где u — единица кольца $\mathfrak{o}$, а значит, и кольца $\mathfrak{O}$. Из равенства

$$a = \varepsilon u \pi_1^{se_1} \ldots \pi_m^{se_m} \tag{8}$$

следует теперь, что

$$\nu_i(a) = e_i \nu_0(a), \qquad a \in k^*, \tag{9}$$

а это и требовалось доказать.

Теорема 7 подсказывает нам, как можно доказать существование продолжений показателя ν_0 на поле K: достаточно для этого убедиться, что в целом замыкании $\mathfrak{O}$ кольца $\mathfrak{o}$ в поле K имеет место однозначность разложения на простые множители. В самом деле, пусть нам известно, что в $\mathfrak{O}$ разложение на простые множители однозначно и число неассоциированных простых элементов конечно. В силу теоремы 6 § 3 это равносильно тому, что в $\mathfrak{O}$ существует теория дивизоров с конечным числом простых главных дивизоров $\mathfrak{p}_1 = (\pi_1), \ldots, \mathfrak{p}_m = (\pi_m)$. Обозначим через $\nu_1, \ldots, \nu_m$ показатели поля K, соответствующие этим простым дивизорам. Простой элемент $p \in \mathfrak{o}$ в кольце $\mathfrak{O}$ имеет разложение вида (7) с неотрицательными показателями e_i. Следовательно, произвольный элемент $a = p^s u$ из k^* ($s = \nu_0(a)$) в кольце $\mathfrak{O}$ имеет разложение вида (8), из которого для каждого $i = 1, \ldots, m$ следует формула (9). Если бы $e_i = 0$, то все значения показателя ν_i на k^* были бы равны нулю, а это, как мы видели в начале пункта, невозможно. Значит, $e_i > 0$. Формула (9) означает, стало быть, что все показатели $\nu_1, \ldots, \nu_m$ являются продолжениями показателя ν_0 на поле K.

4. Существование продолжений. Пусть, как и прежде, k — произвольное поле, v_0 — некоторый его показатель, $\mathfrak{o}$ — кольцо показателя v_0 и p — простой элемент кольца $\mathfrak{o}$. Через Σ_0 обозначим поле вычетов показателя v_0. Для каждого элемента $a \in \mathfrak{o}$ соответствующий ему класс вычетов по модулю p будет обозначаться через $\bar{a}$. Равенство $\bar{a} = \bar{b}$ в поле Σ_0 имеет место, следовательно, тогда и только тогда, когда $a \equiv b \pmod{p}$ в кольце $\mathfrak{o}$.

Рассмотрим теперь произвольное конечное расширение K поля k и через $\mathfrak{O}$ обозначим целое замыкание кольца $\mathfrak{o}$ в поле K.

Лемма 2. *Если число элементов в поле вычетов Σ_0 показателя v_0 не меньше степени расширения K/k (в частности, если поле Σ_0 бесконечно), то кольцо $\mathfrak{O}$ евклидово и, следовательно, в нем имеет место однозначность разложения на простые множители. В кольце $\mathfrak{O}$ имеется только конечное число попарно не ассоциированных простых элементов.*

Доказательство. Определим на элементах $\alpha \in K^*$ функцию $\|\alpha\|$, полагая

$$\|\alpha\| = 2^{v_0(N_{K/k}\alpha)}.$$

Ясно, что введенная функция обладает свойством $\|\alpha\beta\| = \|\alpha\| \cdot \|\beta\|$ ($\alpha, \beta \in K^*$). Кроме того, $\|\alpha\|$ принимает, очевидно, натуральные значения при всех $\alpha \in \mathfrak{O}^*$. Мы должны доказать, что для любой пары элементов α и $\beta \neq 0$ из $\mathfrak{O}$ существуют такие $\xi \in \mathfrak{O}$ и $\rho \in \mathfrak{O}$, что

$$\alpha = \beta\xi + \rho, \tag{10}$$

где ρ либо равно нулю, либо удовлетворяет неравенству $\|\rho\| < \|\beta\|$.

Если в кольце $\mathfrak{O}$ элемент α делится на β, т. е. $\alpha = \beta\gamma$, где $\gamma \in \mathfrak{O}$, то равенство (10) будет соблюдаться при $\xi = \gamma$, $\rho = 0$. Предположим, что α не делится на β, т. е. что элемент $\gamma = \alpha\beta^{-1}$ не принадлежит $\mathfrak{O}$. Пусть $f(t) = t^n + c_1 t^{n-1} + \ldots + c_n$ ($c_i \in k$) — характеристический многочлен элемента γ относительно расширения K/k. Так как $\gamma \notin \mathfrak{O}$, то не все коэффициенты c_i принадлежат $\mathfrak{o}$. Если $\min\limits_{1 \leqslant i \leqslant n} v_0(c_i) = -r < 0$, то все коэффициенты многочлена $\varphi(t) = p^r f(t)$ будут принадлежать кольцу $\mathfrak{o}$, причем хоть один из них будет единицей в $\mathfrak{o}$. Заменим все коэффициенты $\varphi(t)$ соответствующими классами вычетов по модулю p. Так как старший коэффициент $\varphi(t)$, равный p^r, делится на p, то мы получим многочлен $\bar{\varphi}(t)$ из кольца $\Sigma_0[t]$ степени $\leqslant n-1$, причем не все его коэффициенты нули. По предположению поле Σ_0 содержит по крайней мере n элементов, поэтому существует элемент $a \in \mathfrak{o}$, для которого класс вычетов $\bar{a}$ не является корнем $\bar{\varphi}(t)$. Последнее означает, что $\varphi(a) \not\equiv 0 \pmod{p}$, т. е. что $\varphi(a)$ — единица кольца $\mathfrak{o}$. Подсчитаем теперь значение $\|\gamma - a\|$. Характеристический

многочлен для $\gamma - a$ равен $f(t+a)$, поэтому

$$N_{K/k}(\gamma - a) = (-1)^n f(a) = (-1)^n \varphi(a) p^{-r},$$

откуда

$$\|\gamma - a\| = 2^{-r} < 1, \qquad \|\alpha - a\beta\| < \|\beta\|.$$

Равенство (10) будет удовлетворено, если мы положим $\xi = a$, $\rho = \alpha - a\beta$.

Мы доказали таким образом, что $\mathfrak{O}$ является евклидовым кольцом, а значит, согласно теореме 2 § 2 разложение на простые множители в нем однозначно.

Пусть π — произвольный простой элемент кольца $\mathfrak{O}$. Так как для всякого $\alpha \in \mathfrak{O}^*$ его норма $N_{K/k}(\alpha)$ всегда делится на α, то $N_{K/k}(\pi) = p^f u$ делится на π (u — единица в $\mathfrak{o}$, $f \geqslant 1$). Но в таком случае в силу простоты π и в силу однозначности разложения на простые множители элемент p также должен делиться на π. Этим доказано, что если разложение p в кольце $\mathfrak{O}$ на простые множители имеет вид

$$p = \varepsilon \pi_1^{e_1} \dots \pi_m^{e_m}$$

(ε — единица в $\mathfrak{O}$), то простые элементы $\pi_1, \dots, \pi_m$ исчерпывают собой с точностью до ассоциированности все простые элементы кольца $\mathfrak{O}$.

Доказательство леммы 2 окончено.

Доказательство теоремы 5. Будем доказывать теорему индукцией по степени n расширения K/k. При $n = 1$ доказывать нечего. Пусть $n > 1$, и пусть теорема 5 уже доказана для всех расширений степени $< n$ при произвольном основном поле.

Если поле вычетов Σ_0 показателя ν_0 содержит не менее n элементов, то по лемме 2 в кольце $\mathfrak{O}$ разложение на простые множители однозначно и, следовательно, теорема 5 справедлива согласно сказанному в конце п. 3.

Мы должны рассмотреть, таким образом, лишь тот случай, когда число элементов q поля вычетов Σ_0 конечно и меньше n. Этот случай мы сведем к уже разобранному, расширив основное поле k до поля k' так, чтобы, во-первых, степень $(k' : k)$ была равна $n - 1$ (в силу индуктивного предположения в поле k' будет, следовательно, существовать показатель ν_0', являющийся продолжением ν_0) и, во-вторых, чтобы поле вычетов Σ' показателя ν_0' уже содержало не менее n элементов. Если через K' мы обозначим наименьшее поле, содержащее K и k', то для расширения K'/k' и показателя ν_0' будет выполнено условие леммы 2, т. е. будем иметь уже разобранный случай. Намеченный план осуществляется следующим образом.

Мы знаем (см. Дополнение, § 3), что над всяким конечным полем существуют неприводимые многочлены произвольной сте-

пени. Пусть $\bar{\varphi}(t)$ — неприводимый многочлен степени $n-1$ с коэффициентами из поля Σ_0, старший коэффициент которого равен $\bar{1}$. Каждый из его коэффициентов является классом вычетов кольца $\mathfrak{o}$ по модулю p. Заменим эти классы какими-нибудь их вычетами по модулю p (в качестве старшего коэффициента возьмем 1), мы получим многочлен $\varphi(t)$ из кольца $\mathfrak{o}[t]$, который будет неприводим над полем k. Действительно, если бы $\varphi(t)$ был приводим в поле k, то его можно было бы разложить на множители с коэффициентами из $\mathfrak{o}$, а тогда, переходя к полю вычетов Σ_0, мы получили бы для $\bar{\varphi}(t)$ разложение с коэффициентами из Σ_0, что противоречит выбору $\bar{\varphi}(t)$. Построим над полем K расширение $K'=K(\theta)$, где θ — корень многочлена $\varphi(t)$. Степень расширения K'/K, во всяком случае, не превосходит $n-1$ (над полем K многочлен $\varphi(t)$ может оказаться приводимым). Рассмотрим в K' промежуточное поле $k'=k(\theta)$. Так как $\varphi(t)$ неприводим над k, то $(k':k)=n-1$. Пусть ν_0' — какой-нибудь показатель поля k', являющийся продолжением ν_0 на k' (существование ν_0' обеспечено индуктивным предположением). Обозначим через $\mathfrak{o}'$ кольцо показателя ν_0', через p' — простой элемент в $\mathfrak{o}'$ и через Σ' — поле вычетов кольца $\mathfrak{o}'$ по модулю p'. Два элемента a и b из $\mathfrak{o}$ сравнимы по модулю p' (в кольце $\mathfrak{o}'$) тогда и только тогда, когда они сравнимы в кольце $\mathfrak{o}$ по модулю p. В силу этого те классы вычетов кольца $\mathfrak{o}'$ по модулю p', которые содержат представителей из $\mathfrak{o}$, образуют подполе поля Σ', изоморфное Σ_0. Имея в виду этот естественный изоморфизм $\Sigma_0 \to \Sigma'$, можно считать, что $\Sigma_0 \subset \Sigma'$. Так как элемент θ является корнем многочлена с коэффициентами из $\mathfrak{o}$ и со старшим коэффициентом 1, то $\theta \in \mathfrak{o}'$ (в силу целозамкнутости $\mathfrak{o}'$). Обозначим через $\bar{\theta}$ соответствующий ему класс вычетов из Σ'. Равенство $\varphi(\theta)=0$ при переходе к классам вычетов по модулю p' дает нам $\bar{\varphi}(\bar{\theta})=\bar{0}$. Но $\bar{\varphi}(t)$ по выбору неприводим над полем Σ_0, а значит, степени $\bar{1}$, $\bar{\theta}$, ..., $\bar{\theta}^{n-2}$ линейно независимы над Σ_0. Отсюда легко следует, что поле Σ' (т. е. поле вычетов показателя ν_0') содержит по крайней мере q^{n-1} элементов (напомним, что q обозначает число элементов поля Σ_0). С другой стороны,

$$(K':k')=\frac{(K':K)\,(K:k)}{(k':k)}\leqslant\frac{(n-1)\,n}{n-1}=n.$$

Но при $q\geqslant 2$ и $n\geqslant 2$ справедливо неравенство $q^{n-1}\geqslant n$. Следовательно, число элементов в поле вычетов Σ' показателя ν_0' не меньше степени $(K':k')$. По доказанному для показателя ν_0' существует его продолжение ν' на поле K'. Так как ν' является продолжением ν_0 на поле K', то показатель ν, индуцированный показателем ν' на подполе K, будет продолжением показателя ν_0 (см. п. 3). Этим мы закончили доказательство теоремы 5.

Задачи

1. Показать, что для алгебраически замкнутых полей показателей не существует.

2. Пусть $K = k(x)$ — поле рациональных функций над полем k и ν — показатель поля K, соответствующий многочлену $x - a$ $(a \in k)$. Показать, что поле классов вычетов Σ_ν показателя ν изоморфно k. Показать, далее, что два элемента $f(x)$ и $g(x)$ из кольца показателя ν тогда и только тогда лежат в одном классе вычетов, когда $f(a) = g(a)$.

3. Пусть $K = k(x)$ — поле рациональных функций над полем вещественных чисел k и ν — показатель K, соответствующий неприводимому многочлену $x^2 + 1$. Найти поле классов вычетов Σ_ν показателя ν.

4. Пусть $\mathfrak{O}_1$ и $\mathfrak{O}_2$ — кольца показателей ν_1 и ν_2 некоторого поля K, E_1 и E_2 — группы единиц этих колец. Доказать, что если $E_1 \subset E_2$, то $\nu_1 = \nu_2$. Пусть, далее, ν, ν_1, ..., ν_m — показатели поля K и $\mathfrak{O}$, $\mathfrak{O}_1$, ..., $\mathfrak{O}_m$ — их кольца. Доказать, что если $\bigcap_{i=1}^{m} \mathfrak{O}_i \subset \mathfrak{O}$, то ν совпадает с одним из $\nu_1, \ldots, \nu_m$.

5. Найти целое замыкание кольца 3-целых чисел в поле $\mathbb{Q}(\sqrt{-5})$ и определить все продолжения 3-адического показателя ν_3 на это поле.

6. Найти для любого простого числа p все продолжения p-адического показателя ν_p на поле $\mathbb{Q}(\sqrt{-1})$ и определить соответствующие индексы ветвления.

7. Пусть K/k — нормальное расширение и ν_0 — показатель поля k. Показать, что если ν — какое-нибудь продолжение ν_0 на поле K, то все прочие продолжения имеют вид $\nu^\sigma(\alpha) = \nu(\sigma(\alpha))$, $\alpha \in K$, где σ пробегает все автоморфизмы K/k.

8. Пусть $\mathfrak{O}_1$, ..., $\mathfrak{O}_m$ — кольца показателей ν_1, ..., ν_m некоторого поля. Доказать, что в кольце $\bigcap_{i=1}^{m} \mathfrak{O}_i$ все идеалы главные.

9. Пусть $k = k_0(x, y)$ — поле рациональных функций от x и y над некоторым полем k_0. Выберем в поле формальных степенных рядов $k_0\{t\}$ (см. задачу 7 § 4 гл. I или п. 5 § 1 гл. IV) ряд

$$\xi(t) = \sum_{n=0}^{\infty} c_n t^n \quad (c_n \in k_0),$$

трансцендентный над полем рациональных функций $k_0(t)$ (существование таких рядов следует из того, что мощность поля $k_0\{t\}$ больше мощности подполя $k_0(t)$ и, следовательно, больше мощности множества тех элементов из $k_0\{t\}$, которые алгебраичны над $k_0(t)$). Для отличного от нуля многочлена $f = f(x, y) \in k_0[x, y]$ ряд $f(t, \xi(t))$ по выбору ξ также отличен от нуля. Если t^n есть наименьшая степень t, входящая в этот ряд с ненулевым коэффициентом, то полагаем $\nu_0(f) = n$. Показать, что функция ν_0 (при надлежащем доопределении) является показателем поля k и что поле вычетов этого показателя изоморфно полю k_0.

§ 5. Теория дивизоров для конечного расширения

1. Существование. Теорема 1. *Если для кольца $\mathfrak{o}$ с полем отношений k имеется теория дивизоров $\mathfrak{o}^* \to \mathfrak{D}_0$, определяемая набором показателей $\mathfrak{N}_0$, и если K — конечное расширение поля k, то совокупность $\mathfrak{N}$ всех тех показателей поля K, которые являются продолжениями показателей из $\mathfrak{N}_0$, определяет теорию дивизоров для целого замыкания $\mathfrak{O}$ кольца $\mathfrak{o}$ в поле K.*

Доказательство. В силу теоремы 4 § 3 нам достаточно лишь проверить, что множество показателей $\mathfrak{N}$ удовлетворяет всем трем условиям этой теоремы. Проверим сначала второе условие. Для всякого показателя $\nu \in \mathfrak{N}$ и любого $a \in \mathfrak{o}$ мы, очевидно, имеем $\nu(a) \geqslant 0$. Это значит, что $\mathfrak{o}$ содержится в кольце показателя ν. Но тогда по теореме 1 § 4 целое замыкание кольца $\mathfrak{o}$ в поле K также содержится в кольце показателя ν. Другими словами, $\nu(\alpha) \geqslant 0$ для всех $\alpha \in \mathfrak{D}$. Обратно, пусть для некоторого элемента $\alpha \in K$ неравенство $\nu(\alpha) \geqslant 0$ выполнено для всех показателей $\nu \in \mathfrak{N}$. Обозначим через $t^r + a_1 t^{r-1} + \ldots + a_r$ минимальный многочлен α относительно k. Пусть ν_0 — произвольный показатель поля k, принадлежащий множеству $\mathfrak{N}_0$, и $\nu_1, \ldots, \nu_m$ — все его продолжения на поле K. Так как $\nu_1(\alpha) \geqslant 0, \ldots, \nu_m(\alpha) \geqslant 0$, то согласно теореме 6 § 4 элемент α принадлежит целому замыканию в K кольца показателя ν_0. Но в таком случае все коэффициенты $a_1, \ldots, a_r$ должны принадлежать самому кольцу показателя ν_0 (см. Дополнение, § 4, п. 3), т. е. $\nu_0(a_1) \geqslant 0, \ldots, \nu_0(a_r) \geqslant 0$. Поскольку последнее справедливо для всех $\nu_0 \in \mathfrak{N}_0$, то коэффициенты $a_1, \ldots, a_r$ принадлежат $\mathfrak{o}$, а значит, $\alpha \in \mathfrak{D}$.

Обратимся к первому условию. Пусть $\alpha \in \mathfrak{D}$, $\alpha \neq 0$. Среди показателей ν_0 из $\mathfrak{N}_0$ имеется только конечное число таких, что $\nu_0(a_r) \neq 0$. Отсюда следует, что в $\mathfrak{N}$ также имеется только конечное число показателей ν, для которых $\nu(a_r) \neq 0$. Но если $\nu(a_r) = 0$, то помимо неравенства $\nu(\alpha) \geqslant 0$ мы имеем также $\nu(\alpha^{-1}) = \nu\left(a_r^{-1}(\alpha^{r-1} + \ldots + a_{r-1})\right) \geqslant 0$, а значит, $\nu(\alpha) = 0$. Таким образом, $\nu(\alpha) = 0$ почти для всех $\nu \in \mathfrak{N}$.

Остается проверить выполнение третьего условия. Пусть $\nu_1, \ldots, \nu_m$ — различные показатели из $\mathfrak{N}$ и $k_1, \ldots, k_m$ — неотрицательные целые числа. Обозначим через $\nu_{01}, \ldots, \nu_{0m}$ соответствующие показатели из $\mathfrak{N}_0$ (среди ν_{0i} могут, конечно, оказаться равные). Дополним нашу исходную систему показателей *до* системы $\nu_1, \ldots, \nu_m, \nu_{m+1}, \ldots, \nu_s$, содержащей все продолжения ν_{0i} на поле K. По теореме 3 § 4 в поле K существует элемент γ, для которого

$$\nu_1(\gamma) = k_1, \ \ldots, \ \nu_m(\gamma) = k_m, \ \nu_{m+1}(\gamma) = 0, \ \ldots, \ \nu_s(\gamma) = 0.$$

Если этот элемент γ принадлежит кольцу $\mathfrak{D}$, то мы положим $\alpha = \gamma$. Допустим, что γ не принадлежит $\mathfrak{D}$. Обозначим в таком случае через $\nu_1', \ldots, \nu_r'$ все те показатели из $\mathfrak{N}$, которые на элементе γ принимают отрицательные значения:

$$\nu_1'(\gamma) = -l_1, \ \ldots, \ \nu_r'(\gamma) = -l_r,$$

и через $\nu_{01}', \ldots, \nu_{0r}'$ — соответствующие им показатели из $\mathfrak{N}_0$ (среди ν_{0j}' также могут быть равные). Так как каждый из показателей ν_{0j}' отличен от каждого из ν_{0i}, то в $\mathfrak{o}$ найдется такой

элемент a, что

$$v_{0i}(a) = 0, \quad 1 \leqslant i \leqslant m, \qquad v'_{0j}(a) = l, \quad 1 \leqslant j \leqslant r,$$

где l мы возмем равным $\max(l_1, \ldots, l_r)$. Положим $\alpha = \gamma a$. Так как

$$v'_j(\alpha) = v'_j(\gamma) + v'_j(a) \geqslant -l_j + v'_{0j}(a) = -l_j + l \geqslant 0,$$

то $\alpha \in \mathfrak{O}$. Таким образом, в обоих случаях в кольце $\mathfrak{O}$ мы нашли элемент α с условием $v_1(\alpha) = k_1, \ldots, v_m(\alpha) = k_m$, так что условие 3) теоремы 4 § 3 для множества показателей $\mathfrak{N}$ также выполнено. Доказательство теоремы 1 окончено.

Применим теорему 1 к случаю поля алгебраических чисел.

Максимальный порядок $\mathfrak{O}$ поля алгебраических чисел K является, как мы знаем, целым замыканием в K кольца целых рациональных чисел $\mathbb{Z}$. Так как в $\mathbb{Z}$ теория дивизоров имеется (однозначность разложения на простые множители), то по теореме 1 теория дивизоров существует и для $\mathfrak{O}$. Согласно теореме 5 § 3 теория дивизоров для $\mathbb{Z}$ связана с совокупностью всех показателей поля рациональных чисел $\mathbb{Q}$, а так как каждый показатель поля K является продолжением некоторого показателя поля $\mathbb{Q}$, то получаем, что теория дивизоров кольца $\mathfrak{O}$ определяется всеми показателями поля K. Мы имеем, таким образом, следующую теорему.

Теорема 2. *Для максимального порядка $\mathfrak{O}$ произвольного поля алгебраических чисел K существует теория дивизоров $\mathfrak{O}^* \to \mathfrak{D}$, и эта теория определяется совокупностью всех показателей поля K.*

2. Норма дивизоров. Пусть k — поле отношений кольца $\mathfrak{o}$ с теорией дивизоров $\mathfrak{o}^* \to \mathfrak{D}_0$, K — конечное расширение поля k, $\mathfrak{O}$ — целое замыкание кольца $\mathfrak{o}$ в поле K и $\mathfrak{O}^* \to \mathfrak{D}$ — теория дивизоров для кольца $\mathfrak{O}$. В этом пункте нами будут установлены некоторые связи между полугруппами дивизоров $\mathfrak{D}_0$ и $\mathfrak{D}$.

Так как $\mathfrak{o} \subset \mathfrak{O}$, то элементам из $\mathfrak{o}^*$ соответствуют главные дивизоры как в полугруппе $\mathfrak{D}_0$, так и в полугруппе $\mathfrak{D}$. Чтобы различать их, мы условимся здесь главный дивизор из $\mathfrak{D}_0$, соответствующий элементу $a \in \mathfrak{o}^*$, обозначать через $(a)_k$, а главный дивизор из $\mathfrak{D}$, соответствующий элементу $\alpha \in \mathfrak{O}^*$,— через $(\alpha)_K$.

Для полугрупп $\mathfrak{o}^*$ и $\mathfrak{O}^*$ мы имеем изоморфное вложение $\mathfrak{o}^* \to \mathfrak{O}^*$. Так как единицы кольца $\mathfrak{O}$, содержащиеся в $\mathfrak{o}$, совпадают с единицами кольца $\mathfrak{o}$, то это вложение определяет изоморфизм $(a)_k \to (a)_K$, $a \in \mathfrak{o}^*$, полугруппы главных дивизоров кольца $\mathfrak{o}$ в полугруппу главных дивизоров кольца $\mathfrak{O}$. Мы покажем сейчас, что этот изоморфизм можно продолжить до изоморфизма $\mathfrak{D}_0 \to \mathfrak{D}$.

Теорема 3. *Для полугруппы $\mathfrak{D}_0$ существует изоморфизм в полугруппу $\mathfrak{D}$, который на главных дивизорах совпадает с изоморфизмом $(a)_k \to (a)_K$, $a \in \mathfrak{o}^*$.*

Изоморфизм $\mathfrak{D}_0 \to \mathfrak{D}$ характеризуется, очевидно, коммутативностью диаграммы

$$\begin{array}{ccc} \mathfrak{o}^* & \to & \mathfrak{D}^* \\ \downarrow & & \downarrow \\ \mathfrak{D}_0 & \to & \mathfrak{D} \end{array}$$

т. е. тем, что два «сквозных» гомоморфизма $\mathfrak{o}^* \to \mathfrak{D}^* \to \mathfrak{D}$ и $\mathfrak{o}^* \to \mathfrak{D}_0 \to \mathfrak{D}$ совпадают (вертикальные гомоморфизмы обозначают отображения мультипликативных полугрупп колец на полугруппы главных дивизоров).

Пусть $\mathfrak{p}$ — произвольный простой дивизор кольца $\mathfrak{o}$, $\nu_\mathfrak{p}$ — соответствующий ему показатель поля k и $\nu_{\mathfrak{P}_1}, \ldots, \nu_{\mathfrak{P}_m}$ — все продолжения $\nu_\mathfrak{p}$ на поле K ($\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ — простые дивизоры кольца $\mathfrak{D}$). Обозначим через $e_1, \ldots, e_m$ соответственно индексы ветвления показателей $\nu_{\mathfrak{P}_1}, \ldots, \nu_{\mathfrak{P}_m}$ относительно $\nu_\mathfrak{p}$. Так как $\nu_{\mathfrak{P}_i}(a) = e_i \nu_\mathfrak{p}(a)$ при любом $a \in \mathfrak{o}^*$, то множителю $\mathfrak{p}^{\nu_\mathfrak{p}(a)}$ из главного дивизора $(a)_k \in \mathfrak{D}_0$ в главном дивизоре $(a)_K \in \mathfrak{D}$ будет соответствовать произведение $(\mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_m^{e_m})^{\nu_\mathfrak{p}(a)}$. Это показывает, что изоморфизм $\mathfrak{D}_0$ в $\mathfrak{D}$, определяемый отображением

$$\mathfrak{p} \to \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_m^{e_m} \tag{1}$$

(для всех $\mathfrak{p}$), удовлетворяет условию теоремы 3.

Нетрудно доказать, что изоморфизм $\mathfrak{D}_0 \to \mathfrak{D}$, удовлетворяющий требованиям теоремы 3, единственный (задача 5).

В силу изоморфизма $\mathfrak{D}_0 \to \mathfrak{D}$ мы можем полугруппу $\mathfrak{D}_0$ отождествить с ее образом в полугруппе $\mathfrak{D}$. При таком отождествлении простые дивизоры из $\mathfrak{D}_0$ перестают, вообще говоря, быть простыми в $\mathfrak{D}$. Именно, ввиду (1) для каждого простого $\mathfrak{p} \in \mathfrak{D}_0$ в полугруппе $\mathfrak{D}$ имеет место разложение

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_m^{e_m}. \tag{2}$$

Пользуясь вложением $\mathfrak{D}_0 \to \mathfrak{D}$, можно говорить о делимости дивизоров кольца $\mathfrak{o}$ на дивизоры кольца $\mathfrak{D}$. В частности, ввиду (2) получаем, что простые дивизоры $\mathfrak{P}$ кольца $\mathfrak{D}$, делящие простой дивизор $\mathfrak{p}$ кольца $\mathfrak{o}$, характеризуются тем, что соответствующие им показатели $\nu_\mathfrak{P}$ являются продолжениями показателя $\nu_\mathfrak{p}$. Очевидно, далее, что взаимно простые дивизоры из $\mathfrak{D}_0$ остаются взаимно простыми и в $\mathfrak{D}$.

Определение. *Пусть* $\mathfrak{P} | \mathfrak{p}$. *Индекс ветвления* $e = e_\mathfrak{P}$ *показателя* $\nu_\mathfrak{P}$ *относительно показателя* $\nu_\mathfrak{p}$ *называется также индексом ветвления простого дивизора* $\mathfrak{P}$ *относительно* $\mathfrak{p}$ (*или относительно* k).

Индекс ветвления является, таким образом, наибольшим натуральным числом e, для которого $\mathfrak{P}^e \mid \mathfrak{p}$.

Для всякого элемента $\alpha \in \mathfrak{O}^*$ его норма $N(\alpha) = N_{K/k}(\alpha)$ принадлежит $\mathfrak{o}^*$. Отображение $\alpha \to N(\alpha)$, $\alpha \in \mathfrak{O}^*$, является поэтому гомоморфизмом мультипликативной полугруппы $\mathfrak{O}^*$ в полугруппу $\mathfrak{o}^*$. Так как норма всякой единицы кольца $\mathfrak{O}$ является единицей в $\mathfrak{o}$, то этот гомоморфизм однозначно определяет гомоморфизм $(\alpha)_K \to (N(\alpha))_k$ полугруппы главных дивизоров кольца $\mathfrak{O}$ в полугруппу главных дивизоров кольца $\mathfrak{o}$. Покажем, что этот гомоморфизм можно продолжить до гомоморфизма всей полугруппы $\mathfrak{D}$ в $\mathfrak{D}_0$.

Теорема 4. *Для полугрупп дивизоров $\mathfrak{D}$ и $\mathfrak{D}_0$ существует гомоморфизм N: $\mathfrak{D} \to \mathfrak{D}_0$, для которого*

$$N((\alpha)_K) = (N_{K/k}(\alpha))_k \tag{3}$$

при любом $\alpha \in \mathfrak{O}^*$.

Свойство гомоморфизма N, выраженное равенством (3), означает, что для гомоморфизмов диаграммы

$$\begin{array}{ccc} \mathfrak{O}^* & \xrightarrow{N} & \mathfrak{o}^* \\ \downarrow & & \downarrow \\ \mathfrak{D} & \xrightarrow{N} & \mathfrak{D}_0 \end{array}$$

имеет место коммутативный закон.

Для фиксированного простого дивизора $\mathfrak{p} \in \mathfrak{D}_0$ через $\mathfrak{o}_\mathfrak{p}$ мы обозначим кольцо показателя $\nu_\mathfrak{p}$ и через $\mathfrak{O}_\mathfrak{p}$ — его целое замыкание в поле K. Согласно теореме 7 § 4 все простые дивизоры $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ кольца $\mathfrak{O}$, делящие $\mathfrak{p}$, находятся во взаимно однозначном соответствии с попарно не ассоциированными простыми элементами $\pi_1, \ldots, \pi_m$ кольца $\mathfrak{O}_\mathfrak{p}$. Это соответствие $\mathfrak{P}_i \leftrightarrow \pi_i$ обладает тем свойством, что если для элемента $\alpha \neq 0$ из K имеет место разложение

$$\alpha = \varepsilon \pi_1^{k_1} \ldots \pi_m^{k_m}, \tag{4}$$

где ε — единица кольца $\mathfrak{O}_\mathfrak{p}$, то

$$k_i = \nu_{\mathfrak{P}_i}(\alpha). \tag{5}$$

Пусть $\mathfrak{P}$ — один из простых дивизоров $\mathfrak{P}_i$, делящих $\mathfrak{p}$, и π — соответствующий ему простой элемент кольца $\mathfrak{O}_\mathfrak{p}$. Положим

$$d_\mathfrak{P} = \nu_\mathfrak{p}(N_{K/k}(\pi)). \tag{6}$$

Ясно, что $d_\mathfrak{P}$ не зависит от выбора π. Переходя в равенстве (4)

к нормам и учитывая (5) и (6), мы получаем соотношение

$$v_{\mathfrak{p}}(N_{K/k}(\alpha)) = \sum_{\mathfrak{P}/\mathfrak{p}} d_{\mathfrak{P}} v_{\mathfrak{P}}(\alpha) \tag{7}$$

($\mathfrak{P}$ пробегает все простые дивизоры кольца $\mathfrak{D}$, делящие $\mathfrak{p}$).

Теперь мы уже легко можем построить гомоморфизм N: $\mathfrak{D} \to \mathfrak{D}_0$, о котором говорится в теореме 4.

Каждый дивизор $\mathfrak{A} = \mathfrak{P}_1^{A_1} \dots \mathfrak{P}_r^{A_r}$ из полугруппы $\mathfrak{D}$ удобно записывать в виде формально бесконечного произведения:

$$\mathfrak{A} = \prod_{\mathfrak{P}} \mathfrak{P}^{A(\mathfrak{P})},$$

распространенного по всем простым дивизорам $\mathfrak{P}$ из $\mathfrak{D}$, в котором, однако, только конечное число неотрицательных показателей $A(\mathfrak{P})$ отлично от нуля ($A(\mathfrak{P})$ равно A_i, если $\mathfrak{P} = \mathfrak{P}_i$, и равно нулю, если дивизор $\mathfrak{P}$ отличен от $\mathfrak{P}_1, \dots, \mathfrak{P}_r$). Аналогичным образом мы можем записывать и дивизоры кольца $\mathfrak{o}$.

Рассмотрим для элемента $\alpha \in \mathfrak{D}^*$ главный дивизор $(\alpha)_K$. Так как простой дивизор $\mathfrak{P}$ входит в $(\alpha)_K$ с показателем $v_{\mathfrak{P}}(\alpha)$, то

$$(\alpha)_K = \prod_{\mathfrak{P}} \mathfrak{P}^{v_{\mathfrak{P}}(\alpha)}. \tag{8}$$

Согласно соотношению (7) для показателей $c(\mathfrak{p})$ главного дивизора

$$(N(\alpha))_k = \prod_{\mathfrak{p}} \mathfrak{p}^{c(\mathfrak{p})} \tag{9}$$

мы имеем формулу

$$c(\mathfrak{p}) = \sum_{\mathfrak{P}/\mathfrak{p}} d_{\mathfrak{P}} v_{\mathfrak{P}}(\alpha). \tag{10}$$

Это подсказывает нам следующее определение.

Определение. *Пусть* $\mathfrak{A} = \prod_{\mathfrak{P}} \mathfrak{P}^{A(\mathfrak{P})}$ — *дивизор кольца* $\mathfrak{D}$. *Для каждого простого дивизора* $\mathfrak{p}$ *кольца* $\mathfrak{o}$ *положим*

$$a(\mathfrak{p}) = \sum_{\mathfrak{P}/\mathfrak{p}} d_{\mathfrak{P}} A(\mathfrak{P}).$$

Дивизор $\prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$ *кольца* $\mathfrak{o}$ *называется нормой дивизора* $\mathfrak{A}$ *относительно расширения* K/k *и обозначается через* $N_{K/k}(\mathfrak{A})$ *или, короче, через* $N(\mathfrak{A})$.

Так как числа $A(\mathfrak{P})$ равны нулю почти для всех $\mathfrak{P}$ (т. е. для всех, за исключением конечного числа), то $a(\mathfrak{p})$ также равны нулю почти для всех $\mathfrak{p}$, и, значит, выражение $\prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$ действительно является дивизором кольца $\mathfrak{o}$.

Из определения очевидным образом следует, что

$$N(\mathfrak{AB}) = N(\mathfrak{A})N(\mathfrak{B})$$

для любых двух дивизоров $\mathfrak{A}$ и $\mathfrak{B}$ из $\mathfrak{D}$. Отображение $\mathfrak{A} \to N(\mathfrak{A})$ является, таким образом, гомоморфизмом полугруппы $\mathfrak{D}$ в полугруппу $\mathfrak{D}_0$.

В случае простого дивизора $\mathfrak{A} = \mathfrak{P}$ мы, очевидно, имеем

$$N(\mathfrak{P}) = \mathfrak{p}^{d_{\mathfrak{P}}} \qquad (\mathfrak{P} \mid \mathfrak{p}). \tag{11}$$

Так как ввиду равенства (10) норма дивизора (8) равна дивизору (9), то нами, следовательно, и доказано существование гомоморфизма $N\colon \mathfrak{D} \to \mathfrak{D}_0$, удовлетворяющего условию (3).

Как и в случае изоморфизма $\mathfrak{D}_0 \to \mathfrak{D}$, можно показать (задача 4), что гомоморфизм $N\colon \mathfrak{D} \to \mathfrak{D}_0$ условием (3) определен однозначно.

Одной из центральных задач теории дивизоров является установление законов разложения простых дивизоров $\mathfrak{p}$ кольца $\mathfrak{o}$ на простые множители при переходе к целому замыканию $\mathfrak{O}$ кольца $\mathfrak{o}$ в конечном расширении. В общем случае, однако, об этих законах разложения к настоящему времени известно совсем немного (см. по этому поводу конец п. 2 § 8). Каждое разложение вида (2) характеризуется числом m простых делителей $\mathfrak{P}_i$ и набором их индексов ветвления $e_i = e_{\mathfrak{P}_i}$. Натуральные числа $e_{\mathfrak{P}}$, оказывается, не могут быть произвольными (для данного расширения K/k). Именно, они связаны с числами $d_{\mathfrak{P}}$ (см. (6)) соотношением

$$\sum_{\mathfrak{P} \mid \mathfrak{p}} d_{\mathfrak{P}} e_{\mathfrak{P}} = n = (K : k), \tag{12}$$

для доказательства которого достаточно формулу (7) применить к простому элементу p кольца $\mathfrak{o}_{\mathfrak{p}}$ (напомним, что $v_{\mathfrak{P}_i}(p) = e_i$).

3. Степень инерции. Определение гомоморфизма $N\colon \mathfrak{D} \to \mathfrak{D}_0$ опиралось на числа $d_{\mathfrak{P}}$, которые, довольно формальным образом, определялись формулой (6). Теперь мы выясним более глубокий арифметический смысл этих чисел.

Пусть $\mathfrak{P} \mid \mathfrak{p}$. Обозначим через $\mathfrak{o}_{\mathfrak{p}}$ и $\mathfrak{O}_{\mathfrak{P}}$ кольца показателей $v_{\mathfrak{p}}$ и $v_{\mathfrak{P}}$ и через p и π — простые элементы в этих кольцах соответственно. Так как для элементов a и b из $\mathfrak{o}_{\mathfrak{p}}$ сравнения $a \equiv b \pmod{p}$ в кольце $\mathfrak{o}_{\mathfrak{p}}$ и $a \equiv b \pmod{\pi}$ в кольце $\mathfrak{O}_{\mathfrak{P}}$ равносильны, то каждый класс вычетов в $\mathfrak{o}_{\mathfrak{p}}$ по модулю p содержится целиком в некотором классе вычетов в $\mathfrak{O}_{\mathfrak{P}}$ по модулю π. Это определяет изоморфное вложение поля вычетов $\Sigma_{\mathfrak{p}} = \mathfrak{o}_{\mathfrak{p}}/(p)$ показателя $v_{\mathfrak{p}}$ в поле вычетов $\Sigma_{\mathfrak{P}} = \mathfrak{O}_{\mathfrak{P}}/(\pi)$ показателя $v_{\mathfrak{P}}$. В силу этого изоморфизма мы будем считать, что $\Sigma_{\mathfrak{p}} \subset \Sigma_{\mathfrak{P}}$. Для

любого $\xi \in \mathfrak{O}_{\mathfrak{P}}$ через $\bar{\xi}$ обозначим класс вычетов по модулю π с представителем ξ. Подполе $\Sigma_{\mathfrak{p}}$ поля $\Sigma_{\mathfrak{P}}$ состоит, очевидно, из классов вычетов вида $\bar{a}$, где $a \in \mathfrak{o}_{\mathfrak{p}}$.

Пусть классы вычетов $\bar{\omega}_1, \ldots, \bar{\omega}_m$ из $\Sigma_{\mathfrak{P}}$ $(\omega_i \in \mathfrak{O}_{\mathfrak{P}})$ линейно независимы над полем $\Sigma_{\mathfrak{p}}$. Покажем, что тогда представители $\omega_1, \ldots, \omega_m$ из этих классов линейно независимых над полем k. Предположим, что это не так, т. е. что при некоторых коэффициентах $a_i \in k$, не равных одновременно нулю, имеет место равенство

$$a_1\omega_1 + \ldots + a_m\omega_m = 0.$$

Умножив это соотношение на надлежащую степень p, мы можем добиться того, чтобы все a_i принадлежали кольцу $\mathfrak{o}_{\mathfrak{p}}$ и чтобы хоть один из них не делился на p. Переходя тогда к полю вычетов $\Sigma_{\mathfrak{P}}$, мы придем к равенству

$$\bar{a}_1\bar{\omega}_1 + \ldots + \bar{a}_m\bar{\omega}_m = \bar{0},$$

в котором не все коэффициенты $\bar{a}_i \in \Sigma_{\mathfrak{p}}$ нули. Полученное противоречие и доказывает наше утверждение.

Из линейной независимости $\omega_1, \ldots, \omega_m$ над полем k следует, что $m \leqslant n = (K : k)$. Таким образом, *поле вычетов* $\Sigma_{\mathfrak{P}}$ *является конечным расширением поля* $\Sigma_{\mathfrak{p}}$, *при этом*

$$(\Sigma_{\mathfrak{P}} : \Sigma_{\mathfrak{p}}) \leqslant (K : k).$$

Определение. *Пусть простой дивизор* $\mathfrak{P}$ *кольца* $\mathfrak{O}$ *является делителем простого дивизора* $\mathfrak{p}$ *кольца* $\mathfrak{o}$. *Степень* $f = f_{\mathfrak{P}} = (\Sigma_{\mathfrak{P}} : \Sigma_{\mathfrak{p}})$ *поля вычетов показателя* $\nu_{\mathfrak{P}}$ *над полем вычетов показателя* $\nu_{\mathfrak{p}}$ *называется степенью инерции простого дивизора* $\mathfrak{P}$ *относительно* $\mathfrak{p}$ *(или относительно* k*).*

Обозначим, как и в п. 2, через $\mathfrak{O}_{\mathfrak{p}}$ целое замыкание кольца $\mathfrak{o}_{\mathfrak{p}}$ в поле K. По аналогии с понятием фундаментального базиса в полях алгебраических чисел введем следующее определение.

Определение. *Базис* $\omega_1, \ldots, \omega_n$ *расширения* K/k *будем называть фундаментальным базисом кольца* $\mathfrak{O}_{\mathfrak{p}}$ *относительно* $\mathfrak{o}_{\mathfrak{p}}$, *если все его элементы принадлежат* $\mathfrak{O}_{\mathfrak{p}}$ *и каждый элемент* $\alpha \in \mathfrak{O}_{\mathfrak{p}}$ *представляется в виде линейной комбинации*

$$\alpha = a_1\omega_1 + \ldots + a_n\omega_n \tag{13}$$

с коэффициентами a_i *из* $\mathfrak{o}_{\mathfrak{p}}$.

Ниже мы увидим, что в случае сепарабельного расширения K/k фундаментальный базис для кольца $\mathfrak{O}_{\mathfrak{p}}$ (при любом $\mathfrak{p}$) всегда существует. С другой стороны, согласно задачам 11 и 12 для

несепарабельных расширений K/k могут встретиться случаи, когда кольцо $\mathfrak{O}_\mathfrak{p}$ не имеет фундаментального базиса относительно $\mathfrak{o}_\mathfrak{p}$.

Значение понятия фундаментального базиса определяется следующей теоремой.

Теорема 5. *Пусть $\mathfrak{P}$ — простой дивизор кольца $\mathfrak{O}$, делящий $\mathfrak{p}$, и π — соответствующий ему простой элемент кольца $\mathfrak{O}_\mathfrak{p}$. Если для кольца $\mathfrak{O}_\mathfrak{p}$ существует фундаментальный базис относительно $\mathfrak{o}_\mathfrak{p}$, то $f_\mathfrak{P} = d_\mathfrak{P} = v_\mathfrak{p}(N_{K/k}(\pi))$.*

Доказательство. Простой элемент $\pi \in \mathfrak{O}_\mathfrak{p}$ является, очевидно, простым элементом и в кольце $\mathfrak{O}_\mathfrak{P}$. Покажем, что в каждом классе вычетов $\bar{\xi}$ кольца $\mathfrak{O}_\mathfrak{P}$ по модулю π содержится представитель из $\mathfrak{O}_\mathfrak{p}$, т. е. для любого $\xi \in \mathfrak{O}_\mathfrak{P}$ найдется такой элемент $\alpha \in \mathfrak{O}_\mathfrak{p}$, что

$$\xi \equiv \alpha \pmod{\pi}.$$

Пусть $\mathfrak{P} = \mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_m$ — все простые дивизоры кольца $\mathfrak{O}$, являющиеся делителями $\mathfrak{p}$. В силу теоремы 6 § 4 условие $\gamma \in \mathfrak{O}_\mathfrak{p}$ равносильно тому, что $v_{\mathfrak{P}_i}(\gamma) \geqslant 0$ при всех $i = 1, \ldots, m$. Искомый элемент α должен поэтому определяться условиями

$$v_\mathfrak{P}(\xi - \alpha) \geqslant 1, \qquad v_{\mathfrak{P}_i}(\alpha) \geqslant 0, \qquad i = 2, \ldots, m,$$

и для доказательства его существования нам достаточно сослаться на теорему 4 § 4.

Пусть теперь $\omega_1, \ldots, \omega_n$ — фундаментальный базис кольца $\mathfrak{O}_\mathfrak{p}$ относительно $\mathfrak{o}_\mathfrak{p}$. По доказанному каждый элемент из $\Sigma_\mathfrak{P}$ может быть представлен в виде $\bar{a}_1\bar{\omega}_1 + \ldots + \bar{a}_n\bar{\omega}_n$, где $a_i \in \mathfrak{o}_\mathfrak{p}$ и, следовательно, $\bar{a}_i \in \Sigma_\mathfrak{p}$. Это значит, что классы вычетов $\bar{\omega}_1, \ldots, \bar{\omega}_n$ являются образующими $\Sigma_\mathfrak{P}$ как линейного пространства над $\Sigma_\mathfrak{p}$. Если $f = (\Sigma_\mathfrak{P} : \Sigma_\mathfrak{p}) = f_\mathfrak{P}$, то среди них мы можем выбрать f линейно независимых над $\Sigma_\mathfrak{p}$. Пусть это будут $\bar{\omega}_1, \ldots, \bar{\omega}_f$. Ясно, что тогда в кольце $\mathfrak{O}_\mathfrak{p}$ сравнение

$$a_1\omega_1 + \ldots + a_f\omega_f \equiv 0 \pmod{\pi},$$

где $a_i \in \mathfrak{o}_\mathfrak{p}$, имеет место тогда и только тогда, когда $a_i \equiv 0 \pmod{p}$, где p — простой элемент кольца $\mathfrak{o}_\mathfrak{p}$.

Так как каждый класс вычетов $\bar{\omega}_j \in \Sigma_\mathfrak{P}$ при $j = f+1, \ldots, n$ выражается через $\bar{\omega}_1, \ldots, \bar{\omega}_f$, то

$$\omega_j \equiv \sum_{s=1}^{f} b_{js}\omega_s \pmod{\pi}, \qquad j = f+1, \ldots, n,$$

при некоторых b_{js} из $\mathfrak{o}_\mathfrak{p}$. Положим

$$\theta_i = \omega_i \quad \text{при} \quad i = 1, \ldots, f,$$

$$\theta_j = -\sum_{s=1}^{f} b_{js}\omega_s + \omega_j \quad \text{при} \quad j = f+1, \ldots, n.$$

Ясно, что $\theta_1, \ldots, \theta_n$ также образуют фундаментальный базис $\mathfrak{D}_\mathfrak{p}$ относительно $\mathfrak{o}_\mathfrak{p}$ (так как все ω_s могут быть выражены через θ_s с коэффициентами из $\mathfrak{o}_\mathfrak{p}$). Все элементы $\theta_{f+1}, \ldots, \theta_n$ делятся в кольце $\mathfrak{D}_\mathfrak{p}$ на π, поэтому сравнение

$$a_1\theta_1 + \ldots + a_n\theta_n \equiv 0 \pmod{\pi}$$

имеет место тогда и только тогда, когда

$$a_1 \equiv \ldots \equiv a_f \equiv 0 \pmod{p}.$$

Рассмотрим совокупность $\mathfrak{M}$ всех элементов кольца $\mathfrak{D}_\mathfrak{p}$, делящихся на π. По только что доказанному совокупность $\mathfrak{M}$ совпадает со всеми линейными комбинациями элементов

$$p\theta_1, \ldots, p\theta_f, \theta_{f+1}, \ldots, \theta_n \tag{14}$$

с коэффициентами из $\mathfrak{o}_\mathfrak{p}$. С другой стороны, очевидно, что $\mathfrak{M}$ совпадает также со всеми линейными комбинациями элементов

$$\pi\theta_1, \ldots, \pi\theta_n \tag{15}$$

с коэффициентами из $\mathfrak{o}_\mathfrak{p}$. Обозначим через C матрицу перехода от базиса (14) к базису (15). Так как все элементы $\pi\theta_j$ выражаются через базис (14) с коэффициентами из $\mathfrak{o}_\mathfrak{p}$, то $\det C$ является элементом из $\mathfrak{o}_\mathfrak{p}$. В силу симметрии то же справедливо и для $\det C^{-1}$. Следовательно, $\det C$ — единица кольца $\mathfrak{o}_\mathfrak{p}$, т. е. $v_\mathfrak{p}(\det C) = 0$. Если мы первые f столбцов матрицы C умножим на p, то получим, очевидно, матрицу $A = (a_{ij})$, для которой

$$\pi\theta_i = \sum_{j=1}^{n} a_{ij}\theta_j,$$

поэтому $N_{K/k}(\pi) = \det A = p^f \det C$, откуда

$$v_\mathfrak{p}(N_{K/k}(\pi)) = f,$$

и теорема 5 доказана.

Теорема 6. *Если расширение K/k сепарабельно, то для $\mathfrak{D}_\mathfrak{p}$ всегда существует фундаментальный базис относительно $\mathfrak{o}_\mathfrak{p}$.*

Приступая к доказательству этой теоремы, заметим, что оно аналогично, по существу, доказательству теоремы 6 § 2 гл. II.

Так как каждый элемент из K при умножении на надлежащую степень простого элемента кольца $\mathfrak{o}_\mathfrak{p}$ становится целым относительно $\mathfrak{o}_\mathfrak{p}$, то для расширения K/k существует базис $\alpha_1, \ldots, \alpha_n$, все элементы которого принадлежат $\mathfrak{D}_\mathfrak{p}$. Рассмотрим взаимный с ним базис $\alpha_1^*, \ldots, \alpha_n^*$ (см. Дополнение, § 2, п. 3; здесь мы уже пользуемся сепарабельностью K/k). Если $\alpha \in \mathfrak{D}_\mathfrak{p}$ и

$$\alpha = c_1\alpha_1^* + \ldots + c_n\alpha_n^*, \tag{16}$$

где $c_i \in k$, то $c_i = \mathrm{Sp}(\alpha\alpha_i)$, а значит, $c_i \in \mathfrak{o}_\mathfrak{p}$ (так как $\alpha\alpha_i \in \mathfrak{D}_\mathfrak{p}$). Для каждого $s = 1, \ldots, n$ рассмотрим в кольце $\mathfrak{D}_\mathfrak{p}$ элементы, выражения которых через базис $\alpha_1^*, \ldots, \alpha_n^*$ имеют вид

$$c_s\alpha_s^* + \ldots + c_n\alpha_n^*, \qquad c_i \in \mathfrak{o}_\mathfrak{p}, \tag{17}$$

и выберем среди них такой элемент

$$\omega_s = c_{ss}\alpha_s^* + \ldots + c_{sn}\alpha_n^*, \qquad c_{sj} \in \mathfrak{o}_\mathfrak{p},$$

что $v_\mathfrak{p}(c_s) \geqslant v_\mathfrak{p}(c_{ss})$ для всех коэффициентов c_s элементов вида (17) из $\mathfrak{D}_\mathfrak{p}$. Ясно, что $c_{ss} \neq 0$ при всех s, так что элементы $\omega_1, \ldots, \omega_n$ из $\mathfrak{D}_\mathfrak{p}$ линейно независимы над k. Пусть теперь α — произвольный элемент из $\mathfrak{D}_\mathfrak{p}$. Если мы представим его в виде (16), то $c_1 = c_{11}a_1$, где $a_1 \in \mathfrak{o}_\mathfrak{p}$, по выбору ω_1. Для разности $\alpha - a_1\omega_1 \in \mathfrak{D}_\mathfrak{p}$ мы имеем разложение

$$\alpha - a_1\omega_1 = c_2'\alpha_2^* + \ldots + c_n'\alpha_n^*, \qquad c_l' \in \mathfrak{o}_\mathfrak{p},$$

при этом $c_2' = c_{22}a_2$, где $a_2 \in \mathfrak{o}_\mathfrak{p}$, по выбору ω_2. Повторив это рассуждение n раз, мы придем в конце концов к разложению (13), в котором все коэффициенты a_i принадлежат $\mathfrak{o}_\mathfrak{p}$. Базис $\omega_1, \ldots, \omega_n$ является, таким образом, фундаментальным относительно $\mathfrak{o}_\mathfrak{p}$, и теорема 6 доказана.

Из теорем 5 и 6 и формулы (12) очевидным образом вытекает следующее утверждение.

Теорема 7. *Если расширение K/k сепарабельно, то индексы ветвления $e_\mathfrak{P}$ и степени инерции $f_\mathfrak{P}$ простых дивизоров $\mathfrak{P}$ кольца $\mathfrak{D}$, делящих фиксированный простой дивизор $\mathfrak{p}$ кольца $\mathfrak{o}$, связаны между собой соотношением*

$$\sum_{\mathfrak{P} \mid \mathfrak{p}} e_\mathfrak{P} f_\mathfrak{P} = n = (K : k).$$

В случае сепарабельного расширения K/k формула (7) может быть переписана в виде

$$v_\mathfrak{p}(N_{K/k}(\alpha)) = \sum_{\mathfrak{P} \mid \mathfrak{p}} f_\mathfrak{P} v_\mathfrak{P}(\alpha). \tag{18}$$

Замечание. Для несепарабельных расширений равенство теоремы 7 может не иметь места. Однако всегда справедливо неравенство $\sum_{\mathfrak{P}\mid\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}} \leqslant n$ (см. задачу 13). Можно показать также, что в общем случае имеет место неравенство $f_{\mathfrak{P}} \leqslant d_{\mathfrak{P}}$.

Рассмотрим теперь случай, когда K/k является конечным расширением Галуа с группой Галуа G (см. п. 4 § 2 Дополнения). Пусть $\mathfrak{P}$ — какой-нибудь простой дивизор кольца $\mathfrak{O}$, делящий фиксированный простой дивизор $\mathfrak{p}$ кольца $\mathfrak{o}$, и $\nu = \nu_{\mathfrak{P}}$ — соответствующий ему показатель поля K. Для каждого автоморфизма $\sigma \in G$ через $\sigma\nu$ обозначим показатель поля K, определяемый равенством

$$(\sigma\nu)(\alpha) = \nu(\sigma^{-1}(\alpha)), \quad \alpha \in K.$$

Согласно задаче 7 § 4 показатели $\sigma\nu$ для всех $\sigma \in G$ исчерпывают собой все продолжения показателя $\nu_{\mathfrak{p}}$ на поле K (для различных σ и τ из G показатели $\sigma\nu$ и $\tau\nu$ не обязательно различны). Простой дивизор кольца $\mathfrak{O}$, соответствующий показателю $\sigma\nu$, обозначим через $\sigma\mathfrak{P}$. Рассмотрим индексы ветвления и степени инерции дивизоров $\sigma\mathfrak{P}$. Если p — простой элемент кольца $\mathfrak{o}_{\mathfrak{p}}$ показателя $\nu_{\mathfrak{p}}$, то

$$e_{\sigma\mathfrak{P}} = \nu_{\sigma\mathfrak{P}}(p) = (\sigma\nu)(p) = \nu(\sigma^{-1}(p)) = \nu_{\mathfrak{P}}(p) = e_{\mathfrak{P}}.$$

Далее, пусть π — простой элемент кольца $\mathfrak{O}_{\mathfrak{p}}$, соответствующий простому дивизору $\mathfrak{P}$ (для которого $\nu_{\mathfrak{P}}(\pi) = 1$). Ясно, что $\sigma(\pi)$ также является простым элементом кольца $\mathfrak{O}_{\mathfrak{p}}$, и так как $\nu_{\sigma\mathfrak{P}}(\sigma(\pi)) = \nu(\sigma^{-1}(\sigma(\pi))) = 1$, то этот простой элемент соответствует простому дивизору $\sigma\mathfrak{P}$. Расширение Галуа K/k сепарабельно (теорема 13 § 2 Дополнения), а значит, в $\mathfrak{O}_{\mathfrak{p}}$ существует фундаментальный базис относительно $\mathfrak{o}_{\mathfrak{p}}$ (теорема 6). Применяя теперь теорему 5, получаем

$$f_{\sigma\mathfrak{P}} = \nu_{\mathfrak{p}}(N_{K/k}(\sigma(\pi))) = \nu_{\mathfrak{p}}(N_{K/k}(\pi)) = f_{\mathfrak{P}}.$$

Нами доказано, таким образом, что для любого $\sigma \in G$ справедливы формулы $e_{\sigma\mathfrak{P}} = e_{\mathfrak{P}}$, $f_{\sigma\mathfrak{P}} = f_{\mathfrak{P}}$. Так как простые дивизоры $\sigma\mathfrak{P}$ ($\sigma \in G$) исчерпывают собой все простые дивизоры кольца $\mathfrak{O}$, делящие данный простой дивизор $\mathfrak{p}$ кольца $\mathfrak{o}$ (задача 7 § 4), то полученные нами формулы означают, что все простые дивизоры кольца $\mathfrak{O}$, делящие $\mathfrak{p}$, имеют общее значение индекса ветвления и общее значение степени инерции. Эти общие значения можно, следовательно, обозначить через $e_{\mathfrak{p}}$ и $f_{\mathfrak{p}}$ соответственно.

Обозначим через $m_{\mathfrak{p}}$ число различных дивизоров вида $\sigma\mathfrak{P}$, когда σ пробегает все автоморфизмы из G (т. е. число различных

простых дивизоров кольца $\mathfrak{O}$, делящих $\mathfrak{p}$). Формулу теоремы 7 для случая расширений Галуа мы можем теперь переписать в виде

$$e_{\mathfrak{p}} f_{\mathfrak{p}} m_{\mathfrak{p}} = n = (K:k).$$

4. Конечность числа разветвленных простых дивизоров. Определение. *Простой дивизор $\mathfrak{p}$ кольца $\mathfrak{o}$ называется разветвленным в кольце $\mathfrak{O}$, если он делится на квадрат простого дивизора кольца $\mathfrak{O}$, и называется неразветвленным в противном случае.*

Неразветвленные $\mathfrak{p}$ характеризуются, следовательно, тем, что для них в разложении (2) все e_i равны 1.

Предполагая расширение K/k сепарабельным, мы приведем одно важное условие неразветвленности $\mathfrak{p}$.

Допустим, что в кольце $\mathfrak{O}_{\mathfrak{p}}$ имеется такой примитивный элемент θ (для расширения K/k), что дискриминант $D(f)$ его минимального многочлена $f(t)$ является единицей в $\mathfrak{o}_{\mathfrak{p}}$. Покажем, что в этом случае степени $1, \theta, \ldots, \theta^{n-1}$, где $n=(K:k)$, образуют фундаментальный базис кольца $\mathfrak{O}_{\mathfrak{p}}$ над $\mathfrak{o}_{\mathfrak{p}}$. Действительно, пусть $\omega_1, \ldots, \omega_n$ — какой-нибудь фундаментальный базис $\mathfrak{O}_{\mathfrak{p}}$ и C — матрица перехода от базиса ω_i к базису θ^j. Тогда

$$D(f) = D(1, \theta, \ldots, \theta^{n-1}) = (\det C)^2 D(\omega_1, \ldots, \omega_n)$$

(см. § 2 Дополнения, формула (12)). Так как $D(f)$ является единицей в $\mathfrak{o}_{\mathfrak{p}}$, а множители справа принадлежат кольцу $\mathfrak{o}$, то $\det C$ есть единица в $\mathfrak{o}_{\mathfrak{p}}$, откуда и следует, что $1, \theta, \ldots, \theta^{n-1}$ — также фундаментальный базис.

Пусть p — простой элемент кольца $\mathfrak{o}_{\mathfrak{p}}$ и $\Sigma_{\mathfrak{p}}$ — поле вычетов показателя $\nu_{\mathfrak{p}}$. Для произвольного многочлена $g(t)$ с коэффициентами из $\mathfrak{o}_{\mathfrak{p}}$ через $\bar{g}(t)$ мы будем обозначать многочлен из кольца $\Sigma_{\mathfrak{p}}[t]$, получающийся заменой всех коэффициенттов $g(t)$ их классами вычетов по модулю p. Так как дискриминант $D(\bar{f}) \in \Sigma_{\mathfrak{p}}$ многочлена $\bar{f}(t) \in \Sigma_{\mathfrak{p}}[t]$ равен классу вычетов по модулю p с представителем $D(f) \in \mathfrak{o}_{\mathfrak{p}}$, то ввиду условия этот дискриминант $D(\bar{f})$ отличен от нуля. Следовательно, в разложении

$$\bar{f}(t) = \bar{\varphi}_1(t) \ldots \bar{\varphi}_m(t) \tag{19}$$

на неприводимые множители в кольце $\Sigma_{\mathfrak{p}}[t]$ многочлены $\bar{\varphi}_i$ все различны (здесь φ_i — некоторые многочлены из $\mathfrak{o}_{\mathfrak{p}}[t]$). Если через d_i мы обозначим степень $\bar{\varphi}_i$, то, очевидно,

$$d_1 + \ldots + d_m = n = (K:k). \tag{20}$$

Теорема 8. *Если дискриминант минимального многочлена $f(t)$ примитивного элемента $\theta \in \mathfrak{O}_\mathfrak{p}$ является единицей в $\mathfrak{o}_\mathfrak{p}$, то простой дивизор $\mathfrak{p}$ не разветвлен в $\mathfrak{O}$ и все простые дивизоры $\mathfrak{P}_i$ из разложения*

$$\mathfrak{p} = \mathfrak{P}_1 \dots \mathfrak{P}_m$$

находятся во взаимно однозначном соответствии с неприводимыми многочленами $\bar{\varphi}_i \in \Sigma_\mathfrak{p}[t]$ из разложения (19). *Степень инерции f_i простого дивизора $\mathfrak{P}_i$ совпадает со степенью d_i соответствующего ему многочлена $\bar{\varphi}_i(t)$.*

Доказательство. Пусть $g(t)$ — произвольный многочлен из $\mathfrak{o}_\mathfrak{p}[t]$. Докажем, что если многочлены $\bar{g}$ и $\bar{\varphi}_i$ взаимно просты в кольце $\Sigma_\mathfrak{p}[t]$, то элементы $g(\theta)$ и $\varphi_i(\theta)$ взаимно просты в кольце $\mathfrak{O}_\mathfrak{p}$. Действительно, при взаимно простых $\bar{g}$ и $\bar{\varphi}_i$ в кольце $\mathfrak{o}_\mathfrak{p}[t]$ существуют такие многочлены $u(t)$, $v(t)$ и $l(t)$, что

$$g(t)u(t) + \varphi_i(t)v(t) = 1 + pl(t).$$

Если бы $g(\theta)$ и $\varphi_i(\theta)$ делились в кольце $\mathfrak{O}_\mathfrak{p}$ на некоторый простой элемент π, то, поскольку $\pi | p$ (теорема 7 § 4), из последнего равенства (при $t = \theta$) следовало бы, что $\pi | 1$. Полученное противоречие и доказывает наше утверждение.

Так как неприводимые многочлены $\bar{\varphi}_i$ различны, то, в частности, мы получаем, что $\varphi_1(\theta), \dots, \varphi_m(\theta)$ попарно взаимно просты.

Допустим, что $\varphi_i(\theta)$ является единицей в $\mathfrak{O}_\mathfrak{p}$, т. е. что $\varphi_i(\theta)\xi = 1$, $\xi \in \mathfrak{O}_\mathfrak{p}$. Так как $1, \theta, \dots, \theta^{n-1}$ образуют фундаментальный базис $\mathfrak{O}_\mathfrak{p}$ над $\mathfrak{o}_\mathfrak{p}$, то $\xi = h(\theta)$, где $h(t) \in \mathfrak{o}_\mathfrak{p}[t]$. Равенство $\varphi_i(\theta)h(\theta) = 1$ означает, что $\varphi_i(t)h(t) = 1 + f(t)q(t)$, где $q(t) \in \mathfrak{o}_\mathfrak{p}[t]$ (поскольку старший коэффициент $f(t)$ равен 1). При переходе к полю вычетов $\Sigma_\mathfrak{p}$ это дает нам равенство $\bar{\varphi}_i\bar{h} = 1 + \bar{\varphi}_1 \dots \bar{\varphi}_m\bar{q}$, и мы опять получили противоречие. Следовательно, все элементы $\varphi_1(\theta), \dots, \varphi_m(\theta)$ не являются единицами в $\mathfrak{O}_\mathfrak{p}$.

Для каждого i выберем в $\mathfrak{O}_\mathfrak{p}$ простой элемент $\pi_i | \varphi_i(\theta)$. Так как по доказанному все $\varphi_i(\theta)$ попарно взаимно просты, то простые элементы $\pi_1, \dots, \pi_m$ попарно не ассоциированы. Обозначим через $\mathfrak{P}_1, \dots, \mathfrak{P}_m$ соответствующие им простые дивизоры кольца $\mathfrak{O}$ и через $f_1, \dots, f_m$ степени инерции этих дивизоров. В поле вычетов $\Sigma_{\mathfrak{P}_i}$ показателя $\nu_{\mathfrak{P}_i}$ классы вычетов $\bar{1}, \bar{\theta}, \dots, \bar{\theta}^{d_i-1}$ линейно независимы над $\Sigma_\mathfrak{p}$ (d_i — степень $\bar{\varphi}_i$). Действительно, если для многочлена $g(t) \in \mathfrak{o}_\mathfrak{p}[t]$ степени $< d_i$ имеет место равенство $\bar{g}(\bar{\theta}) = 0$, то элемент $g(\theta)$ делится в кольце $\mathfrak{O}_\mathfrak{p}$ на π_i и поэтому

$g(\theta)$ и $\varphi_i(\theta)$ не взаимно просты. Но в таком случае, как мы видели в начале доказательства, $\bar{g}(t)$ должен делиться на $\bar{\varphi}_i(t)$ и, следовательно, все коэффициенты $\bar{g}(t)$ — нули.

Нами доказано, таким образом, что

$$d_i \leqslant f_i, \qquad i = 1, \ldots, m.$$

Сопоставляя эти неравенства с равенством (20) и принимая во внимание теорему 7, мы приходим к выводу, что $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ — это все простые дивизоры, делящие $\mathfrak{p}$, что их индексы ветвления e_i равны 1 и, наконец, что $d_i = f_i$. Все это и составляет содержание теоремы 8. Заметим попутно, что поскольку $\varphi_i(\theta)$, делясь на π_i, не делится на другие простые элементы π_j, то π_i может быть определен как общий наибольший делитель в кольце $\mathfrak{O}_\mathfrak{p}$ элементов $\varphi_i(\theta)$ и p.

Следствие. *Если K/k сепарабельно, то в кольце $\mathfrak{o}$ имеется только конечное число простых дивизоров $\mathfrak{p}$, разветвленных в $\mathfrak{O}$.*

Выберем для расширения K/k примитивный элемент θ, содержащийся в $\mathfrak{O}$. Дискриминант $D = D(1, \theta, \ldots, \theta^{n-1})$ является элементом из $\mathfrak{o}^*$. Если $\mathfrak{p} \nmid D$, то по теореме $\mathfrak{p}$ не разветвлен в $\mathfrak{O}$. Таким образом, разветвленными в $\mathfrak{O}$ могут быть только те простые дивизоры кольца $\mathfrak{o}$, которые делят D.

Задачи

1. Пусть $\mathfrak{o}$ — кольцо с теорией дивизоров, k — его поле отношений и $k \subset K \subset K'$ — цепочка конечных расширений. Обозначим через $\mathfrak{O}$ и $\mathfrak{O}'$ целые замыкания кольца $\mathfrak{o}$ в полях K и K' соответственно. Для простого дивизора $\mathfrak{P}'$ кольца $\mathfrak{O}'$ через $\mathfrak{P}$ обозначим простой дивизор кольца $\mathfrak{O}$, делящийся на $\mathfrak{P}'$ и через $\mathfrak{p}$ — простой дивизор кольца $\mathfrak{o}$, делящийся на $\mathfrak{P}$. Доказать, что степень инерции $\mathfrak{P}'$ относительно k равна произведению степени инерции $\mathfrak{P}'$ относительно K на степень инерции $\mathfrak{P}$ относительно k. Сформулировать и доказать аналогичное утверждение для индексов ветвления.

2. Пусть в кольце $\mathfrak{o}$ с полем отношений k имеется теория дивизоров с конечным числом простых дивизоров, и пусть простому дивизору $\mathfrak{p}$ соответствует простой элемент p кольца $\mathfrak{o}$. Доказать, что кольцо вычетов $\mathfrak{o}/(p)$ изоморфно полю вычетов $\Sigma_\mathfrak{p}$ показателя $\nu_\mathfrak{p}$.

3. Пусть $\nu_\mathfrak{p}$ — показатель поля k, $\mathfrak{o}_\mathfrak{p}$ — его кольцо, K/k — конечное сепарабельное расширение, $\mathfrak{O}_\mathfrak{p}$ — целое замыкание кольца $\mathfrak{o}_\mathfrak{p}$ в поле K и $\omega_1, \ldots, \omega_n$ — базис K над k, все элементы которого принадлежат кольцу $\mathfrak{O}_\mathfrak{p}$. Доказать, что если дискриминант $D(\omega_1, \ldots, \omega_n)$ является единицей кольца $\mathfrak{o}_\mathfrak{p}$, то $\omega_1, \ldots, \omega_n$ образуют фундаментальный базис кольца $\mathfrak{O}_\mathfrak{p}$ над $\mathfrak{o}_\mathfrak{p}$.

4. Доказать единственность гомоморфизма N: $\mathfrak{D} \to \mathfrak{D}_0$, удовлетворяющего условию теоремы 4.

5. Доказать единственность изоморфного вложения $\mathfrak{D}_0 \to \mathfrak{D}$, удовлетворяющего условию теоремы 3.

6. Пусть $\mathfrak{a}$ — дивизор кольца $\mathfrak{o}$. Рассматривая его как дивизор кольца $\mathfrak{O}$ (в силу вложения $\mathfrak{D}_0 \to \mathfrak{D}$), доказать, что

$$N_{K/k}(\mathfrak{a}) = \mathfrak{a}^n, \qquad n = (K : k).$$

7. Пусть K/k — сепарабельное расширение степени n. Доказать, что если дивизор $\mathfrak{a}$ кольца $\mathfrak{o}$ становится главным дивизором в кольце $\mathfrak{O}$, то $\mathfrak{a}^n$ — главный дивизор в $\mathfrak{o}$.

8. Пусть K/k сепарабельно. Доказать, что норма $N_{K/k}(\mathfrak{A})$ дивизора $\mathfrak{A}$ кольца $\mathfrak{O}$ есть общий наибольший делитель главных дивизоров $(N_{K/k}(\alpha))_k$, где α пробегает все элементы из $\mathfrak{O}^*$, делящиеся на $\mathfrak{A}$.

9. Многочлен $f(t) = t^n + a_1 t^{n-1} + \ldots + a_n$ с коэффициентами из кольца $\mathfrak{o}$ называется многочленом Эйзенштейна относительно простого дивизора $\mathfrak{p}$, если $a_1, \ldots, a_n$ все делятся на $\mathfrak{p}$ и a_n, делясь на $\mathfrak{p}$, не делится на $\mathfrak{p}^2$. Доказать, что если в кольце $\mathfrak{O}$ существует примитивный элемент θ для расширения K/k степени n, минимальный многочлен которого является многочленом Эйзенштейна относительно $\mathfrak{p}$, то $\mathfrak{p}$ делится только на один простой дивизор $\mathfrak{P}$ кольца $\mathfrak{O}$ и $\mathfrak{p} = \mathfrak{P}^n$ (степень инерции $\mathfrak{P}$ относительно $\mathfrak{p}$ равна, следовательно, 1).

10. При тех же условиях доказать, что базис $1, \theta, \ldots, \theta^{n-1}$ является фундаментальным базисом кольца $\mathfrak{O}_\mathfrak{p}$ относительно $\mathfrak{o}_\mathfrak{p}$.

11. Пусть k_0 — произвольное поле характеристики p и $k = k_0(x, y)$ — поле рациональных функций от x и y над полем k_0. Рассмотрим на k показатель ν_0, определение которого дано в задаче 9 § 4, при этом в качестве ряда $\xi(t) \in k_0\{t\}$ (трансцендентного над $k_0(t)$) мы возьмем ряд вида

$$\xi(t) = \eta(t)^p = \left(\sum_{n=0}^{\infty} a_n t^n\right)^p = \sum_{n=0}^{\infty} a_n^p t^{np}, \qquad a_n \in k_0.$$

Согласно задаче 8 § 4 для показателя ν_0 существует единственное продолжение ν на чисто несепарабельное расширение $K = k(\sqrt[p]{y})$ степени p над k. Доказать, что индекс ветвления ν относительно ν_0 равен 1 и что поле вычетов показателя ν_0 совпадает с полем вычетов показателя ν (в смысле изоморфного вложения). Ввиду теоремы 5 и равенства (12) отсюда следует, что для кольца $\mathfrak{O}$ показателя ν, являющегося целым замыканием в K кольца $\mathfrak{o}$ показателя ν_0, не существует фундаментального базиса относительно $\mathfrak{o}$.

12. В условиях и обозначениях предыдущей задачи доказать непосредственно отсутствие фундаментального базиса в $\mathfrak{O}$ относительно $\mathfrak{o}$ (без использования теоремы 5).

13. Пусть $\mathfrak{o}$ — кольцо с теорией дивизоров, k — его поле отношений, K/k — конечное расширение степени n, $\mathfrak{O}$ — целое замыкание кольца $\mathfrak{o}$ в поле K, $\mathfrak{p}$ — простой дивизор кольца $\mathfrak{o}$, $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ — простые дивизоры кольца $\mathfrak{O}$, делящие $\mathfrak{p}$, $e_1, \ldots, e_m$ — их индексы ветвления и $f_1, \ldots, f_m$ — их степени инерции относительно $\mathfrak{p}$. Для каждого $s = 1, \ldots, m$ через $\overline{\alpha}^{\mathfrak{P}_s}$ будем обозначать класс вычетов в поле $\Sigma_{\mathfrak{P}_s}$ с представителем $\alpha \in \mathfrak{O}_{\mathfrak{P}_s}$. Выберем элементы $\omega_{si} \in \mathfrak{O}_\mathfrak{p}$ $(1 \leqslant i \leqslant f_s)$ так, чтобы классы вычетов $\overline{\omega}_{si}^{\mathfrak{P}_s}$ образовали базис $\Sigma_{\mathfrak{P}_s}/\Sigma_\mathfrak{p}$ и, кроме того, чтобы $\nu_{\mathfrak{P}_j}(\omega_{si}) \geqslant e_j$ при $j \neq s$, $1 \leqslant j \leqslant m$. Простые элементы кольца $\mathfrak{O}_\mathfrak{p}$, соответствующие дивизорам $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$, обозначим через $\pi_1, \ldots, \pi_m$. Доказать, что система элементов

$$\omega_{si}\pi_s^j, \qquad (*)$$

$$s = 1, \ldots, m, \quad i = 1, \ldots, f_s, \quad j = 0, 1, \ldots, e_s - 1,$$

линейно независима относительно k.

Указание. Рассмотрим линейную комбинацию

$$\alpha = \sum c_{sij}\omega_{si}\pi_s^j$$

с коэффициентами из $\mathfrak{o}_\mathfrak{p}$, среди которых хоть один является единицей в $\mathfrak{o}_\mathfrak{p}$. Пусть $\nu_\mathfrak{p}\left(c_{s_0 i_0 j_0}\right) = 0$, где j_0 выбрано так, что $\nu_\mathfrak{p}\left(c_{s_0 i j}\right) > 0$ при $j < j_0$ и всех i. Тогда

$$\nu_{\mathfrak{P}_{s_0}}(\alpha) = j_0.$$

14. Доказать, что в случае сепарабельного расширения K/k система $(*)$ является фундаментальным базисом $\mathfrak{O}_\mathfrak{p}$ относительно $\mathfrak{o}_\mathfrak{p}$.

15. Доказать, что в случае сепарабельного K/k для любого $\alpha \in \mathfrak{O}_\mathfrak{p}$ имеет место формула

$$\overline{\mathrm{Sp}_{K/k}(\alpha)}^{\mathfrak{p}} = \sum_{s=1}^{m} e_s \,\mathrm{Sp}_{\Sigma_{\mathfrak{P}_s}/\Sigma_\mathfrak{p}}\left(\bar{\alpha}^{\mathfrak{P}_s}\right).$$

16. Пусть $f(t)$ — характеристический многочлен элемента $\alpha \in \mathfrak{O}_\mathfrak{p}$ относительно K/k. Заменяя его коэффициенты соответствующими классами вычетов из $\Sigma_\mathfrak{p}$, мы получим многочлен $\bar{f}(t) \in \Sigma_\mathfrak{p}[t]$. Для каждого $s = 1, \ldots, m$ обозначим, далее, через $\varphi_s(t)$ характеристический многочлен элемента $\bar{\alpha}^{\mathfrak{P}_s} \in \Sigma_{\mathfrak{P}_s}$ относительно расширения $\Sigma_{\mathfrak{P}_s}/\Sigma_\mathfrak{p}$. Обобщая предыдущую задачу (при сепарабельном K/k), доказать, что

$$\bar{f}(t) = \varphi_1(t)^{e_1} \ldots \varphi_m(t)^{e_m}.$$

17. Пусть K/k сепарабельно. Для каждого $\mathfrak{p}$ выберем в кольце $\mathfrak{O}_\mathfrak{p}$ фундаментальный базис $\alpha_1, \ldots, \alpha_n$ относительно $\mathfrak{o}_\mathfrak{p}$. Положим

$$d_\mathfrak{p} = \nu_\mathfrak{p}\left(D(\alpha_1, \ldots, \alpha_n)\right).$$

Доказать, что целые числа $d_\mathfrak{p} \geqslant 0$ почти все равны нулю. Целый дивизор кольца $\mathfrak{o}$

$$\mathfrak{d}_{K/k} = \prod_\mathfrak{p} \mathfrak{p}^{d_\mathfrak{p}}$$

называется *дискриминантом расширения* K/k (относительно кольца $\mathfrak{o}$).

18. Доказать, что простой дивизор $\mathfrak{p}$ кольца $\mathfrak{o}$ не входит в дискриминант $\mathfrak{d}_{K/k}$ (т. е. $d_\mathfrak{p} = 0$) тогда и только тогда, когда $\mathfrak{p}$ не разветвляется в $\mathfrak{O}$ (все индексы ветвления e_i равны 1) и все расширения $\Sigma_{\mathfrak{P}_s}/\Sigma_\mathfrak{p}$ $(s = 1, \ldots, m)$ сепарабельны.

19. Пусть для кольца $\mathfrak{O}$ существует фундаментальный базис $\omega_1, \ldots, \omega_n$ относительно $\mathfrak{o}$. Доказать, что тогда дискриминант $\mathfrak{d}_{K/k}$ совпадает с главным дивизором $(D(\omega_1, \ldots, \omega_n))$.

20. Сохраняя обозначения начала п. 2, предположим, что K/k — расширение Галуа с группой Галуа G. Для автоморфизма $\sigma \in G$ и дивизора $\mathfrak{A} = \prod_\mathfrak{P} \mathfrak{P}^{A(\mathfrak{P})}$ кольца $\mathfrak{O}$ положим

$$\sigma(\mathfrak{A}) = \prod_\mathfrak{P} (\sigma\mathfrak{P})^{A(\mathfrak{P})}.$$

Доказать, что для любого $\alpha \neq 0$ из $\mathfrak{O}$ справедлива формула

$$\sigma((\alpha)_K) = (\sigma(\alpha))_K.$$

§ 6. Дедекиндовы кольца

1. Сравнения по модулю дивизора. Рассмотрим кольцо $\mathfrak{O}$ с полем отношений K, для которого существует теория дивизоров $\mathfrak{O}^* \to \mathfrak{D}$.

Определение. *Мы говорим, что элементы* α *и* β *из кольца* $\mathfrak{O}$ *сравнимы между собой по модулю дивизора* $\mathfrak{a} \in \mathfrak{D}$, *и пишем*

$$\alpha \equiv \beta \pmod{\mathfrak{a}},$$

если разность $\alpha - \beta$ *делится на* $\mathfrak{a}$.

В случае главного дивизора (μ) сравнение $\alpha \equiv \beta (\mathrm{mod}\,(\mu))$ эквивалентно, очевидно, сравнению $\alpha \equiv \beta (\mathrm{mod}\,\mu)$ в смысле определения п. 1 § 4 Дополнения.

Перечислим ряд элементарных свойств сравнений, легко вытекающих из определения.

1) Сравнения по модулю $\mathfrak{a}$ можно почленно складывать и перемножать.

2) Если некоторое сравнение имеет место по модулю $\mathfrak{a}$, то оно имеет место также и по любому делителю $\mathfrak{b}$ дивизора $\mathfrak{a}$.

3) Если некоторое сравнение имеет место по модулю дивизоров $\mathfrak{a}$ и $\mathfrak{b}$, то оно имеет место и по модулю их общего наименьшего кратного.

4) Если элемент $\alpha \in \mathfrak{O}$ взаимно прост с $\mathfrak{a}$ (т. е. дивизоры (α) и $\mathfrak{a}$ взаимно просты), то из сравнения $\alpha\beta \equiv 0 \pmod{\mathfrak{a}}$ следует $\beta \equiv 0 \pmod{\mathfrak{a}}$.

5) Обе части сравнения по модулю $\mathfrak{a}$ можно сократить на общий множитель, если только этот множитель взаимно прост с $\mathfrak{a}$.

6) Если $\mathfrak{p}$ — простой дивизор и $\alpha\beta \equiv 0 \pmod{\mathfrak{p}}$, то либо $\alpha \equiv 0 \pmod{\mathfrak{p}}$, либо $\beta \equiv 0 \pmod{\mathfrak{p}}$.

Ввиду свойства 1) на множестве классов вычетов элементов кольца $\mathfrak{O}$ по модулю данного дивизора $\mathfrak{a}$ мы можем ввести действия сложения и умножения. Легко проверяется, что относительно этих действий все классы вычетов по модулю $\mathfrak{a}$ образуют кольцо. Оно называется *кольцом классов вычетов по модулю дивизора* $\mathfrak{a}$ и обозначается через $\mathfrak{O}/\mathfrak{a}$.

Свойство 6) в терминах кольца вычетов означает, что для простого дивизора $\mathfrak{p}$ кольцо классов вычетов $\mathfrak{O}/\mathfrak{p}$ не имеет делителей нуля.

Предположим теперь, что $\mathfrak{O}$ — максимальный порядок поля алгебраических чисел K. Дивизоры кольца $\mathfrak{O}$ мы называем в этом случае также *дивизорами поля* K.

Так как произвольный дивизор $\mathfrak{a}$ поля K является делителем некоторого отличного от нуля числа $\alpha \in \mathfrak{O}$, а число α в свою очередь является делителем натурального числа a (например, $|N(\alpha)|$ делится на α), то получаем, что для каждого дивизора $\mathfrak{a}$ существует делящееся на него натуральное a. По свойству 2 чис-

ла из разных классов вычетов по модулю $\mathfrak{a}$ находятся в разных классах вычетов по модулю a. Вспоминая теперь, что в порядке $\mathfrak{O}$ число классов вычетов по модулю a конечно (и равно a^n, где n — степень поля K, см. доказательство теоремы 5 § 2 гл. II), получаем следующую теорему.

Теорема 1. *Для любого дивизора $\mathfrak{a}$ поля алгебраических чисел K кольцо классов вычетов $\mathfrak{O}/\mathfrak{a}$ конечно.*

Пусть $\mathfrak{p}$ — произвольный простой дивизор поля K. Соответствующий ему показатель $\nu_\mathfrak{p}$ индуцирует на $\mathbb{Q}$ p-адический показатель ν_p при некотором вполне определенном простом p. Так как $\nu_p(p) = 1$, то $\nu_\mathfrak{p}(p) > 0$. т. е. $p \equiv 0 \pmod{\mathfrak{p}}$. Если же простое рациональное q отлично от p, то $\nu_p(q) = 0$, а потому $\nu_\mathfrak{p}(q) = 0$, т. е. $q \not\equiv 0 \pmod{\mathfrak{p}}$.

Кольцо вычетов $\mathfrak{O}/\mathfrak{p}$, будучи конечным и без делителей нуля, является конечным полем (см. Дополнение, § 3). Так как для всякого $\alpha \in \mathfrak{O}$ имеем $p\alpha \equiv 0 \pmod{\mathfrak{p}}$, то характеристика этого поля равна p. Таким образом, имеет место

Теорема 2. *Всякий простой дивизор $\mathfrak{p}$ поля алгебраических чисел является делителем одного и только одного простого рационального числа p. Кольцо вычетов $\mathfrak{O}/\mathfrak{p}$ является конечным полем характеристики p.*

Теория дивизоров в полях алгебраических чисел обладает, как видим, тем свойством, что кольцо классов вычетов по модулю любого простого дивизора есть поле. В общем случае это не всегда так. Например, в кольце многочленов $k[x, y]$ от двух переменных над полем k кольцо вычетов по простому дивизору (x) изоморфно кольцу многочленов $k[y]$ от одной переменной и, следовательно, не является полем.

Предположение о том, что кольцо классов вычетов $\mathfrak{O}/\mathfrak{p}$ есть поле, равносильно, очевидно, разрешимости сравнения $\alpha\xi \equiv 1 \pmod{\mathfrak{p}}$ при любом $\alpha \not\equiv 0 \pmod{\mathfrak{p}}$. Это показывает, что только при таком предположении можно рассчитывать на построение в кольце $\mathfrak{O}$ достаточно полной теории сравнений со свойствами обычных сравнений теории чисел.

2. Сравнения в дедекиндовых кольцах. Определение. *Кольцо $\mathfrak{O}$ называется дедекиндовым, если в нем существует теория дивизоров $\mathfrak{O}^* \to \mathfrak{D}$ и для каждого простого дивизора $\mathfrak{p} \in \mathfrak{D}$ кольцо вычетов $\mathfrak{O}/\mathfrak{p}$ является полем.*

Примерами дедекиндовых колец, кроме максимальных порядков в полях алгебраических чисел, могут служить целые замыкания кольца многочленов $k[x]$ от одной переменной в конечных расширениях поля рациональных функций $k(x)$ (задачи 1 и 2). Дедекиндовым кольцом является также кольцо $\mathfrak{O}_\nu$ произвольного показателя ν на некотором поле (см. § 4, п. 1) и вообще всякое кольцо, в котором имеется теория дивизоров с конечным числом простых дивизоров (задача 3).

Лемма 1. *В дедекиндовом кольце* $\mathfrak{D}$ *для всякого* $\alpha \in \mathfrak{D}$, *не делящегося на простой дивизор* $\mathfrak{p}$, *сравнение* $\alpha\xi \equiv 1 \pmod{\mathfrak{p}^m}$ *разрешимо в* $\mathfrak{D}$ *при любом натуральном* m.

Доказательство. При $m = 1$ разрешимость сравнения постулируется определением. Доказательство леммы в общем случае проведем индукцией по m. Если

$$\alpha\xi_1 \equiv 1 \pmod{\mathfrak{p}} \quad \text{и} \quad \alpha\xi_m \equiv 1 \pmod{\mathfrak{p}^m},$$

то при некоторых $\beta_1 \equiv 0 \pmod{\mathfrak{p}}$ и $\beta_m \equiv 0 \pmod{\mathfrak{p}^m}$ имеют место равенства $1 = \alpha\xi_1 + \beta_1$, $1 = \alpha\xi_m + \beta_m$, перемножая которые получим $1 = \alpha\xi + \beta_1\beta_m$, где

$$\xi = \alpha\xi_1\xi_m + \xi_1\beta_m + \xi_m\beta_1 \quad \text{и} \quad \beta_1\beta_m \equiv 0 \pmod{\mathfrak{p}^{m+1}}.$$

Таким образом, $\alpha\xi \equiv 1 \pmod{\mathfrak{p}^{m+1}}$, и лемма 1 доказана.

Теорема 3. *В дедекиндовом кольце* $\mathfrak{D}$ *существует элемент* ξ, *удовлетворяющий сравнениям*

$$\xi \equiv \beta_1 \pmod{\mathfrak{p}_1^{k_1}},$$
$$\cdots\cdots\cdots$$
$$\xi \equiv \beta_m \pmod{\mathfrak{p}_m^{k_m}}$$

при любых $\beta_1, \ldots, \beta_m$ *из* $\mathfrak{D}$ *и любых попарно различных простых дивизорах* $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ ($k_1, \ldots, k_m$ — *натуральные числа*).

Доказательство. Для каждого дивизора

$$\mathfrak{a}_i = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_{i-1}^{k_{i-1}} \mathfrak{p}_{i+1}^{k_{i+1}} \ldots \mathfrak{p}_m^{k_m}, \qquad i = 1, \ldots, m$$

мы можем найти элемент $\alpha_i \in \mathfrak{D}$, который делится на $\mathfrak{a}_i$, но не делится на $\mathfrak{p}_i$. По лемме 1 сравнение $\alpha_i\xi_i \equiv \beta_i \pmod{\mathfrak{p}_i^{k_i}}$ разрешимо относительно $\xi_i \in \mathfrak{D}$. Легко проверить, что элемент

$$\xi = \alpha_1\xi_1 + \ldots + \alpha_m\xi_m$$

удовлетворяет требованиям теоремы.

Теорема 4. *В дедекиндовом кольце* $\mathfrak{D}$ *для элементов* $\alpha \neq 0$ *и* β *сравнение*

$$\alpha\xi \equiv \beta \pmod{\mathfrak{a}} \tag{1}$$

разрешимо тогда и только тогда, когда β *делится на общий наибольший делитель дивизоров* (α) *и* $\mathfrak{a}$.

Доказательство. Мы предположим сначала, что дивизоры (α) и $\mathfrak{a}$ взаимно просты, и докажем, что в этом случае сравнение (1) разрешимо при любом β. Пусть $\mathfrak{a} = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_m^{k_m} = \mathfrak{p}_i^{k_i}\mathfrak{a}_i$, где простые дивизоры $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ попарно различны. По лемме 1 для каждого $i = 1, \ldots, m$ в кольце $\mathfrak{D}$ существует такой элемент ξ_i', что $\alpha\xi_i' \equiv \beta \pmod{\mathfrak{p}_i^{k_i}}$. Согласно теореме 3 мы можем найти для каждого i элемент ξ_i, для которого $\xi_i \equiv \xi_i' \pmod{\mathfrak{p}_i^{k_i}}$ и $\xi_i \equiv 0 \pmod{\mathfrak{a}_i}$.

Очевидно теперь, что сумма $\xi_1 + \ldots + \xi_m = \xi$ будет удовлетворять сравнению $\alpha\xi \equiv \beta \pmod{\mathfrak{p}_i^{h_i}}$ при любом $i = 1, \ldots, m$, а значит, будет удовлетворять также и сравнению (1).

Перейдем к доказательству теоремы в общем случае. Пусть $\mathfrak{b} = \mathfrak{p}_1^{l_1} \ldots \mathfrak{p}_m^{l_m}$ — общий наибольший делитель дивизоров (α) и $\mathfrak{a}$. Если сравнение (1) имеет место по модулю $\mathfrak{a}$, то оно должно иметь место и по модулю $\mathfrak{b}$, а так как $\alpha \equiv 0 \pmod{\mathfrak{b}}$, то должно выполняться и сравнение $\beta \equiv 0 \pmod{\mathfrak{b}}$. Этим доказана необходимость условия.

Предположим теперь, что β делится на $\mathfrak{b}$. Согласно теореме 3 § 4 в поле K существует элемент μ, для которого

$$\nu_{\mathfrak{p}_i}(\mu) = -l_i, \qquad i = 1, \ldots, m. \tag{2}$$

Покажем, что элемент μ, удовлетворяющий условиям (2), мы можем выбрать так, что

$$\nu_{\mathfrak{q}}(\mu) \geqslant 0 \tag{3}$$

для всех простых дивизоров $\mathfrak{q} \in \mathfrak{D}$, отличных от $\mathfrak{p}_1, \ldots \mathfrak{p}_m$. Пусть μ не удовлетворяет условиям (3), и пусть $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ — все отличные от $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ простые дивизоры, для которых $\nu_{\mathfrak{q}_j}(\mu) = -r_j < 0$. Выберем в $\mathfrak{D}$ такой элемент γ, что $\nu_{\mathfrak{q}_j}(\gamma) = r_j (1 \leqslant j \leqslant s)$ и $\nu_{\mathfrak{p}_i}(\gamma) = 0 (1 \leqslant i \leqslant m)$. Ясно, что элемент $\mu' = \mu\gamma$ удовлетворяет обоим условиям (2) и (3), и наше утверждение доказано. Пусть дивизор $\mathfrak{b}$ определяется равенством $\mathfrak{a} = \mathfrak{b}\mathfrak{b}$. Если μ удовлетворяет условиям (2) и (3), то элемент $\alpha\mu$ принадлежит $\mathfrak{D}$ и взаимно прост с $\mathfrak{b}$. Так как по условию β делится на $\mathfrak{b}$, то $\beta\mu$ также принадлежит $\mathfrak{D}$. По доказанному в кольце $\mathfrak{D}$ существует такой элемент ξ, что $\alpha\mu\xi \equiv \beta\mu \pmod{\mathfrak{b}}$. Для каждого $i = 1, \ldots, m$ мы имеем

$$\nu_{\mathfrak{p}_i}(\alpha\xi - \beta) = \nu_{\mathfrak{p}_i}(\alpha\mu\xi - \beta\mu) + l_i \geqslant k_i - l_i + l_i = k_i,$$

а это и означает, что ξ удовлетворяет сравнению (1).

3. Дивизоры и идеалы. В этом пункте мы покажем, что в дедекиндовом кольце $\mathfrak{D}$ все дивизоры находятся в естественном взаимно однозначном соответствии со всеми ненулевыми идеалами.

Для каждого дивизора $\mathfrak{a}$ через $\bar{\mathfrak{a}}$ мы обозначим совокупность всех элементов кольца $\mathfrak{D}$, делящихся на $\mathfrak{a}$. Очевидно, что $\bar{\mathfrak{a}}$ является ненулевым идеалом кольца $\mathfrak{D}$.

Теорема 5. *В дедекиндовом кольце $\mathfrak{D}$ отображение $\mathfrak{a} \to \bar{\mathfrak{a}}$ $(\mathfrak{a} \in \mathfrak{D})$ является изоморфизмом полугруппы дивизоров $\mathfrak{D}$ на полугруппу всех ненулевых идеалов кольца $\mathfrak{D}$.*

Докажем предварительно следующую лемму.

Лемма 2. *Если $\alpha_1, \ldots, \alpha_s$ — произвольные, отличные от нуля элементы дедекиндова кольца $\mathfrak{D}$ и $\mathfrak{b}$ — общий наибольший дели-*

тель главных дивизоров $(\alpha_1), \ldots, (\alpha_s)$, *то всякий элемент* $\alpha \in \mathfrak{O}$, *делящийся на* $\mathfrak{b}$, *может быть представлен в виде*

$$\alpha = \xi_1\alpha_1 + \ldots + \xi_s\alpha_s, \qquad \xi_i \in \mathfrak{O}.$$

Доказательство леммы проведем индукцией по s. При $s = 1$ утверждение леммы очевидно. Пусть $s \geqslant 2$. Обозначим через $\mathfrak{b}_1$ общий наибольший делитель дивизоров $(\alpha_1), \ldots, (\alpha_{s-1})$. Ясно, что тогда $\mathfrak{b}$ будет общим наибольшим делителем дивизоров $\mathfrak{b}_1$ и (α_s). Пусть α делится на $\mathfrak{b}$. Согласно теореме 4 сравнение $\alpha_s\xi \equiv \alpha \pmod{\mathfrak{b}_1}$ разрешимо относительно элемента $\xi \in \mathfrak{O}$. По индуктивному предположению в кольце $\mathfrak{O}$ существуют такие элементы $\xi_1, \ldots, \xi_{s-1}$, что $\alpha - \xi\alpha_s = \xi_1\alpha_1 + \ldots + \xi_{s-1}\alpha_{s-1}$. Лемма 2 доказана.

Доказательство теоремы 5. Согласно условию 3° определения теории дивизоров отображение $\mathfrak{a} \to \bar{\mathfrak{a}}$ взаимно однозначно.

Пусть A — произвольный ненулевой идеал кольца $\mathfrak{O}$. Для каждого простого дивизора $\mathfrak{p}$ положим

$$a(\mathfrak{p}) = \min_{\alpha \in A} v_{\mathfrak{p}}(\alpha).$$

Очевидно, что $a(\mathfrak{p})$ отлично от нуля только для конечного числа простых дивизоров $\mathfrak{p}$. Произведение $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$, в котором $\mathfrak{p}$ пробегает все те простые дивизоры, для которых $a(\mathfrak{p}) \neq 0$, является, следовательно, дивизором. Докажем, что $\bar{\mathfrak{a}} = A$. Пусть α — произвольный элемент из $\bar{\mathfrak{a}}$. В A можно найти такое конечное множество элементов $\alpha_1, \ldots, \alpha_s$, что $a(\mathfrak{p}) = \min\left(v_{\mathfrak{p}}(\alpha_1), \ldots, v_{\mathfrak{p}}(\alpha_s)\right)$. Это значит, что дивизор $\mathfrak{a}$ является общим наибольшим делителем главных дивизоров $(\alpha_1), \ldots, (\alpha_s)$. По лемме 2 элемент $\alpha \in \bar{\mathfrak{a}}$ может быть представлен в виде $\alpha = \xi_1\alpha_1 + \ldots + \xi_s\alpha_s$ с некоторыми коэффициентами ξ_i из $\mathfrak{O}$. Из этого представления явствует, что $\alpha \in A$, а значит, $\bar{\mathfrak{a}} \subset A$. Сопоставляя это с очевидным обратным включением $A \subset \bar{\mathfrak{a}}$, получим равенство $A = \bar{\mathfrak{a}}$. Нами доказано, таким образом, что отображение $\mathfrak{a} \to \bar{\mathfrak{a}}$ устанавливает взаимно однозначное соответствие между всеми дивизорами кольца $\mathfrak{O}$, с одной стороны, и всеми его ненулевыми идеалами, с другой.

Остается проверить, что это соответствие является изоморфизмом, т. е. что для любых дивизоров $\mathfrak{a}$ и $\mathfrak{b}$ имеем

$$\overline{\mathfrak{ab}} = \bar{\mathfrak{a}}\bar{\mathfrak{b}}. \tag{4}$$

Обозначим произведение $\bar{\mathfrak{a}}\bar{\mathfrak{b}}$ через C. Так как C есть ненулевой идеал в $\mathfrak{O}$, то по доказанному существует такой дивизор $\mathfrak{c}$, что $C = \bar{\mathfrak{c}}$. Нам надо доказать, что $\mathfrak{c} = \mathfrak{ab}$. Пусть простой дивизор $\mathfrak{p}$

входит в $\mathfrak{a}$ и $\mathfrak{b}$ с показателями a и b соответственно. Тогда

$$\min_{\gamma \in C} \nu_{\mathfrak{p}}(\gamma) = \min_{\alpha \equiv \bar{\mathfrak{a}}, \beta \equiv \bar{\mathfrak{b}}} \nu_{\mathfrak{p}}(\alpha\beta) = \min_{\alpha \equiv \bar{\mathfrak{a}}} \nu_{\mathfrak{p}}(\alpha) + \min_{\beta \equiv \bar{\mathfrak{b}}} \nu_{\mathfrak{p}}(\beta) = a + b.$$

Так как это верно для любого простого дивизора $\mathfrak{p}$, то $\mathfrak{c} = \mathfrak{ab}$, и равенство (4) доказано.

Из того факта, что отображение $\mathfrak{a} \to \bar{\mathfrak{a}}$ является изоморфизмом, следует, в частности, что все ненулевые идеалы кольца $\mathfrak{O}$ относительно действия умножения образуют полугруппу с однозначным разложением на простые множители. Для построения теории дивизоров в дедекиндовом кольце (в частности, в максимальном порядке поля алгебраических чисел) в качестве полугруппы $\mathfrak{D}$ можно взять, таким образом, полугруппу ненулевых идеалов. Образом элемента $\alpha \in \mathfrak{O}^*$ при гомоморфизме $\mathfrak{O}^* \to \mathfrak{D}$ будет тогда главный идеал (α), порожденный этим элементом. Такой способ построения теории дивизоров принадлежит Дедекинду.

4. Дробные дивизоры. Если для кольца $\mathfrak{O}$ построена теория дивизоров $\mathfrak{O}^* \to \mathfrak{D}$, то это дает нам некоторую информацию о строении полугруппы $\mathfrak{O}^*$. Естественно попытаться аналогичным образом получить сведения о строении всей мультипликативной группы K^* поля отношений K. Для этой цели нам надо расширить понятие дивизора.

В соответствии с установившейся традицией мы сохраним термин «дивизор» для этого более широкого понятия, а дивизоры в прежнем смысле будем теперь называть целыми дивизорами.

Определение. *Пусть в кольце $\mathfrak{O}$ с полем отношений K имеем теорию дивизоров, и пусть $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ — конечная система простых дивизоров. Выражение*

$$\mathfrak{a} = \mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_m^{k_m} \tag{5}$$

с целыми показателями $k_1, \ldots, k_m$ (не обязательно положительными) называется дивизором поля K. Если среди показателей k_i нет отрицательных, то дивизор $\mathfrak{a}$ называется целым (или дивизором кольца $\mathfrak{O}$). В противном случае он называется дробным.

Дивизор (5) иногда удобно записывать в виде формально бесконечного произведения

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}, \tag{6}$$

распространенного на все простые дивизоры $\mathfrak{p}$, в котором, однако, только конечное число показателей $a(\mathfrak{p})$ отлично от нуля.

Умножение дивизоров определяется формулой

$$\left(\prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}\right)\left(\prod_{\mathfrak{p}} \mathfrak{p}^{b(\mathfrak{p})}\right) = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})+b(\mathfrak{p})}.$$

Для случая целых дивизоров это правило умножения совпадает, очевидно, с правилами умножения в полугруппе $\mathfrak{D}$. Легко видеть

также, что относительно введенного действия все дивизоры поля K образуют абелеву группу, обозначаемую в дальнейшем через $\widehat{\mathfrak{D}}$. Единичным элементом этой группы является единичный дивизор $\mathfrak{e}$, для которого в представлении (6) все показатели $a(\mathfrak{p})$ равны нулю.

Так как каждый элемент $\xi \neq 0$ из поля K является отношением двух элементов из $\mathfrak{D}$, то согласно условию 1) теоремы 4 § 3 среди показателей $\nu_{\mathfrak{p}}$ поля k, соответствующих простым дивизорам $\mathfrak{p}$, имеется только конечное число таких, для которых $\nu_{\mathfrak{p}}(\xi) \neq 0$ Пусть это будут показатели $\nu_{\mathfrak{p}_1}, \ldots, \nu_{\mathfrak{p}_m}$. Дивизор

$$\prod_{i=1}^{m} \mathfrak{p}_i^{\nu_{\mathfrak{p}_i}(\xi)} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\xi)}$$

называется *главным дивизором*, соответствующим элементу $\xi \in K^*$, и обозначается через (ξ). Это новое понятие главного дивизора в применении к элементам из $\mathfrak{D}$ совпадает, очевидно, с первоначальным (см. § 3, п. 4). В силу условия 2) теоремы 4 § 3 главный дивизор (ξ) будет целым тогда и только тогда, когда ξ принадлежит кольцу $\mathfrak{D}$.

Из условия 2 определения показателя (§ 3, п. 4) легко следует, что отображение $\xi \to (\xi)$, $\xi \in K^*$, является гомоморфизмом $K^* \to \widehat{\mathfrak{D}}$ мультипликативной группы поля K в группу дивизоров $\widehat{\mathfrak{D}}$. Согласно теореме 2 § 3 этот гомоморфизм является отображением на всю группу $\widehat{\mathfrak{D}}$ (эпиморфизмом) тогда и только тогда, когда в $\mathfrak{D}$ имеет место однозначность разложения на простые множители. Его ядром является, очевидно, группа единиц кольца $\mathfrak{D}$, а значит, для элементов ξ и η из K^* равенство $(\xi) = (\eta)$ имеет место тогда и только тогда, когда $\xi = \eta\varepsilon$, где ε — единица кольца $\mathfrak{D}$.

Перенесем понятие делимости целых дивизоров на произвольные дивизоры. Пусть $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$ и $\mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{b(\mathfrak{p})}$ — два произвольных дивизора (не обязательно целых). Мы говорим, что $\mathfrak{a}$ делится на $\mathfrak{b}$ ($\mathfrak{b}$ — делитель $\mathfrak{a}$, $\mathfrak{a}$ кратно $\mathfrak{b}$), если существует такой целый дивизор $\mathfrak{c}$, что $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$. В других терминах делимость $\mathfrak{a}$ на $\mathfrak{b}$ может быть охарактеризована неравенствами $a(\mathfrak{p}) \geqslant b(\mathfrak{p})$ при всех $\mathfrak{p}$.

Для произвольных $\mathfrak{a}$ и $\mathfrak{b}$ положим $d(\mathfrak{p}) = \min(a(\mathfrak{p}), b(\mathfrak{p}))$. Так как целые рациональные числа $d(\mathfrak{p})$ равны нулю почти для всех $\mathfrak{p}$, то выражение $\mathfrak{d} = \prod_{\mathfrak{p}} \mathfrak{p}^{d(\mathfrak{p})}$ является дивизором. Этот дивизор $\mathfrak{d}$ называется общим наибольшим делителем дивизоров $\mathfrak{a}$ и $\mathfrak{b}$ (он является делителем $\mathfrak{a}$ и $\mathfrak{b}$ и сам делится на все общие делители $\mathfrak{a}$ и $\mathfrak{b}$). Аналогичным образом определяется общее наименьшее кратное дивизоров $\mathfrak{a}$ и $\mathfrak{b}$.

Элемент $\alpha \in K$ называется *делящимся на дивизор* $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$, если либо $\alpha = 0$, либо главный дивизор (α) делится на $\mathfrak{a}$. В терминах показателей делимость α на $\mathfrak{a}$ характеризуется неравенствами $v_{\mathfrak{p}}(\alpha) \geqslant a(\mathfrak{p})$ при всех $\mathfrak{p}$.

Изложенное в предшествующем пункте соответствие между целыми дивизорами дедекиндова кольца и его ненулевыми идеалами можно распространить и на дробные дивизоры, если воспользоваться понятием дробного идеала (см. п. 4, § 4 Дополнения).

Как и в п. 3, через $\overline{\mathfrak{a}}$ мы обозначим совокупность всех элементов поля K, делящихся на дивизор $\mathfrak{a}$ (теперь уже не обязательно целый). Из условия 3 определения показателя (§ 3, п. 4) следует, что если α и β делятся на $\mathfrak{a}$, то $\alpha \pm \beta$ также делится на $\mathfrak{a}$. Это означает, что совокупность $\overline{\mathfrak{a}}$ является группой относительно действия сложения. Очевидно, далее, что для любого $\alpha \in \overline{\mathfrak{a}}$ и любого $\xi \in \mathfrak{O}$ произведение $\xi\alpha$ также принадлежит $\overline{\mathfrak{a}}$. Чтобы выявить еще одно свойство групп $\overline{\mathfrak{a}}$, убедимся сначала в справедливости формулы

$$\overline{(\gamma)\mathfrak{a}} = \gamma\overline{\mathfrak{a}}, \qquad \gamma \in K^*, \qquad \mathfrak{a} \in \widehat{\mathfrak{O}}. \tag{7}$$

Действительно, делимость элемента ξ на $(\gamma)\mathfrak{a}$ равносильна условиям: $v_{\mathfrak{p}}(\xi) \geqslant v_{\mathfrak{p}}(\gamma) + a(\mathfrak{p})$ при всех $\mathfrak{p}$, $v_{\mathfrak{p}}(\xi/\gamma) \geqslant a(\mathfrak{p})$ при всех $\mathfrak{p}$, $\xi/\gamma \in \overline{\mathfrak{a}}$, $\xi \in \gamma\overline{\mathfrak{a}}$ (здесь $a(\mathfrak{p})$ обозначает показатель, с которым $\mathfrak{p}$ входит в дивизор $\mathfrak{a}$). Очевидно, что для любого дивизора мы можем найти такой элемент $\gamma \in \mathfrak{O}^*$, что дивизор $(\gamma)\mathfrak{a}$ будет целым. Формула (7) показывает, что для такого γ будем иметь включение $\gamma\overline{\mathfrak{a}} \subset \mathfrak{O}$.

Мы видим, таким образом, что совокупность $\overline{\mathfrak{a}}$ для любого дивизора $\mathfrak{a}$ является идеалом поля K в смысле определения п. 4 § 4 Дополнения. Предположим, что для двух дивизоров $\mathfrak{a}$ и $\mathfrak{b}$ имеет место равенство $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$. Выберем элемент $\gamma \neq 0$ так, чтобы дивизоры $(\gamma)\mathfrak{a}$ и $(\gamma)\mathfrak{b}$ были целыми. В силу формулы (7) мы имеем $\overline{(\gamma)\mathfrak{a}} = \overline{(\gamma)\mathfrak{b}}$, откуда $(\gamma)\mathfrak{a} = (\gamma)\mathfrak{b}$ и, следовательно, $\mathfrak{a} = \mathfrak{b}$. Этим доказано, что отображение $\mathfrak{a} \to \overline{\mathfrak{a}}$ взаимно однозначно (если кольцо $\mathfrak{O}$ не дедекиндово, то это отображение не будет отображением «на»: не всякий ненулевой идеал кольца $\mathfrak{O}$ представляется в виде $\overline{\mathfrak{a}}$, см. задачу 11).

Предположим теперь, что $\mathfrak{O}$ — дедекиндово кольцо с полем отношений K. Возьмем произвольный идеал A поля K. Если элемент $\gamma \neq 0$ выбран так, что $\gamma A \subset \mathfrak{O}$, то γA будет ненулевым идеалом кольца $\mathfrak{O}$, а потому по теореме 5 существует такой целый дивизор $\mathfrak{c}$, что $\overline{\mathfrak{c}} = \gamma A$. Положим $\mathfrak{a} = \mathfrak{c}(\gamma)^{-1}$. Тогда $\gamma A = \overline{(\gamma)\mathfrak{a}} = \gamma\overline{\mathfrak{a}}$,

откуда $A = \overline{\mathfrak{a}}$. Таким образом, каждый идеал поля K является образом некоторого дивизора при отображении $\mathfrak{a} \to \overline{\mathfrak{a}}$. Если $\mathfrak{a}$ и $\mathfrak{b}$ — два дивизора, то, выбрав элементы $\gamma \neq 0$ и $\gamma' \neq 0$ так, чтобы дивизоры $(\gamma)\mathfrak{a}$ и $(\gamma')\mathfrak{b}$ были целыми, будем иметь (в силу теоремы 5 и формулы (7))

$$\gamma\gamma'\overline{\mathfrak{a}\mathfrak{b}} = \overline{(\gamma)\mathfrak{a} \cdot (\gamma')\mathfrak{b}} = \overline{(\gamma)\mathfrak{a}} \cdot \overline{(\gamma')\mathfrak{b}} = \gamma\overline{\mathfrak{a}} \cdot \gamma'\overline{\mathfrak{b}} = \gamma\gamma'\overline{\mathfrak{a}}\,\overline{\mathfrak{b}},$$

откуда $\overline{\mathfrak{a}\mathfrak{b}} = \overline{\mathfrak{a}}\,\overline{\mathfrak{b}}$. Отображение $\mathfrak{a} \to \overline{\mathfrak{a}}$ является, таким образом, изоморфизмом. Отсюда, в частности, следует, что все идеалы поля K относительно действия умножения образуют группу. Единичным элементом в этой группе будет кольцо $\mathfrak{O} = \overline{e}$. Для идеала $\overline{\mathfrak{a}}$ обратным будет идеал $\overline{\mathfrak{a}^{-1}}$.

Сформулируем полученное обобщение теоремы 5.

Теорема 6. *Пусть $\mathfrak{O}$ — дедекиндово кольцо с полем отношений K. Для каждого дивизора $\mathfrak{a}$ через $\overline{\mathfrak{a}}$ обозначим совокупность всех делящихся на $\mathfrak{a}$ элементов поля K. Отображение $\mathfrak{a} \to \overline{\mathfrak{a}}$ является изоморфизмом группы дивизоров поля K на группу идеалов поля K. Целые дивизоры при этом изоморфизме соответствуют целым идеалам, и обратно.*

Замечание. Дедекиндовы кольца допускают следующую абстрактную характеристику. Кольцо $\mathfrak{O}$ (коммутативное, с единицей и без делителей нуля) является дедекиндовым кольцом тогда и только тогда, когда оно 1) целозамкнуто, 2) нётерово (т. е. каждый идеал в $\mathfrak{O}$ допускает конечную систему образующих) и 3) каждый ненулевой простой идеал в $\mathfrak{O}$ максимален. Необходимость этих условий вытекает из теоремы 3 § 3, задачи 8 и теоремы 5 настоящего параграфа (см. также задачу 15). Относительно их достаточности см., например, книгу [5].

Задачи

1. Доказать, что кольцо $k[x]$ многочленов от одной переменной над произвольным полем k дедекиндово.

2. Пусть $\mathfrak{o}$ — дедекиндово кольцо и k — его поле отношений. Доказать, что целое замыкание $\mathfrak{O}$ кольца $\mathfrak{o}$ в произвольном конечном расширении поля k является также дедекиндовым кольцом.

3. Доказать, что кольцо, в котором имеется теория дивизоров с конечным числом простых дивизоров, дедекиндово.

4. Доказать, что в дедекиндовом кольце система сравнений

$$\xi \equiv \alpha_1 \pmod{\mathfrak{a}_1},$$
$$\cdots\cdots\cdots$$
$$\xi \equiv \alpha_m \pmod{\mathfrak{a}_m}$$

разрешима тогда и только тогда, когда $\alpha_i \equiv \alpha_j \pmod{\mathfrak{b}_{ij}}$, $i \neq j$, где $\mathfrak{b}_{ij}$ — общий наибольший делитель дивизоров $\mathfrak{a}_i$ и $\mathfrak{a}_j$.

5. Пусть $\mathfrak{O}$ — дедекиндово кольцо и $\mathfrak{a}$ — дивизор кольца $\mathfrak{O}$. Доказать, что совокупность тех классов вычетов из $\mathfrak{O}/\mathfrak{a}$, которые состоят из элементов, взаимно простых с $\mathfrak{a}$, относительно действия умножения образуют группу.

6. Доказать, что если $f(x)$ — многочлен степени m с коэффициентами из дедекиндова кольца $\mathfrak{O}$, не все коэффициенты которого делятся на простой дивизор $\mathfrak{p}$, то сравнение $f(x) \equiv 0 \pmod{\mathfrak{p}}$ имеет в $\mathfrak{O}$ не более m решений.

7. Пусть $\mathfrak{O}$ — дедекиндово кольцо, $\mathfrak{p}$ — простой дивизор кольца $\mathfrak{O}$ и $f(x)$ — многочлен с коэффициентами из $\mathfrak{O}$. Доказать, что если для элемента $\alpha \in \mathfrak{O}$ мы имеем

$$f(\alpha) \equiv 0 \pmod{\mathfrak{p}}, \qquad f'(\alpha) \not\equiv 0 \pmod{\mathfrak{p}},$$

то для любого $m \geqslant 2$ в кольце $\mathfrak{O}$ существует элемент ξ, для которого

$$f(\xi) \equiv 0 \pmod{\mathfrak{p}^m}, \qquad \xi \equiv \alpha \pmod{\mathfrak{p}}.$$

8. Доказать, что в дедекиндовом кольце всякий идеал либо является главным, либо порождается двумя элементами.

9. Пусть $\mathfrak{O}$ — дедекиндово кольцо с полем отношений K. Доказать, что при изоморфизме $\mathfrak{a} \to \bar{\mathfrak{a}}$ группы дивизоров поля K на группу идеалов поля K общему наименьшему кратному дивизоров соответствует пересечение идеалов, а общему наибольшему делителю дивизоров — сумма идеалов (под суммой $A + B$ идеалов A и B понимается совокупность всех сумм $\alpha + \beta$, где $\alpha \in A$, $\beta \in B$).

10. В кольце $\mathfrak{O} = k[x, y]$ многочленов от двух переменных над полем k разложение на простые множители однозначно и, значит, существует теория дивизоров. Доказать, что идеал $A = (x, y)$ кольца $\mathfrak{O}$, порожденный переменными x и y, не соответствует никакому дивизору.

11. Доказать, что если в кольце $\mathfrak{O}$ с теорией дивизоров $\mathfrak{O}^* \to \mathfrak{D}$ каждый ненулевой идеал имеет вид $\bar{\mathfrak{a}}$ (где $\mathfrak{a} \in \mathfrak{D}$), то это кольцо дедекиндово. В частности, кольцо главных идеалов дедекиндово (см. задачу 12 § 2).

12. Доказать, что если в кольце $\mathfrak{O}$ все ненулевые идеалы относительно действия умножения образуют полугруппу с однозначным разложением на простые множители, то это кольцо дедекиндово.

13. Пусть $\mathfrak{O}$ — дедекиндово кольцо и K — его поле отношений. Если A и B — идеалы поля K (относительно $\mathfrak{O}$), то под делимостью A на B понимают существование такого целого идеала C, что $A = BC$. Доказать, что делимость A на B имеет место тогда и только тогда, когда $A \subset B$.

14. Пусть $\mathfrak{O}$ — произвольное кольцо с теорией дивизоров и $\mathfrak{p}$ — простой дивизор кольца $\mathfrak{O}$. Доказать, что совокупность $\bar{\mathfrak{p}}$ всех элементов $\alpha \in \mathfrak{O}$, делящихся на $\mathfrak{p}$, является минимальным простым идеалом кольца $\mathfrak{O}$. (Идеал P кольца $\mathfrak{O}$ называется *простым*, если фактор-кольцо $\mathfrak{O}/P$ не имеет делителей нуля, т. е. если произведение двух элементов из $\mathfrak{O}$, не принадлежащих P, также не принадлежит P. Простой идеал P называется *минимальным*, если он не содержит других простых идеалов, кроме нулевого.)

15. Доказать, что в кольце $\mathfrak{O}$ с теорией дивизоров всякий ненулевой простой идеал P содержит простой идеал вида $\bar{\mathfrak{p}}$, где $\mathfrak{p}$ — некоторый простой дивизор кольца $\mathfrak{O}$.

16. Пусть $\mathfrak{O}$ — кольцо с теорией дивизоров и K — его поле отношений. Доказать, что для любого дивизора $\mathfrak{a}$ поля K (целого или дробного) идеал $\bar{\mathfrak{a}}$, состоящий из всех элементов поля K, делящихся на $\mathfrak{a}$, является d-идеалом (задача 5 § 4 Дополнения). Точнее, $\bar{\mathfrak{a}}$ есть пересечение двух главных идеалов поля K. Доказать, далее, обратное утверждение: для всякого d-идеала A поля K существует такой дивизор $\mathfrak{a}$ поля K, что $\bar{\mathfrak{a}} = A$. Таким образом, отображение $\mathfrak{a} \to \bar{\mathfrak{a}}$ является взаимно однозначным соответствием между всеми дивизорами $\mathfrak{a}$ и всеми d-идеалами A поля K.

17. Пусть $\mathfrak{N}$ — множество показателей поля K, определяющих теорию дивизоров для кольца $\mathfrak{O}$. Доказать, что если кольцо $\mathfrak{O}$ дедекиндово, то $\mathfrak{N}$ содержит все показатели ν поля K, для которых $\nu(\alpha) \geqslant 0$ при всех $\alpha \in \mathfrak{O}$. (Справедливо и обратное утверждение: если $\mathfrak{N}$ содержит все показатели ν поля K, для которых $\nu(\alpha) \geqslant 0$ при всех $\alpha \in \mathfrak{O}$, то кольцо $\mathfrak{O}$ дедекиндово.)

§ 7. Дивизоры в полях алгебраических чисел

1. Абсолютная норма дивизора. Согласно теореме 2 § 5 максимальный порядок $\mathfrak{O}$ произвольного поля алгебраических чисел K является кольцом с теорией дивизоров. Далее, в п. 1 § 6 мы видели, что кольцо вычетов $\mathfrak{O}/\mathfrak{p}$ по модулю простого дивизора $\mathfrak{p}$ является конечным полем, а значит, кольцо $\mathfrak{O}$ дедекиндово.

Рассмотрим поле алгебраических чисел K как расширение поля рациональных чисел $\mathbb{Q}$ (конечной степени). Так как дивизоры кольца $\mathbb{Z}$ целых рациональных чисел могут быть отождествлены с натуральными числами, то мы можем считать, что группа всех дивизоров (целых и дробных) поля $\mathbb{Q}$ совпадает с мультипликативной группой положительных рациональных чисел. В п. 2 § 5 было определено понятие нормы дивизора кольца $\mathfrak{O}$ относительно данного расширения K/k. В случае поля алгебраических чисел норму $N(\mathfrak{a}) = N_{K/\mathbb{Q}}(\mathfrak{a})$ дивизора $\mathfrak{a}$ порядка $\mathfrak{O}$ относительно расширения $K/\mathbb{Q}$ мы будем называть *абсолютной нормой* $\mathfrak{a}$. Распространим это понятие абсолютной нормы на дробные дивизоры, полагая

$$N\left(\frac{\mathfrak{m}}{\mathfrak{n}}\right) = \frac{N(\mathfrak{m})}{N(\mathfrak{n})}$$

для любых целых дивизоров $\mathfrak{m}$ и $\mathfrak{n}$. Ясно, что отображение $\mathfrak{a} \to N(\mathfrak{a})$ будет тогда гомоморфизмом группы всех дивизоров поля K в мультипликативную группу положительных рациональных чисел.

Абсолютная норма главного дивизора (ξ), $\xi \in K^*$, равна абсолютной величине нормы числа ξ:

$$N((\xi)) = |N(\xi)|. \tag{1}$$

Действительно, для целых ξ это совпадает с равенством (3) § 5. Если же $\xi = \alpha/\beta$ с целыми α и β, то

$$N((\xi)) = \frac{N((\alpha))}{N((\beta))} = \frac{|N(\alpha)|}{|N(\beta)|} = |N(\xi)|.$$

Степень инерции f простого дивизора $\mathfrak{p}$ поля K относительно $\mathbb{Q}$ называется *абсолютной степенью инерции* $\mathfrak{p}$ (или просто степенью). Индекс ветвления e дивизора $\mathfrak{p}$ относительно $\mathbb{Q}$ называется *абсолютным индексом ветвления* $\mathfrak{p}$.

Если $\mathfrak{p}$ является делителем простого рационального числа p и если $\mathfrak{p}$ имеет степень f, то согласно равенству (11) § 5

$$N(\mathfrak{p}) = p^f. \tag{2}$$

Пусть $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ — все простые дивизоры поля K, делящие p, и $e_1, \ldots, e_m$ — их индексы ветвления. Тогда для p в поле K имеем разложение $p = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_m^{e_m}$. По теореме 7 § 5 индексы

ветвления e_i связаны со степенями f_i дивизоров $\mathfrak{p}_i$ соотношением

$$f_1e_1 + \ldots + f_me_m = n = (K:\mathbb{Q}). \tag{3}$$

Теорема 1. *Абсолютная норма целого дивизора* $\mathfrak{a}$ *поля алгебраических чисел* K *равна числу классов вычетов в максимальном порядке* $\mathfrak{O}$ *по модулю* $\mathfrak{a}$.

Доказательство. Докажем сначала теорему для простого дивизора $\mathfrak{p}$. Пусть p — простое рациональное число, делящееся на $\mathfrak{p}$. Степень инерции f дивизора $\mathfrak{p}$ (согласно определению § 5, п. 3) равна степени поля вычетов $\Sigma_\mathfrak{p}$ показателя $v_\mathfrak{p}$ над полем вычетов Σ_p показателя v_p. Но Σ_p состоит, очевидно, из p элементов, поэтому $\Sigma_\mathfrak{p}$ есть конечное поле из p^f элементов. Нам достаточно, следовательно, показать, что поле вычетов $\mathfrak{O}/\mathfrak{p}$ изоморфно полю $\Sigma_\mathfrak{p}$, т. е. что при изоморфном вложении $\mathfrak{O}/\mathfrak{p} \to \Sigma_\mathfrak{p}$ поле $\mathfrak{O}/\mathfrak{p}$ отображается на все поле $\Sigma_\mathfrak{p}$. Для этого в свою очередь достаточно показать, что для любого $\xi \in K$, для которого $v_\mathfrak{p}(\xi) \geqslant 0$, существует такое $\alpha \in \mathfrak{O}$, что $v_\mathfrak{p}(\xi - \alpha) \geqslant 1$. Обозначим через $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ все те простые дивизоры поля K, для которых $v_{\mathfrak{q}_i}(\xi) = -k_i < 0$. По теореме 3 § 6 в порядке $\mathfrak{O}$ существует такой элемент γ, что

$$\gamma \equiv 1 \pmod{\mathfrak{p}}, \qquad \gamma \equiv 0 \pmod{\mathfrak{q}_i^{k_i}}, \qquad i = 1, \ldots, s.$$

Ясно, что $\alpha = \gamma\xi \in \mathfrak{O}$ и $v_\mathfrak{p}(\xi - \alpha) \geqslant 1$. В случае простого дивизора теорема 1, таким образом, доказана.

Для доказательства теоремы 1 в общем случае достаточно теперь показать, что если она справедлива для целых дивизоров $\mathfrak{a}$ и $\mathfrak{b}$, то она справедлива и для произведения $\mathfrak{ab}$. По условию 3) теоремы 4 § 3 в максимальном порядке $\mathfrak{O}$ существует такое число $\gamma \neq 0$, что $\mathfrak{a} | \gamma$ и дивизор $(\gamma)\mathfrak{a}^{-1}$ взаимно прост с $\mathfrak{b}$. Пусть $\alpha_1, \ldots, \alpha_r$ $(r = N(\mathfrak{a}))$ — полная система вычетов в кольце $\mathfrak{O}$ по модулю дивизора $\mathfrak{a}$, а $\beta_1, \ldots, \beta_s$ $(s = N(\mathfrak{b}))$ — полная система вычетов по модулю $\mathfrak{b}$. Покажем, что тогда rs чисел

$$\alpha_i + \beta_j\gamma \tag{4}$$

образуют полную систему вычетов по модулю $\mathfrak{ab}$. Пусть α — произвольное число из $\mathfrak{O}$. При некотором i $(1 \leqslant i \leqslant r)$

$$\alpha \equiv \alpha_i \pmod{\mathfrak{a}}.$$

Рассмотрим сравнение

$$\gamma\xi \equiv \alpha - \alpha_i \pmod{\mathfrak{ab}}. \tag{5}$$

Так как по выбору γ общий наибольший делитель дивизоров (γ) и $\mathfrak{ab}$ равен $\mathfrak{a}$ и $\alpha - \alpha_i$ делится на $\mathfrak{a}$, то по теореме 4 § 6 это сравнение имеет решение относительно числа $\xi \in \mathfrak{O}$. Если $\xi \equiv \beta_j \pmod{\mathfrak{b}}$ при некотором j $(1 \leqslant j \leqslant s)$, то $\gamma\xi \equiv \gamma\beta_j \pmod{\mathfrak{ab}}$.

Вместе с (5) это дает нам сравнение

$$\alpha \equiv \alpha_i + \gamma\beta_j \pmod{\mathfrak{ab}}.$$

Этим доказано, что в каждом классе вычетов по модулю $\mathfrak{ab}$ имеется представитель вида (4). Остается проверить, что числа (4) попарно не сравнимы между собой по модулю $\mathfrak{ab}$. Пусть

$$\alpha_i + \gamma\beta_j \equiv \alpha_k + \gamma\beta_l \pmod{\mathfrak{ab}}.$$

Так как это сравнение имеет место и по модулю $\mathfrak{a}$, то ввиду условия $\gamma \equiv 0 \pmod{\mathfrak{a}}$ получаем $\alpha_i \equiv \alpha_k \pmod{\mathfrak{a}}$, а значит, $i = k$, и мы получаем

$$\gamma(\beta_j - \beta_l) \equiv 0 \pmod{\mathfrak{ab}}. \tag{6}$$

Пусть простой дивизор $\mathfrak{p}$ входит в дивизоры $\mathfrak{a}$ и $\mathfrak{b}$ с показателями a и $b > 0$ соответственно. По условию $\nu_{\mathfrak{p}}(\gamma) = a$, поэтому из (6) следует, что $\nu_{\mathfrak{p}}(\beta_j - \beta_l) \geqslant b$. Так как это верно для любого простого дивизора $\mathfrak{p}$, входящего в $\mathfrak{b}$ с положительным показателем, то $\beta_j \equiv \beta_l \pmod{\mathfrak{b}}$, откуда $j = l$.

Таким образом, числа (4) действительно образуют полную систему вычетов по модулю $\mathfrak{ab}$. Число классов вычетов в кольце $\mathfrak{O}$ по модулю $\mathfrak{ab}$ равно, следовательно, $rs = N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{ab})$.

Теорема 1 доказана.

Как и в п. 3 § 6, для произвольного дивизора $\mathfrak{a}$ поля K (целого или дробного) через $\bar{\mathfrak{a}}$ обозначим соответствующий ему идеал поля K, состоящий из всех тех чисел $\alpha \in K$, которые делятся на $\mathfrak{a}$. Пусть число γ выбрано так, что $\gamma\bar{\mathfrak{a}} \subset \mathfrak{O}$. По следствию теоремы 2 § 2 гл. II совокупность $\gamma\bar{\mathfrak{a}}$ является модулем поля K (подмодулем кольца $\mathfrak{O}$). Но тогда идеал $\bar{\mathfrak{a}}$ также есть модуль поля K. Если $\alpha \in \bar{\mathfrak{a}}$, $\alpha \neq 0$ и $\omega_1, \ldots, \omega_n$ — базис кольца $\mathfrak{O}$, то все произведения $\alpha\omega_1, \ldots, \alpha\omega_n$ принадлежат $\bar{\mathfrak{a}}$, а значит, в $\bar{\mathfrak{a}}$ мы имеем $n = (K : \mathbb{Q})$ линейно независимых чисел поля K. Этим доказано, что идеал $\bar{\mathfrak{a}}$ для произвольного дивизора $\mathfrak{a}$ является полным модулем поля K. Его кольцом множителей будет, очевидно, максимальный порядок $\mathfrak{O}$. Обратно, если A — полный модуль поля K, кольцо множителей которого совпадает с максимальным порядком $\mathfrak{O}$, то для A будут выполнены все три условия определения идеала (см. § 6, п. 4). Таким образом, множество всех идеалов $\bar{\mathfrak{a}}$ совпадает с совокупностью всех полных модулей поля K, принадлежащих максимальному порядку $\mathfrak{O}$.

В п. 1 § 6 гл. II нами было введено понятие нормы полного модуля в поле алгебраических чисел. Можно говорить поэтому о норме идеалов $\bar{\mathfrak{a}}$. Покажем, что норма любого дивизора совпадает с нормой соответствующего ему идеала:

$$N(\mathfrak{a}) = N(\bar{\mathfrak{a}}). \tag{7}$$

Для целых дивизоров это следует из теоремы 1 настоящего параграфа и теоремы 1 § 6 гл. II. Если же дивизор $\mathfrak{a}$ дробный, то можем найти такое $\gamma \in K^*$, что дивизор $(\gamma^{-1})\mathfrak{a} = \mathfrak{b}$ будет целым. Тогда ввиду теоремы 2 § 6 гл. II мы будем иметь

$$N(\mathfrak{a}) = N(\mathfrak{b})|N(\gamma)| = N(\overline{\mathfrak{b}})|N(\gamma)| = N(\overline{\gamma}\overline{\mathfrak{b}}) = N(\overline{\gamma\mathfrak{b}}) = N(\overline{\mathfrak{a}}),$$

и формула (7) доказана для любых $\mathfrak{a}$.

В качестве одного из простейших приложений понятия нормы дадим более точную оценку для числа $\omega(a)$ неассоциированных чисел максимального порядка, нормы которых по абсолютной величине равны a (при доказательстве теоремы 5 § 2 гл. II нами была установлена оценка $\omega(a) \leqslant a^n$).

Обозначим через $\psi(a)$ число целых дивизоров с нормой a. Так как числа α и β ассоциированы тогда и только тогда, когда главные дивизоры (α) и (β) равны, то ввиду формулы (1) имеем

$$\omega(a) \leqslant \psi(a).$$

Займемся поэтому оценкой числа $\psi(a)$. Пусть $a = p_1^{k_1} \dots p_s^{k_s}$ с различными простыми числами p_i. Если $N(\mathfrak{a}) = a$, то $\mathfrak{a} = \mathfrak{a}_1 \dots \mathfrak{a}_s$, где $\mathfrak{a}_i$ состоит только из тех простых дивизоров $\mathfrak{p}$, которые являются делителями p_i. По формуле (2) и по мультипликативности нормы мы имеем $N(\mathfrak{a}_i) = p_i^{k_i}$, а значит, $\psi(a) = \psi(p_1^{k_1}) \dots \psi(p_s^{k_s})$. Нам достаточно поэтому получить оценку для $\psi(p^k)$. Пусть $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ — все простые дивизоры, делящие p, и пусть $f_1, \dots, f_m$ — их степени. В силу равенства

$$N(\mathfrak{p}_1^{x_1} \dots \mathfrak{p}_m^{x_m}) = p^{f_1 x_1 + \dots + f_m x_m}$$

задача сводится к оценке числа решений уравнения

$$f_1 x_1 + \dots + f_m x_m = k$$

относительно неотрицательных x_i. Так как, очевидно, $0 \leqslant x_i \leqslant k$, то число этих решений не превосходит $(k+1)^m$. Но $m \leqslant n = (K : \mathbb{Q})$, поэтому

$$\psi(a) \leqslant ((k_1 + 1) \dots (k_s + 1))^n.$$

Выражение в скобках справа равно, как известно, числу $\tau(a)$ всех делителей a. Мы получили, следовательно, оценку

$$\omega(a) \leqslant \psi(a) \leqslant (\tau(a))^n. \tag{8}$$

Для сравнения оценки (8) с нашей прежней оценкой $\omega(a) \leqslant a^n$ заметим, что при любом сколь угодно малом $\varepsilon > 0$ отношение $\tau(a)/a^\varepsilon$ стремится к нулю при $a \to \infty$.

2. Классы дивизоров. Определение. *Два дивизора $\mathfrak{a}$ и $\mathfrak{b}$ поля алгебраических чисел K называются эквивалентными, в обозначении $\mathfrak{a} \sim \mathfrak{b}$, если они различаются между собой на множи-*

тель, являющийся главным дивизором: $\mathfrak{a} = \mathfrak{b}(\alpha)$, $\alpha \in K^*$. *Совокупность всех дивизоров поля K, эквивалентных данному дивизору $\mathfrak{a}$, называется классом дивизоров и обозначается через* $[\mathfrak{a}]$.

В терминах теории групп эквивалентность $\mathfrak{a} \sim \mathfrak{b}$ означает, что дивизоры $\mathfrak{a}$ и $\mathfrak{b}$ принадлежат одному и тому же смежному классу группы всех дивизоров по подгруппе главных дивизоров. Класс дивизоров $[\mathfrak{a}]$ можно также определить, следовательно, как класс смежности по подгруппе главных дивизоров, содержащий $\mathfrak{a}$ в качестве представителя. Равенство классов $[\mathfrak{a}] = [\mathfrak{b}]$ равносильно, очевидно, эквивалентности $\mathfrak{a} \sim \mathfrak{b}$.

Для любых двух классов дивизоров $[\mathfrak{a}]$ и $[\mathfrak{b}]$ положим

$$[\mathfrak{a}] \cdot [\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}].$$

Легко проверяется, что так определенное произведение классов дивизоров не зависит от выбора представителей $\mathfrak{a}$ и $\mathfrak{b}$ в перемножаемых классах, а также что относительно этого действия умножения все классы образуют (коммутативную) группу — *группу классов дивизоров* поля K. Единичным элементом будет здесь, очевидно, класс $[\mathfrak{e}]$, состоящий из всех главных дивизоров. Для класса $[\mathfrak{a}]$ обратным будет класс $[\mathfrak{a}^{-1}]$.

В теоретико-групповых терминах группа классов дивизоров — это фактор-группа группы всех дивизоров по подгруппе главных дивизоров.

Группа классов дивизоров и, в частности, ее порядок — число классов дивизоров — являются важными арифметическими характеристиками поля алгебраических чисел K. Если число классов дивизоров равно 1, то это значит, что все дивизоры главные, а это в свою очередь эквивалентно тому, что в кольце целых чисел поля K имеет место однозначность разложения на простые множители (теорема 2 § 3). Таким образом, для однозначности разложения на множители необходимо и достаточно, чтобы число классов дивизоров было равно единице. Вопрос о том, однозначно ли разложение целых чисел поля K на простые множители, является, следовательно, частным случаем вопроса об определении числа классов дивизоров этого поля. Мы докажем сейчас, что оно всегда конечно.

Теорема 2. *Группа классов дивизоров любого поля алгебраических чисел конечна.*

Доказательство. Из определения эквивалентности дивизоров легко следует, что дивизоры $\mathfrak{a}$ и $\mathfrak{b}$ эквивалентны тогда и только тогда, когда соответствующие им идеалы $\bar{\mathfrak{a}}$ и $\bar{\mathfrak{b}}$ подобны (в смысле подобия модулей, см. п. 3 § 1 гл. II). Разбиению дивизоров на классы эквивалентных дивизоров соответствует, следовательно, разбиение идеалов поля K (т. е. полных модулей, для которых кольцом множителей является максимальный порядок — кольцо $\mathfrak{O}$ всех целых чисел поля K) на классы подобных идеалов. Но согласно теореме 3 § 6 гл. II число классов подобных моду-

лей с данным кольцом множителей конечно, поэтому конечным будет, в частности, число классов подобных идеалов, а значит, и число классов эквивалентных дивизоров.

Замечание 1. Теорема 2 нами получена как простое следствие теоремы 3 § 6 гл. II. Доказательство же последней теоремы было основано на применении геометрического метода, в частности на лемме Минковского о выпуклом теле. Таким образом, в конечном итоге доказательство теоремы 2 также опирается на лемму Минковского.

Замечание 2. Из доказательства теоремы 3 § 6 гл. II можно извлечь следующее уточнение теоремы 2. В каждом классе дивизоров поля алгебраических чисел K степени $n = s + 2t$ существует целый дивизор с нормой $\leqslant (2/\pi)^t \sqrt{|D|}$, где D — дискриминант поля K (т. е. дискриминант кольца всех целых чисел поля K). В самом деле, пусть $[\overline{\mathfrak{b}}]$ — произвольный класс дивизоров. Тогда для идеала $\overline{\mathfrak{b}^{-1}}$ существует подобный ему идеал $A = \alpha\overline{\mathfrak{b}^{-1}}$, для которого $A \supset \mathfrak{O}$ и $(A : \mathfrak{O}) \leqslant (2/\pi)^t \sqrt{|D|}$ (см. доказательство теоремы 3 § 6 гл. II). Так как идеал A содержит $\mathfrak{O}$, то соответствующий ему дивизор будет обратным для целого: $A = \overline{\mathfrak{a}^{-1}}$ с целым $\mathfrak{a}$. Из равенства $\overline{\mathfrak{a}^{-1}} = \alpha\overline{\mathfrak{b}^{-1}}$ следует, что $\mathfrak{a}(\alpha) = \mathfrak{b}$, т. е. целый дивизор $\mathfrak{a}$ содержится в классе $[\overline{\mathfrak{b}}]$, при этом (задача 2)

$$N(\mathfrak{a}) = N(\mathfrak{e})/N(\mathfrak{a}^{-1}) = (\overline{\mathfrak{a}^{-1}} : \overline{\mathfrak{e}}) = (A : \mathfrak{O}) \leqslant (2/\pi)^t \sqrt{|D|}.$$

Теорема 3. *Если число классов дивизоров поля K равно h, то h-я степень любого дивизора является главным дивизором.*

Доказательство. Утверждение теоремы является простым следствием элементарной теоремы теории групп, согласно которой порядок всякого элемента конечной группы является делителем порядка группы. Пусть $\mathfrak{a}$ — произвольный дивизор. Так как $[\mathfrak{a}]^h$ есть единичный элемент группы классов дивизоров, то $[\mathfrak{a}^h] = [\mathfrak{e}]$, а значит, дивизор $\mathfrak{a}^h$ главный.

Следствие. *Если число классов дивизоров h поля K не делится на простое число l и если дивизор $\mathfrak{a}^l$ главный, то $\mathfrak{a}$ также главный.*

Действительно, в силу условия существуют такие целые рациональные числа u и v, что $lu + hv = 1$. Так как дивизоры $\mathfrak{a}^l$ и $\mathfrak{a}^h$ главные (первый — по условию, а второй — по теореме 3), то $\mathfrak{a}^{lu}$ и $\mathfrak{a}^{hv}$ также главные. Но тогда главным будет и их произведение $\mathfrak{a}^{lu+hv} = \mathfrak{a}$.

Согласно задаче 20 любое поле алгебраических чисел K можно вложить в такое более широкое поле $\overline{K}$, что каждый дивизор поля K будет главным дивизором поля $\overline{K}$. Мы не можем, однако, утверждать, что главными будут все дивизоры поля $\overline{K}$: в поле $\overline{K}$ имеются свои дивизоры (не являющиеся образами дивизоров поля K, см. теорему 3 § 5), и они не обязаны быть главными.

Возникает поэтому вопрос, нельзя ли для данного поля K подыскать такое поле алгебраических чисел $\overline{K}$, чтобы $K \subset \overline{K}$ и чтобы $\overline{K}$ было одноклассным (для которого $h = 1$). В некоторых простейших случаях поле $\overline{K}$ может быть найдено. Например, неодноклассное поле $\mathbb{Q}(\sqrt{-5})$, с которым мы встретились в § 2 п. 3, содержится в поле $\mathbb{Q}(\sqrt{-5}, \sqrt{-1})$, которое одноклассно. Однако в общем случае ответ на поставленный вопрос оказывается отрицательным [43]. Более того, можно показать, что поле K заведомо нельзя погрузить в одноклассное поле, если только число простых делителей его дискриминанта больше некоторой границы, зависящей только от степени $(K : \mathbb{Q})$. Например, квадратичное поле $\mathbb{Q}(\sqrt{d})$ не погружаемо в одноклассное, если его дискриминант содержит не менее восьми различных простых чисел в случае $d > 0$ и содержит не менее шести различных простых чисел в случае $d < 0$. Существует также бесконечно много мнимых квадратичных полей, содержащих в своих дискриминантах четыре различных простых множителя и не погружаемых в одноклассные поля. Их примерами являются: $\mathbb{Q}(\sqrt{-13 \cdot 17 \cdot 43 \cdot 53})$, $\mathbb{Q}(\sqrt{-2 \cdot 23 \cdot 41 \cdot 73})$, $\mathbb{Q}(\sqrt{-17 \cdot 89 \cdot 257})$ (см. [14]). Известны также примеры [156] мнимых квадратичных полей $\mathbb{Q}(\sqrt{-p})$ с простым дискриминантом $D = -p$, не погружаемых в одноклассные поля, например, при $p = 4\,724\,490\,703$.

До сих пор открытым является вопрос о том, будет ли вообще число полей с $h = 1$ бесконечным, хотя обзор имеющихся таблиц и показывает, что такие поля встречаются сравнительно часто (см. таблицы для числа h вещественных квадратичных полей и вполне вещественных кубических полей).

Хотя для отдельных классов полей (например, для квадратичных и круговых полей, см. гл. V) формулы для числа классов дивизоров найдены, в общем случае о числе h и тем более о группе классов дивизоров известно очень мало. К числу немногих общих теорем о числе h относится теорема Зигеля — Брауэра, утверждающая, что для всех полей фиксированной степени n число классов дивизоров h, регулятор R и дискриминант D связаны между собой следующим асимптотическим соотношением (см. [15]):

$$\frac{\ln(h\mathrm{R})}{\ln\sqrt{|D|}} \to 1 \quad \text{при} \quad |D| \to \infty. \qquad (*)$$

Так как для мнимых квадратичных полей регулятор равен 1, то из (*) вытекает, что для этих полей $h \to \infty$ при $|D| \to \infty$. В частности, отсюда получаем, что мнимых квадратичных полей, для которых $h = 1$, имеется только конечное число. В пределах таблиц мы видим всего девять мнимых квадратичных полей с $h = 1$ (их дискриминанты равны -3, -4, -7, -8, -11, -19, -43, -67, -163). В настоящее время показано, что этими девятью полями

и исчерпываются все мнимые квадратичные поля с $h=1$. В общем случае на основании соотношения (*) мы почти ничего не можем сказать о поведении числа h, так как величина регулятора **R нам неизвестна.**

Интересно отметить, что предположение о конечности числа мнимых квадратичных полей с $h=1$ (в терминах бинарных квадратичных форм) было впервые высказано в 1801 г. Гауссом, который нашел указанные девять полей и проверил, что среди полей с $|D|<3000$ других нет. Долгое время вопрос оставался открытым и лишь в 1934 г. он был решен положительно. Именно, Хейльброн и Линфут аналитическими средствами доказали, что существует не более десяти мнимых квадратичных полей с $h=1$. Вопрос о том, существует ли десятое поле, получил название проблемы десятого дискриминанта. Эта проблема впервые была решена в 1952 г. Хегнером, использовавшим очень красивую связь теории мнимых квадратичных полей с модулярными функциями (см. [81]). Однако ввиду неясности изложения рассуждения Хегнера долгое время считались неубедительными. В 1967 г. Старк нашел новое доказательство отсутствия десятого поля [134]. Вскоре Дойринг [73] и Берч [62] внесли в рассуждения Хегнера полную ясность.

В самых общих чертах идея метода Хегнера заключается в следующем. Пусть $K=\mathbb{Q}(\sqrt{d})$, $d<0$,— одноклассное мнимое квадратичное поле, и пусть 1, ω — базис максимального порядка поля K (теорема 1 § 7 гл. II). Сначала рассматривается почти очевидный случай, когда в поле K простое число 2 разлагается в произведение двух простых дивизоров (различных или совпадающих). Ввиду предположенной одноклассности эти дивизоры главные, и поэтому $2=N(\alpha)$, где α — целое число из K. В зависимости от вида базиса это приводит нас к уравнениям

$$x^2+|d|y^2=2 \quad \text{или} \quad (2x+y)^2+|d|y^2=8,$$

которые должны быть разрешимы в целых числах. Ясно, что это возможно лишь при $d=-1, -2, -7$.

Далее предполагается, что число 2 остается простым в поле K, и рассматривается значение $j(\omega)$ абсолютного инварианта $j(z)$, о котором упоминалось в п. 7 § 7 гл. II, в точке ω. Это целое алгебраическое число. Так как поле K, по предположению, одноклассно, т. е. $h=1$, то $(\mathbb{Q}(j(\omega)):\mathbb{Q})=1$, а значит, $j(\omega)$ является целым рациональным числом. С другой стороны, ввиду основного свойства абсолютного инварианта значение $j(\omega)$ однозначно определяет ω с точностью до модулярной эквивалентности и тем самым однозначно определяет поле K.

Наряду с $j(z)$ рассматриваются также другие функции с аналогичными свойствами, и вследствие их алгебраической зависимости возникает уравнение $F(x, y)=0$, обладающее свойством: каждому одноклассному полю K соответствует решение этого

уравнения в целых числах, причем разным полям соответствуют разные решения. После некоторых преобразований уравнение приобретает вид

$$y^2 = 2x(x^3 + 1).$$

Уже давно было известно, что это уравнение имеет шесть решений:

$$(0, 0), \quad (1, 2), \quad (1, -2), \quad (-1, 0), \quad (2, 6), \quad (2, -6).$$

Из хода доказательства следует, что они соответствуют полям $K = \mathbb{Q}(\sqrt{d})$ с $d = -3, -11, -67, -19, -43, -163$. Поэтому других одноклассных полей K нет.

Самым удивительным является здесь, пожалуй, то, что уравнение $y^2 = 2x(x^3 + 1)$ не имеет других решений, кроме тех, которые соответствуют одноклассным полям. В связи с этим возникает следующее предположение. В алгебраической геометрии часто бывает, что некоторые объекты (рассматриваемые с точностью до естественного понятия изоморфизма) описываются такими параметрами, как точки алгебраических многообразий. Соответствующее алгебраическое многообразие называется тогда *многообразием модулей* объектов рассматриваемого типа. Например, в п. 7 § 7 гл. II мы видели, что поля эллиптических функций параметризуются множеством всех комплексных чисел. Следовательно, многообразием модулей полей эллиптических функций является комплексная прямая. Можно думать, что аналогичными средствами описываются также и некоторые теоретико-числовые объекты. Возможно, что в теории Хегнера мы и сталкиваемся с простейшим проявлением такого обстоятельства. Кривая с уравнением $y^2 = 2x(x^3 + 1)$ является с этой точки зрения *многообразием модулей для одноклассных мнимых квадратичных полей*. То же явление удалось обнаружить еще в одном, правда весьма специальном, случае двуклассных мнимых квадратичных полей с четным дискриминантом. Здесь также обнаруживается загадочное взаимно однозначное соответствие полей с целыми точками некоторых кривых (см. [88] и [40]). Было бы очень интересно попытаться обобщить теорию Хегнера в другом направлении, заменив поле рациональных чисел некоторым вполне вещественным полем.

Эффективные оценки для абсолютной величины дискриминантов всех мнимых квадратичных полей с числом классов $h = 2$ были получены в 1971 г. Бейкером [59] и Старком [135], [136]. Эти оценки привели к результату: для мнимого квадратичного поля $h = 2$ лишь при условии, что абсолютная величина дискриминанта поля не превосходит 427 (все такие поля можно найти, следовательно, в табл. 4 в конце книги). Недавно в работе [77] для числа классов h мнимого квадратичного поля дискриминанта

D получена оценка

$$h > c_\delta (\log |D|)^{1-\delta},$$

где $\delta > 0$ и c_δ — эффективно вычисляемая константа, зависящая только от δ. Таким образом, в принципе можно найти все дискриминанты D, для которых h не превосходит заданной величины. Однако приведенная оценка слишком завышена, чтобы с ее помощью можно было определить поля даже с $h = 3$, и трехклассные поля явно до сих пор не найдены (хотя гипотетически $h = 3$ лишь при $|D| \leqslant 907$).

3. Приложение к теореме Ферма. Результаты предыдущих пунктов дают возможность доказать справедливость теоремы 1 § 1 для значительно более широкого класса показателей l.

Теорема 4. *Пусть l — простое нечетное число и ζ — первообразный корень степени l из 1. Если число классов дивизоров поля $\mathbb{Q}(\zeta)$ не делится на l, то для показателя l справедлив первый случай теоремы Ферма.*

Доказательство. Предположим, что вопреки утверждению теоремы существуют целые рациональные x, y, z, не делящиеся на l и удовлетворяющие уравнению

$$x^l + y^l = z^l.$$

Можно считать, конечно, что x, y и z попарно взаимно просты. В кольце целых чисел поля $\mathbb{Q}(\zeta)$ наше равенство может быть записано в виде

$$\prod_{k=0}^{l-1} (x + \zeta^k y) = z^l.$$

Так как $x + y \equiv x^l + y^l = z^l \equiv z \pmod{l}$ и z не делится на l, то $x + y$ также не делится на l. А тогда, как это мы видели при доказательстве леммы 5 § 1, при $m \not\equiv n \pmod{l}$ в кольце $\mathbb{Z}[\zeta]$ существуют такие числа ξ_0 и η_0, что

$$(x + \zeta^n y)\xi_0 + (x + \zeta^m y)\eta_0 = 1.$$

Следовательно, главные дивизоры $(x + \zeta^k y)$ $(k = 0, 1, \ldots, l-1)$ попарно взаимно просты. Так как их произведение есть l-я степень (дивизора (z)), то каждый из этих дивизоров в отдельности должен быть l-й степенью. В частности,

$$(x + \zeta y) = \mathfrak{a}^l,$$

где $\mathfrak{a}$ — целый дивизор поля $\mathbb{Q}(\zeta)$. По условию число классов дивизоров поля $\mathbb{Q}(\zeta)$ не делится на l, следовательно, по следствию теоремы 3 дивизор $\mathfrak{a}$ главный, т. е. $\mathfrak{a} = (\alpha)$, где α принадлежит максимальному порядку $\mathfrak{O} = \mathbb{Z}[\zeta]$ поля $\mathbb{Q}(\zeta)$. Из равенства

$$(x + \zeta y) = (\alpha^l)$$

следует теперь, что $x+\zeta y=\varepsilon\alpha^l$, где ε — единица кольца $\mathfrak{O}$. Аналогичным образом мы получим также

$$x-\zeta z=\varepsilon_1\alpha_1^l$$

($\alpha_1\in\mathfrak{O}$, ε_1 — единица в $\mathfrak{O}$). Мы получили равенства, которые, как было показано в п. 3 § 1, ведут к противоречию (в этой части доказательства теоремы 1 § 1 однозначностью разложения мы уже не пользовались). Теорема 4, таким образом, доказана.

Те простые нечетные числа l, для которых число классов дивизоров поля $\mathbb{Q}(\zeta)$, $\zeta^l=1$, не делится на l, называются регулярными, а все остальные — иррегулярными. Теорема 4 устанавливает, стало быть, справедливость первого случая теоремы Ферма для всех регулярных показателей l. В § 7 гл. V мы докажем, что для регулярных l справедлив также и второй случай теоремы Ферма. Таким образом, теорема Ферма справедлива для всех регулярных простых показателей l. Этот результат был получен Куммером в 1850 г.

Чтобы теорему Куммера (в частности, теорему 4) можно было применить к конкретным простым числам l, надо, разумеется, иметь еще критерий, позволяющий узнавать, является ли данное l регулярным или нет. Такой критерий также был найден Куммером. При помощи очень красивых теоретико-числовых и аналитических соображений Куммер доказал, что простое нечетное число l регулярно тогда и только тогда, когда ни один из числителей чисел Бернулли B_2, B_4, ..., B_{l-3} (в несократимой записи) не делится на l (определение чисел Бернулли и некоторые их свойства приведены в § 8 гл. V; доказательство сформулированного критерия Куммера будет приведено в п. 4 § 6 гл. V). При помощи этого критерия можно убедиться, что среди простых чисел <100 только три числа иррегулярны, а именно 37, 59 и 67, все же остальные регулярны. Теорема 4, как видим, охватывает более широкий класс показателей l по сравнению с теоремой 1 § 1 (см. замечание 4 в конце § 1).

В своей первой работе Куммер высказал предположение, что число иррегулярных простых чисел конечно. В более поздней работе он от него отказался и предположил, что регулярных чисел в среднем (на достаточно большом промежутке) в два раза больше, чем иррегулярных. Сейчас при помощи электронных вычислительных машин показано [142], что среди 11 733 нечетных простых чисел $<125\,000$ имеется 7 128 регулярных и 4 605 иррегулярных (в конце книги в табл. 11 приведены все иррегулярные простые числа <8000). В 1915 г. Иенсен довольно просто доказал (см. п. 2 § 7 гл. V), что число иррегулярных простых чисел бесконечно. Однако до сих пор неизвестно (и это представляется весьма трудной проблемой), является ли бесконечным число регулярных простых чисел. В 1964 г. Зигель выдвинул гипотезу [129], что отношение числа регулярных простых чисел к числу

всех простых чисел при увеличении рассматриваемого промежутка стремится к пределу $1/\sqrt{e}$, где e — основание натуральных логарифмов. Таким образом, если гипотеза верна, то на любом достаточно большом промежутке около 61% простых чисел должны быть регулярными. Последний факт весьма хорошо согласуется с табличными данными.

Отметим здесь некоторые другие факты, относящиеся к первому случаю теоремы Ферма. В 1909 г. Виферих доказал [145], что первый случай теоремы Ферма справедлив для всех тех простых l, для которых

$$2^{l-1} \not\equiv 1 \pmod{l^2}.$$

Чтобы показать, насколько сильным является этот замечательный результат, заметим, что среди простых чисел $l < 6 \cdot 10^9$ только два числа: 1093 и 3511 — удовлетворяют сравнению $2^{l-1} \equiv 1 \pmod{l^2}$, см. [95]. Неизвестно, однако, конечно или бесконечно число таких l. Несколько позже Мириманов доказал [110], что первый случай теоремы Ферма справедлив и для тех l, для которых $3^{l-1} \not\equiv 1 \pmod{l^2}$. И здесь проведенные в последнее время вычисления [128] показали, что среди простых $l < 2^{30}$ имеется лишь два числа $l = 11$ и $l = 1\,006\,003$, для которых $3^{l-1} \equiv 1 \pmod{l^2}$.

На основе критериев Вифериха и Мириманова можно констатировать, что первый случай теоремы Ферма справедлив для всех показателей $l < 6 \cdot 10^9$.

Впоследствии утверждения типа: первый случай теоремы Ферма справедлив для простого показателя l, если $q^{l-1} \not\equiv 1 \pmod{l^2}$, — были установлены и для последующих простых чисел $q \leqslant 31$.

В 1965 г. Эйхлер [75] получил следующий критерий. Пусть G — группа классов дивизоров l-кругового поля $\mathbb{Q}(\zeta)$. При иррегулярном l фактор-группа G/G^l есть элементарная абелева l-группа порядка l^γ, $\gamma \geqslant 1$. Если $\gamma = \gamma(l) < \sqrt{l} - 2$, то для l справедлив первый случай теоремы Ферма (частный случай этого утверждения, когда $\gamma = 1$, был получен также в работе [133]). Брюкнер в статье [67] придал критерию Эйхлера более удобную для практического использования форму, связав число γ с *индексом иррегулярности* $ii(l)$ числа l, т. е. с числом тех чисел Бернулли $B_2, B_4, \ldots, B_{l-3}$, числители которых делятся на l. Именно, им доказано, что первый случай теоремы Ферма справедлив, если

$$ii(l) < \sqrt{l} - 2.$$

Отметим еще один результат. Для простого $l \geqslant 47$ положим $\mu = \max\{22, [\sqrt[3]{\ln l}]\}$. Согласно статьям [152] и [154] для показателя l справедлив первый случай теоремы Ферма, если числитель хоть одного из чисел Бернулли B_{l-1-2i}, где $i = 1, 2, \ldots, \mu$, не делится на l (см. также [157]). О недавних достижениях см. [159], [160], [161] (см. «Добавление при корректуре» на с. 279).

В заключение пункта обратим внимание на следующее любопытное обстоятельство, отмеченное в [144]. Числа 1092 и 3510 в двоичной системе исчисления имеют запись:

$$1092 = 0100\,0100\,0100,$$
$$3510 = 110\,110\,110\,110.$$

В обоих случаях мы видим загадочную закономерность в расположении двоичных знаков. Не имеет ли связи этот феномен с тем, что простые числа $l = 1093$ и $l = 3511$ удовлетворяют сравнению $2^{l-1} \equiv 1 \pmod{l^2}$?

4. **Вопросы эффективности.** До сих пор мы обходили молчанием вопрос о фактическом построении дивизоров для данного поля алгебраических чисел K. Так как произвольные дивизоры вполне определяются заданием всех простых дивизоров, а последние в свою очередь определяются показателями поля K, то наш вопрос сводится к эффективному построению всех продолжений на поле K показателя ν_p поля $\mathbb{Q}$ для каждого фиксированного p. Кроме перечисления простых дивизоров важно также иметь финитный алгоритм для вычисления числа h классов дивизоров поля K. Только в этом случае, например, результаты предшествующего пункта, относящиеся к теореме Ферма, будут иметь реальную ценность.

В этом пункте мы покажем, что как построение продолжений показателя ν_p, так и вычисление числа h осуществляются в конечное число действий.

Пусть $\mathfrak{o}_p$ — кольцо показателя ν_p в поле $\mathbb{Q}$ (т. е. кольцо p-целых рациональных чисел, см. п. 2 § 3 гл. I) и $\mathfrak{D}_p$ — его целое замыкание в поле K. Каждое число $\xi \in \mathfrak{D}_p$ является корнем многочлена $t^k + a_1 t^{k-1} + \ldots + a_k$ с p-целыми коэффициентами a_i. Если через m мы обозначим общий знаменатель всех a_i, то число $m\xi = \alpha$ будет корнем многочлена $t^k + ma_1 t^{k-1} + \ldots + m^k a_k$ уже с коэффициентами из $\mathbb{Z}$, т. е. будет принадлежать кольцу $\mathfrak{O}$ всех целых чисел поля K (максимальному порядку). Справедливо, очевидно, и обратное утверждение: если $\alpha \in \mathfrak{O}$ и целое рациональное m не делится на p, то $\alpha/m \in \mathfrak{D}_p$. Таким образом, кольцо $\mathfrak{D}_p$ совпадает с совокупностью чисел вида α/m, где $\alpha \in \mathfrak{O}$ и целое рациональное m не делится на p. Выберем какой-нибудь фундаментальный базис $\omega_1, \ldots, \omega_n$ поля K (т. е. базис кольца $\mathfrak{O}$ над $\mathbb{Z}$). Тогда по доказанному число $\xi \in K$, записанное в виде

$$\xi = a_1\omega_1 + \ldots + a_n\omega_n, \quad a_i \in \mathbb{Q},$$

будет принадлежать кольцу $\mathfrak{D}_p$ тогда и только тогда, когда все a_i будут p-целыми.

В силу теоремы 7 § 4 наша первая задача (т. е. построение продолжений показателя ν_p) сводится к нахождению полной системы попарно не ассоциированных простых элементов $\pi_{i_1}, \ldots, \pi_{i_m}$

кольца $\mathfrak{O}_p$. Действительно, если простые элементы π_i будут найдены, то для всякого $\xi \in \mathfrak{O}_p^*$ мы легко сможем найти разложение

$$\xi = \eta \pi_1^{k_1} \dots \pi_m^{k_m}, \tag{9}$$

где η — единица в $\mathfrak{O}_p$. Для этого надо делить ξ последовательно на каждый из π_i до тех пор, пока частное не будет принадлежать кольцу $\mathfrak{O}_p$; на некотором шаге мы получим в частном число η, которое уже не будет делиться ни на один из простых элементов π_i, а значит, будет единицей в $\mathfrak{O}_p$. Так как каждый элемент из K является отношением двух элементов из $\mathfrak{O}_p$ (даже из $\mathfrak{O}$), то представление вида (9) мы сможем найти и для любого $\xi \in K^*$. Но это и определяет все показатели $\nu_1, \dots, \nu_m$ на K, которые являются продолжениями ν_p. Индексы ветвления $e_1, \dots, e_m$ этих показателей определяются, как мы знаем, разложением $p = \varepsilon \pi_1^{e_1} \dots \pi_m^{e_m}$ (ε — единица в $\mathfrak{O}_p$).

Пусть π — произвольный простой элемент кольца $\mathfrak{O}_p$. Так как целые рациональные числа, не делящиеся на p, являются единицами в $\mathfrak{O}_p$, то можно считать, что $\pi \in \mathfrak{O}$. При любом $\alpha \in \mathfrak{O}$ число $\pi + p^2\alpha = \pi\left(1 + \frac{p^2}{\pi}\alpha\right)$ будет ассоциировано с π, так как множитель $1 + \frac{p^2}{\pi}\alpha$ принадлежит $\mathfrak{O}_p$ и не делится ни на один из простых элементов $\pi_1, \dots, \pi_m$. Таким образом, полный набор попарно не ассоциированных простых элементов в $\mathfrak{O}_p$ мы можем выбрать из системы чисел

$$x_1\omega_1 + \dots + x_n\omega_n,$$

где $0 \leqslant x_i < p^2$ ($i = 1, \dots, n$). Так как число чисел в этой системе конечно, то искомый набор простых элементов будет найден в конечном числе действий и тем самым будут определены показатели $\nu_1, \dots, \nu_m$.

Для нахождения степеней $f_1, \dots, f_m$ простых дивизоров $\mathfrak{p}_1, \dots, \mathfrak{p}_m$, соответствующих найденным показателям $\nu_1, \dots, \nu_m$, можно воспользоваться теоремой 5 § 5. Согласно этой теореме для каждого простого элемента $\pi_i \in \mathfrak{O}$ кольца $\mathfrak{O}_p$ мы имеем

$$N(\pi_i) = p^{f_i}a,$$

где целое рациональное a не делится на p. Степень f_i простого дивизора $\mathfrak{p}_i$ равна, следовательно, показателю степени, с которым p входит в целое рациональное число $N(\pi_i)$.

Перейдем ко второму нашему вопросу — об эффективном вычислении числа h классов дивизоров.

В замечании 2 к теореме 2 было отмечено, что в каждом классе дивизоров имеется целый дивизор $\mathfrak{a}$, для которого

$$N(\mathfrak{a}) \leqslant (2/\pi)^t \sqrt{|D|} \tag{10}$$

(см. по этому поводу также задачу 9). Пусть

$$\mathfrak{a}_1, \ldots, \mathfrak{a}_N \tag{11}$$

— все целые дивизоры поля K, удовлетворяющие условию (10). Число таких дивизоров конечно, так как в K имеется, очевидно, лишь конечное число целых дивизоров с данной нормой (при фиксированном a из равенства $N(\mathfrak{p}_1^{k_1} \ldots \mathfrak{p}_r^{k_r}) = a$ легко следует ограниченность и простых чисел p, делящихся на $\mathfrak{p}_i$, и положительных показателей k_i). Для определения числа классов дивизоров нам надо из системы (11) выделить максимальную подсистему попарно неэквивалентных дивизоров. Чтобы проделать это практически, надо уметь для каждых двух дивизоров решить вопрос, эквивалентны они или нет. Пусть $\mathfrak{a}$ и $\mathfrak{b}$ — два целых дивизора. Выберем в K число $\beta \neq 0$, делящееся на $\mathfrak{b}$, и рассмотрим дивизор $\mathfrak{a}\mathfrak{b}^{-1}(\beta)$. Дивизоры $\mathfrak{a}$ и $\mathfrak{b}$ эквивалентны тогда и только тогда, когда целый дивизор $\mathfrak{a}\mathfrak{b}^{-1}(\beta)$ будет главным. Таким образом, нам надо уметь узнавать, будет ли главным данный целый дивизор.

Обозначим норму целого дивизора $\mathfrak{a}$ через a. В п. 4 § 5 гл. II было показано, что в максимальном порядке $\mathfrak{O}$ мы можем в конечное число действий найти конечную систему чисел

$$\alpha_1, \ldots, \alpha_r \tag{12}$$

с нормой $\pm a$, обладающую тем свойством, что всякое $\alpha \in \mathfrak{O}$ с нормой $\pm a$ ассоциировано с одним из чисел этой системы. Если дивизор $\mathfrak{a}$ главный, т. е. $\mathfrak{a} = (\alpha)$, $\alpha \in \mathfrak{O}^*$, то $|N(\alpha)| = a$, а потому при некотором i $(1 \leqslant i \leqslant r)$ будем иметь $\mathfrak{a} = (\alpha_i)$. Таким образом, если система (12) уже найдена, то для решения вопроса, является ли дивизор $\mathfrak{a}$ главным, надо только проверить, не совпадает ли он с одним из главных дивизоров $(\alpha_1), \ldots, (\alpha_r)$.

Этим и доказано, что задача вычисления числа h для данного поля K решается в конечное число действий.

Разложение простого рационального числа p на простые дивизоры в ряде случаев удается довольно просто найти на основе рассмотрения норм k-членных чисел $(k \geqslant 2)$. Для изложения этого приема нам необходимо одно вспомогательное утверждение.

Пусть θ — целое примитивное число поля алгебраических чисел K степени n. Индекс порядка $\mathfrak{O}' = \{1, \theta, \ldots, \theta^{n-1}\}$ в максимальном порядке $\mathfrak{O}$ называется *индексом* числа θ.

Лемма. *Если простой дивизор $\mathfrak{p}$ не является делителем индекса k числа θ, то всякое целое число $\alpha \in K$ сравнимо по модулю $\mathfrak{p}$ с числом из порядка $\mathfrak{O}' = \{1, \theta, \ldots, \theta^{n-1}\}$.*

Действительно, так как $\mathfrak{p} \nmid k$, то $kx \equiv 1 \pmod{\mathfrak{p}}$ при целом x. Положим $\gamma = kx\alpha$. Поскольку $k\alpha \in \mathfrak{O}'$, то и $\gamma \in \mathfrak{O}'$, при этом $\alpha \equiv \gamma \pmod{\mathfrak{p}}$.

Следствие. *Если $\mathfrak{p}$ не является делителем дискриминанта $D' = D(1, \theta, \ldots, \theta^{n-1})$, то всякое целое $\alpha \in K$ сравнимо по модулю $\mathfrak{p}$ с числом из порядка $\mathfrak{O}' = \{1, \theta, \ldots, \theta^{n-1}\}$.*

Действительно, если $\mathfrak{p}$ не делит D', то $\mathfrak{p}$ не делит также и индекса k числа θ, что следует из формулы $D' = Dk^2$, где D — дискриминант поля K (лемма 1 § 6 гл. II и равенство (12) § 2 Дополнения).

Предположим теперь, что простое рациональное число p не входит в индекс целого числа $\theta \in K$. Пусть $\mathfrak{p}$ — простой дивизор степени f, делящий p, и $\overline{\theta}$ — класс вычетов по модулю $\mathfrak{p}$, содержащий θ. По лемме поле вычетов $\mathfrak{O}/\mathfrak{p}$ порождается классом вычетов $\overline{\theta}$ с представителем θ. Если поэтому $x_1, \ldots, x_f$ независимо друг от друга пробегают полную систему вычетов по модулю p (в кольце $\mathbb{Z}$), то среди чисел

$$\gamma = x_1 + x_2\theta + \ldots + x_f\theta^{f-1} + \theta^f$$

имеется одно и только одно, делящееся на $\mathfrak{p}$. Вычислив нормы $N(\gamma)$, мы легко можем выделить те γ, которые делятся на простые дивизоры, входящие в p. Если, например, при $f = 1$ мы нашли s чисел γ, нормы которых делятся на p точно в первой степени, то этим мы обнаружили s простых дивизоров первой степени, входящих в p. Предположим, что все простые дивизоры первой степени, входящие в p, уже найдены (набором чисел $\beta_1, \ldots, \beta_u$ с нормами pa_i, $p \nmid a_i$). Взяв $f = 2$, выделим те числа γ, норма которых делится на p^2. Делением на найденные β_i мы можем освободить эти γ от простых дивизоров первой степени, и если после этого $N(\gamma) = p^2 b/c$, $(bc, p) = 1$, то γ содержит простой дивизор второй степени. Если таким путем нам удалось найти все простые дивизоры второй степени, входящие в p, то берем $f = 3$ и т. д. Конечно, при большой степени n и на этом пути объем вычислений, вообще говоря, будет большим, но, например, при $n = 3$ или $n = 4$ мы часто приходим к цели довольно быстро. Некоторые уточнения к изложенному приему указаны в задачах 25—27.

Пример 1. Найдем разложения чисел 2, 3, 5, 7 в произведение простых дивизоров в поле пятой степени $\mathbb{Q}(\theta)$, $\theta^5 = 2$. Дискриминант D $(1, \theta, \theta^2, \theta^3, \theta^4)$ равен $2^{15}5^5$, поэтому в индекс числа θ могут входить лишь простые числа 2 и 5. Но число 2 не входит в индекс согласно задаче 15. Так как $\theta^5 = 2$, то $\mathfrak{p}_2 = (\theta)$ является простым дивизором первой степени, и мы имеем разложение

$$2 = \mathfrak{p}_2^5.$$

Из равенств

$$N(\theta) = 2, \quad N(\theta + 1) = 3, \quad N(\theta - 1) = 1 \tag{13}$$

следует, что в разложение числа 3 входит только один простой дивизор первой степени, именно $\mathfrak{p}_3 = (\theta + 1)$, при этом $\mathfrak{p}_3^2 \nmid 3$ по теореме 8 § 5. Далее,

$$N(\theta + 2) = 2 \cdot 17, \quad N(\theta - 2) = -2 \cdot 3 \cdot 5. \tag{14}$$

Второе из этих равенств говорит о том, что для числа 5 имеется простой дивизор $\mathfrak{p}_5$ первой степени, при этом ввиду делимости $\theta-2=(\theta+1)-3$ на $\mathfrak{p}_3$ для $\theta-2$ имеем разложение $(\theta-2)=\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$. Число $\theta-2$ удовлетворяет уравнению

$$(\theta-2)^5+10(\theta-2)^4+40(\theta-2)^3+80(\theta-2)^2+80(\theta-2)+30=0.$$

Согласно задаче 9 § 5 для числа 5 мы имеем, следовательно, разложение $5=\mathfrak{p}_5^5$. Результат задачи 15 показывает также, что 5 не входит в индекс числа θ, а значит, кольцо целых чисел поля $\mathbb{Q}(\theta)$ совпадает с порядком $\{1, \theta, \theta^2, \theta^3, \theta^4\}$.

Присоединим к (13) и (14) равенства

$$N(\theta+3)=5\cdot 7^2, \quad N(\theta-3)=-241.$$

На основании выписанных семи значений норм определенного вывода о простых дивизорах первой степени, входящих в число 7, сделать еще нельзя. Могут представиться три возможности: число $\theta+3$ делится либо на квадрат простого дивизора первой степени, либо на произведение двух различных простых дивизоров первой степени, либо на простой дивизор второй степени. Но для числа $\theta-4=(\theta+3)-7$ мы имеем $N(\theta-4)=-2\cdot 7\cdot 73$, поэтому имеет место первая возможность, а значит, в число 7 входит один (и только один) простой дивизор первой степени $\mathfrak{p}_7$, причем $\mathfrak{p}_7^2 \nmid 7$.

Чтобы выяснить, входят ли в 3 и 7 простые дивизоры второй степени, обратимся к нормам трехчленных чисел $\theta^2+\theta x+y$. Мы имеем

$$N(\theta^2+x\theta+y)=2x^5+y^5-10x^3y+10xy^2+4. \qquad (15)$$

Придавая x и y значения 0, 1, -1, мы получим девять чисел, среди которых ни одно не делится на 9. Это значит, что среди простых дивизоров, делящих 3, нет дивизоров второй степени. Формула (3) для разложения числа 3 оставляет теперь только одну возможность: $3=\mathfrak{p}_3\mathfrak{p}_3'$, где $\mathfrak{p}_3'$ — простой дивизор четвертой степени. Если для x и y в (15) мы возьмем значения 0, ± 1, ± 2, ± 3, то из 49 получающихся чисел только одно будет делиться на 7^2:

$$N(\theta^2+2\theta-3)=5\cdot 7^2.$$

Но $\theta^2+2\theta-3=(\theta+3)(\theta-1)$, поэтому мы имеем здесь квадрат дивизора $\mathfrak{p}_7$, так что и для 7 разложение будет иметь вид $7=\mathfrak{p}_7\mathfrak{p}_7'$, где $\mathfrak{p}_7'$ — простой дивизор четвертой степени.

Пример 2. Рассмотрим кубическое поле $\mathbb{Q}(\theta)$, $\theta^3-9\theta-6=0$. Так как $D(1, \theta, \theta^2)=3^5\cdot 2^3$, то ввиду задачи 15 в индекс числа θ входит, возможно, лишь 2 (можно показать, что порядок $\{1, \theta, \theta^2\}$ максимальный, но мы этим пользоваться не будем). По задаче 9 § 5 для числа 3 имеет место разложение $3=\mathfrak{p}_3^3$. Из

равенств

$$N(\theta)=6, \quad N(\theta+1)=-2, \quad N(\theta-1)=14 \tag{16}$$

заключаем, что в число 2 входят по крайней мере два различных простых дивизора первой степени $\mathfrak{p}_2$ и $\mathfrak{p}_2'$:

$$(\theta)=\mathfrak{p}_2\mathfrak{p}_3, \quad (\theta-1)=\mathfrak{p}_2'\mathfrak{p}_7 \tag{17}$$

(утверждать, что только два, можно было бы в том случае, если бы было известно, что порядок $\{1, \theta, \theta^2\}$ максимальный и, значит, 2 не входит в индекс числа θ). Но ввиду равенства

$$(\theta-1)^3+3(\theta-1)^2-6(\theta-1)-14=0$$

число 2 делится на $\mathfrak{p}_2'^2$, следовательно,

$$2=\mathfrak{p}_2\mathfrak{p}_2'^2, \quad (\theta+1)=\mathfrak{p}_2'. \tag{18}$$

Нормы (16), а также

$$N(\theta+2)=-4, \quad N(\theta-2)=16 \tag{19}$$

все не делятся на 5. Это означает, что в 5 не входят простые дивизоры первой степени. В случае кубического поля отсюда следует, что главный дивизор 5 является простым. Чтобы найти разложение числа 7, надо помимо (16) и (19) рассмотреть еще нормы

$$N(\theta+3)=6, \quad N(\theta-3)=6.$$

Так как среди этих семи значений имеется только одно, делящееся на 7, то в 7 входит ровно один простой дивизор первой степени. Приняв во внимание, что $\mathfrak{p}_7^2 \nmid 7$, можем написать разложение $7=\mathfrak{p}_7\mathfrak{p}_7'$, где $\mathfrak{p}_7'$ — простой дивизор второй степени.

В процессе разложения простых рациональных чисел в произведение простых дивизоров с помощью рассмотренного нами метода, основанного на изучении значений норм целых чисел, одновременно мы получаем ряд эквивалентностей между дивизорами. Эти эквивалентности позволяют значительно уменьшить число дивизоров в системе (11), из которой должна быть выделена максимальная подсистема попарно неэквивалентных дивизоров для определения числа классов h, а иногда и получить эту максимальную подсистему. Так, в примере 2 в связи с результатом задачи 9 система (11) состоит из целых дивизоров с нормой $\leqslant \frac{3!}{3^3}\sqrt{3^5\cdot 2^3}<10$, т. е. из дивизоров

$$\begin{gathered}1, \quad \mathfrak{p}_2, \quad \mathfrak{p}_2', \quad \mathfrak{p}_3, \quad \mathfrak{p}_2^2, \quad \mathfrak{p}_2'^2, \quad \mathfrak{p}_2\mathfrak{p}_2', \quad \mathfrak{p}_2\mathfrak{p}_3, \quad \mathfrak{p}_2'\mathfrak{p}_3, \quad \mathfrak{p}_7, \\ \mathfrak{p}_2^3, \quad \mathfrak{p}_2^2\mathfrak{p}_2', \quad 2, \quad \mathfrak{p}_2'^3, \quad \mathfrak{p}_3^2.\end{gathered} \tag{20}$$

Но из (18) следует, что $\mathfrak{p}_2'^2 \sim 1$ и $\mathfrak{p}_2 \sim 1$ (1 — единичный дивизор), а затем из (17) и $(\theta+3) = \mathfrak{p}_2'\mathfrak{p}_3$, — что $\mathfrak{p}_3 \sim 1$, $\mathfrak{p}_2' \sim 1$, $\mathfrak{p}_7 \sim 1$. Таким образом, все дивизоры системы (20) главные, а потому для поля $\mathbb{Q}(\theta)$, $\theta^3 - 9\theta - 6 = 0$, число h равно 1.

Иногда (при малых дискриминантах) система дивизоров (11) состоит только из единичного дивизора. В этих случаях мы без вычислений получаем, что $h = 1$. Так, например, для поля $\mathbb{Q}(\theta)$, $\theta^3 - \theta - 1 = 0$, дискриминант базиса 1, θ, θ^2 равен -23, поэтому согласно задаче 8 § 2 гл. II этот базис фундаментальный и -23 является дискриминантом поля. Согласно задаче 9 в каждом классе дивизоров поля $\mathbb{Q}(\theta)$ имеется целый дивизор с нормой $\leqslant \frac{4}{\pi}\frac{3!}{3^3}\sqrt{23} < 2$, а значит, в поле $\mathbb{Q}(\theta)$ все дивизоры главные.

В случае квадратичных полей число классов дивизоров может быть определено также при помощи теории приведения, рассмотренной в задачах 12—15 и 24 § 7 гл. II.

Задачи

1. Показать, что в поле алгебраических чисел степени n число $\psi(a)$ целых дивизоров с данной нормой a не превосходит числа $\tau_n(a)$ всех решений неопределенного уравнения $x_1 x_2 \dots x_n = a$ ($x_1, \dots, x_n$ независимо друг от друга пробегают натуральные значения).

2. Пусть $\mathfrak{a}$ и $\mathfrak{b}$ — два дивизора поля алгебраических чисел (целых или дробных), а $\overline{\mathfrak{a}}$ и $\overline{\mathfrak{b}}$ — соответствующие им идеалы. Доказать, что если $\mathfrak{a}$ делится на $\mathfrak{b}$, то

$$(\overline{\mathfrak{b}} : \overline{\mathfrak{a}}) = N(\mathfrak{a}\mathfrak{b}^{-1}).$$

3. Доказать, что в любых двух различных классах дивизоров содержатся взаимно простые целые дивизоры.

4. Для целого дивизора $\mathfrak{a}$ поля алгебраических чисел через $\varphi(\mathfrak{a})$ обозначим число классов вычетов по модулю $\mathfrak{a}$, состоящих из чисел, взаимно простых с $\mathfrak{a}$ (обобщение теоретико-числовой функции Эйлера). Доказать, что если целые дивизоры $\mathfrak{a}$ и $\mathfrak{b}$ взаимно просты, то

$$\varphi(\mathfrak{a}\mathfrak{b}) = \varphi(\mathfrak{a})\varphi(\mathfrak{b}).$$

5. Доказать формулу

$$\varphi(\mathfrak{a}) = N(\mathfrak{a}) \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})}\right),$$

в которой $\mathfrak{p}$ пробегает все простые дивизоры, делящие целый дивизор $\mathfrak{a}$.

6. Доказать, что для любого целого числа α, взаимно простого с целым дивизором $\mathfrak{a}$, имеет место сравнение $\alpha^{\varphi(\mathfrak{a})} \equiv 1 \pmod{\mathfrak{a}}$ (обобщение теоремы Эйлера). Доказать, что для любого целого α и простого дивизора $\mathfrak{p}$ поля алгебраических чисел справедливо сравнение $\alpha^{N(\mathfrak{p})} \equiv \alpha \pmod{\mathfrak{p}}$ (обобщение малой теоремы Ферма).

7. Доказать формулу $\sum_{\mathfrak{c}} \varphi(\mathfrak{c}) = N(\mathfrak{a})$, в которой $\mathfrak{c}$ пробегает все делители целого дивизора $\mathfrak{a}$ (включая $\mathfrak{e}$ и $\mathfrak{a}$).

8. Пусть $\xi_1, \ldots, \xi_s$ ($s = N(\mathfrak{p}) - 1$) — система вычетов по простому модулю $\mathfrak{p}$, не делящихся на $\mathfrak{p}$. Доказать, что тогда $\xi_1 \ldots \xi_s \equiv -1 \pmod{\mathfrak{p}}$ (аналог теоремы Вильсона).

9. Используя задачу 2 § 6 гл. II, доказать, что в каждом классе дивизоров поля алгебраических чисел K степени $n = s + 2t$ и дискриминанта D содержится целый дивизор $\mathfrak{a}$, для которого

$$N(\mathfrak{a}) \leqslant \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} \sqrt{|D|}.$$

10. Показать, что для квадратичных полей, дискриминанты которых равны 5, 8, 12, 13, —3, —4, —8, —11, число классов дивизоров равно 1.

11. Показать, что число классов дивизоров поля $\mathbb{Q}(\sqrt{-19})$ равно 1.

12. Доказать, что в поле $\mathbb{Q}(\zeta)$, где ζ — первообразный корень 5-й степени из 1, разложение целых чисел на простые множители однозначно.

13. Показать, что для поля $\mathbb{Q}(\sqrt{-23})$ число классов дивизоров равно 3.

14. Пусть K_1, K_2 и K_3 — кубические поля, указанные в задаче 21 § 2 гл. II. Показать, что число 5 в полях K_1 и K_2 остается простым дивизором, а в поле K_3 раскладывается в произведение $5 = \mathfrak{p}\mathfrak{p}'\mathfrak{p}''$ трех различных простых дивизоров первой степени. Показать, далее, что число 11 раскладывается в произведение $11 = \mathfrak{q}\mathfrak{q}'\mathfrak{q}''$ трех различных простых дивизоров в поле K_1 и остается простым в поле K_2. (Отсюда следует, что K_1, K_2 и K_3 различны.)

15. Пусть примитивное целое число $\theta \in K$ является корнем многочлена Эйзенштейна относительно простого числа p. Используя результат задачи 9 § 5, доказать, что p не входит в индекс числа θ.

16. Пусть простое число p меньше степени n поля алгебраических чисел K. Доказать, что если в K существует целое примитивное число, индекс которого не делится на p, то число p в поле K не может раскладываться в произведение n различных простых дивизоров первой степени.

17. Основываясь на задачах 18 и 19 § 5, доказать, что простое рациональное число разветвляется в поле алгебраических чисел K (т. е. делится на квадрат простого дивизора) тогда и только тогда, когда оно входит в дискриминант поля K.

18. Пусть простой дивизор $\mathfrak{p}$ не делит числа 2 и не делит определителя δ квадратичной формы $f(x_1, \ldots, x_n)$ с целыми коэффициентами из поля алгебраических чисел K. Для целого $\alpha \in K$, не делящегося на $\mathfrak{p}$, положим $\left(\frac{\alpha}{\mathfrak{p}}\right) = +1$, если сравнение $\xi^2 \equiv \alpha \pmod{\mathfrak{p}}$ разрешимо в кольце целых чисел поля K, и $\left(\frac{\alpha}{\mathfrak{p}}\right) = -1$ в противном случае. Доказать, что число N решений сравнения

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{\mathfrak{p}}$$

выражается формулами

$$N = N(\mathfrak{p})^{n-1}, \qquad \text{если } n \text{ нечетное;}$$

$$N = N(\mathfrak{p})^{n-1} + \left(\frac{(-1)^{n/2}\delta}{\mathfrak{p}}\right) N(\mathfrak{p})^{(n-2)/2} (N(\mathfrak{p}) - 1),$$

если n четное.

19. Пусть $\mathfrak{a}$ — дивизор поля алгебраических чисел K, и пусть $\mathfrak{a}^m = (\alpha)$ — главный дивизор. Доказать, что в поле $K\left(\sqrt[m]{\alpha}\right)$ дивизор $\mathfrak{a}$ становится главным.

20. Доказать, что для любого поля алгебраических чисел K существует такое конечное расширение $\overline{K}/K$, что всякий дивизор $\mathfrak{a}$ поля K является главным дивизором, если его рассматривать в поле $\overline{K}$.

21. Пусть в кубическом поле K простое число p раскладывается в произведение $p = \mathfrak{p}\mathfrak{p}'\mathfrak{p}''$ трех различных простых дивизоров, и пусть α — целое число из K. Доказать, что если $\mathrm{Sp}(\alpha) = 0$ и $\mathfrak{p}\mathfrak{p}' \mid \alpha$, то $\mathfrak{p}'' \mid \alpha$ и, следовательно, $p \mid \alpha$.

22. Доказать, что число классов дивизоров поля $\mathbb{Q}(\theta)$, $\theta^3 = 6$, равно 1. (Согласно задаче 24 § 2 гл. II числа 1, θ, θ^2 образуют фундаментальный базис поля $\mathbb{Q}(\theta)$.)

23. Доказать, что в кубическом поле $K = \mathbb{Q}(\theta)$, $\theta^3 = 6$, не существует чисел $\alpha \neq 0$ вида $x + y\theta$ со взаимно простыми целыми рациональными x и y, для которых $N(\alpha) = 10z^3$ (z целое рациональное). Вывести отсюда, что уравнение $x^3 + 6y^3 = 10z^3$ (а значит, и уравнение $3x^3 + 4y^3 + 5z^3 = 0$) не имеет нетривиальных решений в целых рациональных числах.

Указание. Предполагая, что числа α существуют, доказать, что они имеют вид $\alpha = \alpha_0\xi^3$, где ξ — целое число поля K, а α_0 — одно из следующих шести чисел:

$$\lambda\mu, \quad \lambda\mu\varepsilon, \quad \lambda\mu\varepsilon^2, \quad \lambda\nu, \quad \lambda\nu\varepsilon, \quad \lambda\nu\varepsilon^2.$$

Здесь $\lambda = 2 - \theta$ ($N(\lambda) = 2$), $\mu = \theta - 1$ ($N(\mu) = 5$), $\nu = (\theta^2 + \theta + 1)^2 = 13 + 8\theta + 3\theta^2$ ($N(\nu) = 5 \cdot 5^3$), $\varepsilon = 1 - 6\theta + 3\theta^2$ — основная единица поля K (задача 4 § 5 гл. II). При доказательстве воспользоваться задачей 21, примененной к числу $\alpha\theta$, задачами 17 и 22, а также разложением в поле K чисел 2, 3 и 5 на простые множители. Далее, полагая $\xi = u + v\theta + w\theta^2$, запишем

$$\alpha = \alpha_0\xi^3 = \Phi + \Psi\theta + \Omega\theta^2,$$

где Φ, Ψ и Ω — целочисленные кубические формы от переменных u, v и w. Показать, что для каждого из шести значений α_0 уравнение $\Omega(u, v, w) = 0$ имеет только тривиальное решение в рациональных (и 3-адических) числах.

24. Пусть a и b — взаимно простые натуральные числа, свободные от квадратов, и пусть $d = ab^2 > 1$. Показать, что в поле $\mathbb{Q}\left(\sqrt[3]{d}\right)$ разложение числа 3 в произведение простых дивизоров имеет вид

$$3 = \mathfrak{p}^3, \qquad \text{если} \quad d \not\equiv \pm 1 \pmod 9,$$

$$3 = \mathfrak{p}^2\mathfrak{q}\ (\mathfrak{p} \neq \mathfrak{q}), \qquad \text{если} \quad d \equiv \pm 1 \pmod 9.$$

Указание. В случае $d \equiv \pm 1 \pmod 9$ рассмотреть нормы $N(\omega - 1)$, $N(\omega)$, $N(\omega + 1)$, где

$$\omega = \frac{1}{3}\left(1 + \sigma\sqrt[3]{ab^2} + \tau\sqrt[3]{a^2b}\right),$$

$$\sigma = \pm 1, \quad \tau = \pm 1, \quad \sigma a \equiv \tau b \equiv 1 \pmod 3.$$

25. Пусть θ — примитивное целое число поля алгебраических чисел K, $\varphi(t)$ — его минимальный многочлен и p — простое рациональное число, не входящее в индекс числа θ. Предположим, что по модулю p имеет место разложение

$$\varphi(t) \equiv \varphi_1(t)^{e_1} \dots \varphi_m(t)^{e_m} \pmod p,$$

где $\varphi_1, \dots, \varphi_m$ — неприводимые попарно различные по модулю p целочисленные многочлены степеней $f_1, \dots, f_m$ соответственно. Доказать, что разложение числа p в произведение простых дивизоров поля K имеет вид $p = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_m^{e_m}$, где различные простые дивизоры $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ имеют соответственно степени $f_1, \dots, f_m$, при этом $\varphi_i(\theta) \equiv 0 \pmod{\mathfrak{p}_i}$ для каждого $i = 1, \dots, m$.

Указание. Воспользоваться тем, что каждое целое число из K сравнимо по модулю $\mathfrak{p}_i$ с целочисленной линейной комбинацией степеней θ^s $(s \geqslant 0)$.

26. Пусть простое рациональное число p не входит в индекс целого примитивного числа θ поля K. Доказать, что при любом целом рациональном x число $\theta + x$ не делится в поле K на простой дивизор, входящий в p, степени выше первой. Доказать, далее, что $\theta + x$ не делится на произведение двух различных простых дивизоров первой степени, входящих в p.

27. Обобщая предшествующую задачу, доказать (в тех же предположениях), что при любых целых рациональных $x_0, \ldots, x_{r-1}$ число $\theta^r + x_{r-1}\theta^{r-1} + \ldots + x_0$ не делится на произведение $\mathfrak{p}_1 \ldots \mathfrak{p}_s$ различных простых дивизоров, входящих в p, степеней $f_1, \ldots, f_s$, если только $f_1 + \ldots + f_s > r$.

28. Пусть число классов дивизоров поля алгебраических чисел K равно 2. Доказать, что для любого $\alpha \neq 0$ из кольца $\mathfrak{O}$ целых чисел поля K (не являющегося единицей) число m простых сомножителей π_i во всяком разложении $\alpha = \pi_1 \ldots \pi_m$ на простые множители зависит только от α. (Справедливо и обратное утверждение: если в кольце $\mathfrak{O}$ разложение на простые множители не однозначно, но для любого α всякое разложение $\alpha = \pi_1 \ldots \pi_m$ имеет одно и то же число простых сомножителей π_i, то для поля K число классов дивизоров равно 2.)

§ 8. Квадратичное поле

В этом параграфе мы рассмотрим несколько подробнее теорию дивизоров для случая квадратичного поля. Начнем с описания простых дивизоров.

1. Простые дивизоры. Так как всякий простой дивизор является делителем одного и только одного простого числа, то для описания всех простых дивизоров в каком бы то ни было поле алгебраических чисел достаточно указать, как каждое простое рациональное число p раскладывается в этом поле в произведение простых дивизоров. Согласно равенству (3) § 7 в случае квадратичного поля (для которого $n = 2$) числа m, f_i, e_i могут принимать лишь следующие значения:

1) $m = 2, \quad f_1 = f_2 = 1, \quad e_1 = e_2 = 1;$
2) $m = 1, \quad f = 2, \quad e = 1;$
3) $m = 1, \quad f = 1, \quad e = 2.$

Соответственно этому мы получаем, что в квадратичном поле возможны три типа разложения:

1) $p = \mathfrak{p}\mathfrak{p}', \quad N(\mathfrak{p}) = N(\mathfrak{p}') = p, \quad \mathfrak{p} \neq \mathfrak{p}';$
2) $p = \mathfrak{p}, \quad N(\mathfrak{p}) = p^2;$
3) $p = \mathfrak{p}^2, \quad N(\mathfrak{p}) = p.$

Наша задача состоит, следовательно, в том, чтобы выяснить, чем определяется тип разложения для того или иного простого числа p. Ответ может быть без труда получен из теоремы 8 § 5.

В п. 1 § 7 гл. II было показано, что каждое квадратичное поле однозначно представляется в виде $\mathbb{Q}(\sqrt{d})$, где d — целое рациональное число, свободное от квадратов.

Рассмотрим сначала нечетное простое число p. Если p не входит в d, то оно не входит и в дискриминант многочлена x^2-d, корень которого порождает наше поле. Следовательно, по теореме 8 § 5 для p имеет место первый или второй тип разложения в зависимости от того, будет ли приводим многочлен x^2-d по модулю p или не будет. Это в свою очередь зависит от того, будет ли d квадратичным вычетом по модулю p или невычетом.

Если $p|d$, то $d=pd_1$, где d_1 не делится на p, так как d свободно от квадратов. Равенство $pd_1=(\sqrt{d})^2$, $(d_1, p)=1$, показывает, что все простые дивизоры, входящие в p, входят в него в четной степени, а это возможно только при третьем типе разложения. Таким образом, для нечетного p мы будем иметь первый, второй или третий тип разложения в зависимости от условий: 1) $p\nmid d$, $\left(\frac{d}{p}\right)=1$; 2) $p\nmid d$, $\left(\frac{d}{p}\right)=-1$; 3) $p|d$. Заметим, что поскольку дискриминант D поля $\mathbb{Q}(\sqrt{d})$ равен d или $4d$ (теорема 1 § 7 гл. II), то во всех этих условиях d можно заменить на D.

Остается рассмотреть случай $p=2$. Предположим сначала, что $2\nmid D$. Согласно теореме 1 § 7 гл. II это имеет место при $D=d\equiv 1 \pmod 4$. Ясно, что $\mathbb{Q}(\sqrt{d})=\mathbb{Q}(\omega)$, где $\omega=\frac{-1+\sqrt{D}}{2}$. Минимальным многочленом для ω является, очевидно, многочлен

$$x^2+x+\frac{1-D}{4}. \tag{1}$$

Так как дискриминант базиса 1, ω нечетен, то, опять применяя теорему 8 § 5, получаем, что для 2 имеет место первый или второй тип разложения в зависимости от того, будет ли многочлен (1) приводим по модулю 2 или не будет. Очевидно, что многочлен x^2+x+a приводим по модулю 2 тогда и только тогда, когда $2|a$. Таким образом, при $2\nmid D$ для 2 первый и второй тип разложения определяются соответственно условиями $D\equiv 1 \pmod 8$ и $D\equiv 5 \pmod 8$.

Докажем теперь, что если $2|D$, то для 2, так же как и для $p\neq 2$, имеет место третий тип разложения. Действительно, если $2|d$, то $d=2d'$, $2\nmid d'$ и из равенства

$$2d'=(\sqrt{d})^2, \quad 2\nmid d',$$

так же как и в случае нечетного p, получаем, что для 2 имеет место третий тип разложения. Если же $2\nmid d$, то $d\equiv 3 \pmod 4$ (теорема 1 § 7 гл. II) и в равенстве $(1+\sqrt{d})^2=2\alpha$ целое число $\alpha=\frac{1+d}{2}+\sqrt{d}$ взаимно просто с 2, так как его норма

$$N(\alpha)=\frac{(1+d)^2}{4}-d=\left(\frac{1-d}{2}\right)^2$$

не делится на 2. Следовательно, и в этом случае для 2 мы имеем третий тип разложения.

Сформулируем полученный результат.

Теорема 1. *В квадратичном поле с дискриминантом D для простого числа p разложение*

$$p = \mathfrak{p}^2, \quad N(\mathfrak{p}) = p,$$

имеет место тогда и только тогда, когда p является делителем D. Если нечетное p не входит в D, то

$$p = \mathfrak{p}\mathfrak{p}', \quad \mathfrak{p} \neq \mathfrak{p}', \quad N(\mathfrak{p}) = N(\mathfrak{p}') = p \quad \text{при} \quad \left(\frac{D}{p}\right) = 1;$$

$$p = \mathfrak{p}, \quad N(\mathfrak{p}) = p^2 \quad \text{при} \quad \left(\frac{D}{p}\right) = -1.$$

Если число 2 не входит в D (значит, $D \equiv 1 \pmod 4$), то

$$2 = \mathfrak{p}\mathfrak{p}', \quad \mathfrak{p} \neq \mathfrak{p}', \quad N(\mathfrak{p}) = N(\mathfrak{p}') = 2 \quad \text{при} \quad D \equiv 1 \pmod 8;$$

$$2 = \mathfrak{p}, \quad N(\mathfrak{p}) = 4 \quad \text{при} \quad D \equiv 5 \pmod 8.$$

2. Закон разложения. Согласно теореме 1 тип разложения простого нечетного p определяется вычетом D (или d) по модулю p, точнее, значением символа Лежандра $\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right)$ как функции от знаменателя p. В связи с этим возникает вопрос, нельзя ли переформулировать теорему 1 так, чтобы тип разложения определялся вычетом p по некоторому постоянному модулю (зависящему только от поля). Чтобы найти эту новую формулировку, воспользуемся законом взаимности для символа Якоби.

Символ Якоби $\left(\frac{c}{b}\right)$ определен, как известно, для целого $c \neq 0$ и нечетного положительного b, взаимно простого с c. Закон взаимности для этого символа утверждает, что при нечетном c

$$\left(\frac{c}{b}\right) = (-1)^{\frac{b-1}{2}\cdot\frac{c-1}{2}} \left(\frac{b}{|c|}\right)$$

(доказательство для $c < 0$ легко сводится к случаю положительного числителя).

Пусть p — произвольное нечетное простое число. Если $d = D \equiv 1 \pmod 4$, то

$$\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{d-1}{2}} \left(\frac{p}{|d|}\right) = \left(\frac{p}{|D|}\right), \tag{2}$$

так как $\frac{d-1}{2}$ четно. Если же $d \equiv 3 \pmod 4$, то

$$\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{d-1}{2}} \left(\frac{p}{|d|}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{|d|}\right), \tag{3}$$

так как $\frac{d-1}{2}$ нечетно. Наконец, при $d=2d'$, $2\nmid d'$ мы имеем

$$\left(\frac{D}{p}\right)=\left(\frac{d}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{d'}{p}\right)=(-1)^{\frac{p^2-1}{8}+\frac{p-1}{2}\cdot\frac{d'-1}{2}}\left(\frac{p}{|d'|}\right). \tag{4}$$

Значение символа Якоби $\left(\frac{p}{|d|}\right)$ или $\left(\frac{p}{|d'|}\right)$ зависит, очевидно, только от вычета p по модулю $|d|$ или $|d'|$. Если $d\equiv 1 \pmod 4$, так что дискриминант D поля $\mathbb{Q}(\sqrt{d})$ равен d, то $\left(\frac{D}{p}\right)$ зависит только от вычета p по модулю $|d|=|D|$. Если $d\equiv 3 \pmod 4$ и, следовательно, $D=4d$, то $\left(\frac{D}{p}\right)$ зависит уже не только от вычета p по модулю $|d|$, но и от числа $(-1)^{(p-1)/2}$, т. е. от вычета p по модулю 4; следовательно, $\left(\frac{D}{p}\right)$ зависит в итоге от вычета p по модулю $4|d|=|D|$. Наконец, если $d=2d'$, $D=4d=8d'$, то $\left(\frac{p}{|d'|}\right)$ зависит от вычета p по модулю $|d'|$, $(-1)^{(p-1)/2}$ — от вычета p по модулю 4, а $(-1)^{(p^2-1)/8}$ — от вычета p по модулю 8. Следовательно, в этом случае $\left(\frac{D}{p}\right)$ зависит от вычета p по модулю $8|d'|=|D|$. Мы видим, таким образом, что во всех случаях тип разложения простого нечетного числа p определяется его вычетом по модулю $|D|$, так что все простые числа, имеющие один и тот же вычет, т. е. лежащие в одной арифметической прогрессии вида $a+|D|x$, имеют один и тот же тип разложения. Этот a priori совершенно не очевидный вывод и является принципиально наиболее важным свойством закона разложения простых чисел в квадратичном поле.

Чтобы сформулировать эту новую форму закона разложения более четко, рассмотрим на целых числах x, взаимно простых с дискриминантом D, функцию $\chi(x)$, полагая

$$\chi(x)=\begin{cases}\left(\frac{x}{|d|}\right) & \text{при } d\equiv 1 \pmod 4,\\ (-1)^{\frac{x-1}{2}}\left(\frac{x}{|d|}\right) & \text{при } d\equiv 3 \pmod 4,\\ (-1)^{\frac{x^2-1}{8}+\frac{x-1}{2}\cdot\frac{d'-1}{2}}\left(\frac{x}{|d'|}\right) & \text{при } d=2d'\end{cases} \tag{5}$$

(в случае $d\equiv 2, 3 \pmod 4$ выражения $(-1)^{(x-1)/2}$ и $(-1)^{(x^2-1)/8}$ имеют смысл, так как ввиду четности дискриминанта $D=4d$ число x нечетно).

В проведенном выше рассуждении, показывающем, что при нечетном p значение $\left(\frac{D}{p}\right)$ зависит только от вычета p по модулю $|D|$, мы нигде не пользовались простотой p. Поэтому то же рассуждение дает нам, что $\chi(x)$ зависит только от вычета x по модулю $|D|$. Далее, легко проверяется, что если $(x, D)=1$ и $(x', D)=1$, то $\chi(xx')=\chi(x)\chi(x')$. Все это показывает, что функцию χ можно рассматривать как гомоморфизм мультипликативной группы классов вычетов по модулю $|D|$, взаимно простых с D, в группу второго порядка, состоящую из чисел $+1$ и -1. Такие функции, доопределенные нулевыми значениями на числах, не взаимно простых с D, называются *числовыми (квадратичными) характерами.*

Определение. *Числовой характер χ по модулю $|D|$, значения которого $\chi(x)$ на целых x, взаимно простых с D, определяются равенствами* (5), *называется характером квадратичного поля* $\mathbb{Q}(\sqrt{d})$.

Возвращаясь к равенствам (2), (3) и (4), мы видим, что разложение для простого нечетного p, не входящего в D, будет первого или второго типа в зависимости от того, будет ли $\chi(p)$ равно $+1$ или -1. Этот же результат справедлив, оказывается, и для $p=2$. В самом деле, если $2 \nmid D$, то $D \equiv 1 \pmod 4$ и, значит, $\chi(2)=\left(\frac{2}{|D|}\right)$, что равно $+1$ при $D \equiv 1 \pmod 8$ и -1 при $D \equiv 5 \pmod 8$.

Нами получена, таким образом, следующая новая формулировка закона разложения в квадратичном поле.

Теорема 2. *В терминах характера χ квадратичного поля $\mathbb{Q}(\sqrt{d})$ разложение рациональных простых чисел в произведение простых дивизоров определяется условиями:*

$$\begin{aligned} &p=\mathfrak{p}\mathfrak{p}', \quad \mathfrak{p}\neq\mathfrak{p}', \quad N(\mathfrak{p})=N(\mathfrak{p}')=p, && \text{если} \quad \chi(p)=1;\\ &p=\mathfrak{p}, \quad N(\mathfrak{p})=p^2, && \text{если} \quad \chi(p)=-1;\\ &p=\mathfrak{p}^2, \quad N(\mathfrak{p})=p, && \text{если} \quad \chi(p)=0. \end{aligned}$$

Все целые рациональные числа в зависимости от значения на них характера χ разбиваются на три группы, каждая из которых является объединением нескольких полных классов вычетов по модулю $|D|$. Согласно теореме 2 тип разложения зависит от того, в какую из этих групп попадает простое число p.

Такой закон разложения, как в квадратичном поле, когда тип разложения определяется только вычетом простого числа p по некоторому постоянному модулю, имеет место и для некоторых других полей. Так обстоит дело, например, для полей деления круга (см. гл. V, § 2, п. 2). Однако далеко не все поля алгебраических чисел обладают аналогичными законами разложения. Так как знание законов разложения в полях алгебраических чисел

дает возможность решать многие теоретико-числовые задачи (см., например, следующий пункт и § 2 гл. V), то интересно было бы знать, каковы те поля, в которых закон разложения имеет только что описанный простой вид. Ответ на этот вопрос дает теория полей классов. Оказывается, что такими полями являются те нормальные расширения поля рациональных чисел, группа Галуа которых абелева. К их числу относятся, конечно, все квадратичные поля, имеющие циклическую группу второго порядка в качестве группы Галуа. Простейший пример неабелева поля дает нам кубическое поле, если только его дискриминант не есть полный квадрат, например поле $\mathbb{Q}(\theta)$, где $\theta^3 - \theta - 1 = 0$. Для этого поля, следовательно, нельзя найти такое число M, чтобы тип разложения простого числа p в произведение простых дивизоров зависел только от вычета p по модулю M.

Теория полей классов решает, впрочем, гораздо более общий вопрос, чем тот, с которым мы встретились. Она описывает закон разложения простых дивизоров произвольного поля алгебраических чисел k на множители в некотором расширении K/k, если группа Галуа этого расширения абелева (мы говорили выше об очень частном случае, когда $k = \mathbb{Q}$). Теория полей классов имеет много теоретико-числовых применений. Так, она позволяет перенести доказанные в гл. I теоремы о квадратичных формах с рациональными коэффициентами на квадратичные формы с коэффициентами из произвольного поля алгебраических чисел k, понять с более глубокой точки зрения теорию родов, которую мы изложим в п. 4, доказать теорему о существовании простых дивизоров в заданном классе дивизоров и т. д. С теорией полей классов можно познакомиться по книгам [1] и [6].

Не меньшее число арифметических задач приводит к лежащему за пределами теории полей классов вопросу о законах разложения простых чисел в полях с неабелевой группой Галуа. Об этих законах разложения известно в настоящее время очень мало.

3. Представление чисел бинарными квадратичными формами. В п. 5 § 7 гл. II мы видели, что существует взаимно однозначное соответствие между классами собственно эквивалентных примитивных бинарных квадратичных форм и классами подобных в узком смысле модулей квадратичного поля (в случае $D < 0$ рассматриваются только положительно определенные формы). С другой стороны, согласно теореме 6 § 6 полные модули, принадлежащие максимальному порядку (т. е. идеалы поля), взаимно однозначно соответствуют дивизорам. Естественно поэтому ожидать, что теория дивизоров в квадратичном поле имеет определенные связи с теорией тех примитивных форм, дискриминант которых совпадает с дискриминантом поля.

Чтобы соответствие между классами форм и классами модулей распространить на дивизоры, мы должны, очевидно, слегка изменить понятие эквивалентности дивизоров.

Определение. *Два дивизора* $\mathfrak{a}$ *и* $\mathfrak{b}$ *квадратичного поля* $\mathbb{Q}(\sqrt{d})$ *называются эквивалентными в узком смысле, если в* $\mathbb{Q}(\sqrt{d})$ *существует такое число* $\alpha \neq 0$, *что* $N(\alpha) > 0$ *и* $\mathfrak{a} = \mathfrak{b}(\alpha)$.

Так как для мнимых квадратичных полей нормы всех отличных от нуля чисел положительны, то в них эквивалентность дивизоров в узком смысле совпадает с обычной (определение п. 2 § 7). Те же рассуждения, что и для модулей (см. п. 5 § 7 гл. II), показывают, что в вещественном поле $\mathbb{Q}(\sqrt{d})$ новое понятие эквивалентности дивизоров совпадает со старым тогда и только тогда, когда норма основной единицы ε поля $\mathbb{Q}(\sqrt{d})$ равна -1. Если же $N(\varepsilon) = +1$, то каждый класс дивизоров относительно обычной эквивалентности распадается ровно на два класса дивизоров, эквивалентных в узком смысле. Таким образом, число $\bar{h}$ классов дивизоров в узком смысле также конечно и, согласно сказанному, связано с числом h классов дивизоров в обычном смысле соотношением:

$$\begin{aligned} &\bar{h} = h \quad \text{при} \quad d < 0; \\ &\bar{h} = h \quad \text{при} \quad d > 0, \quad N(\varepsilon) = -1; \\ &\bar{h} = 2h \quad \text{при} \quad d > 0, \quad N(\varepsilon) = +1. \end{aligned}$$

Теорема 4 § 7 гл. II в применении к модулям, принадлежащим максимальному порядку поля $\mathbb{Q}(\sqrt{d})$ с дискриминантом D, теперь может быть переформулирована следующим образом: классы дивизоров в узком смысле квадратичного поля $\mathbb{Q}(\sqrt{d})$ находятся во взаимно однозначном соответствии с классами собственно эквивалентных примитивных бинарных квадратичных форм дискриминанта D (положительно определенных при $D < 0$).

Попробуем применить результаты пп. 1 и 2 к вопросу о представлении чисел бинарными формами.

Согласно теореме 6 § 7 гл. II натуральное число a представляется некоторой формой дискриминанта D тогда и только тогда, когда в поле $\mathbb{Q}(\sqrt{d})$ существует целый дивизор с нормой a (мы знаем, что норма дивизора совпадает с нормой соответствующего ему модуля). Но нормы всех целых дивизоров могут быть охарактеризованы с помощью теоремы 2. Действительно, согласно этой теореме норма $N(\mathfrak{p})$ простого дивизора $\mathfrak{p}$ равна простому числу p, если $\chi(p) = 0$ или $\chi(p) = 1$, и равна квадрату простого числа, если $\chi(p) = -1$. Следовательно, число a представимо в виде нормы $N(\mathfrak{a})$ целого дивизора $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$ поля $\mathbb{Q}(\sqrt{d})$ тогда и только тогда, когда все простые числа p, для которых $\chi(p) = -1$, входят в a в четной степени.

Найденному условию мы можем придать несколько другой вид, если воспользуемся символом Гильберта, определение кото-

рого было дано нами в п. 3 § 6 гл. I. Вычислим $\left(\frac{a, D}{p}\right)$ для всех простых чисел p, не входящих в D. Пусть $a = p^k b$, где b не делится на p. Согласно свойствам символа Гильберта мы имеем:

$$\left(\frac{a, D}{p}\right) = \left(\frac{b, D}{p}\right)\left(\frac{D}{p}\right)^k = \left(\frac{D}{p}\right)^k = \chi(p)^k \quad \text{при} \quad p \neq 2, \quad p \nmid D;$$

$$\left(\frac{a, D}{2}\right) = (-1)^{\frac{b-1}{2}\cdot\frac{D-1}{2}+k\frac{D^2-1}{8}} = (-1)^{k\frac{D^2-1}{8}} = \chi(2)^k \quad \text{при} \quad p = 2, \ 2 \nmid D$$

(в случае $p = 2$, $2 \nmid D$ следует учесть сравнение $D \equiv 1 \pmod 4$). Полученные формулы доказывают вторую часть следующей теоремы.

Теорема 3. *Для того чтобы натуральное число a представлялось некоторой бинарной формой дискриминанта D, необходимо и достаточно, чтобы оно не содержало простых чисел p с условием $\chi(p) = -1$ в нечетной степени. Для этого в свою очередь необходимо и достаточно, чтобы*

$$\left(\frac{a, D}{p}\right) = +1 \quad \textit{для всех} \quad p \nmid D.$$

Так как целые числа a и ab^2 одновременно представляются или не представляются формами дискриминанта D, то мы можем ограничиться рассмотрением чисел a, свободных от квадратов.

Если $p \neq 2$, $p \nmid D$ и $p \nmid a$, то, как мы знаем, $\left(\frac{a, D}{p}\right) = +1$. Следовательно, теорема 3 накладывает на число a лишь конечное число условий, причем в этих условиях участвуют только вычеты простых делителей числа a (свободного от квадратов) по модулю $|D|$.

Теорему 3 можно было бы легко вывести из теоремы 7 § 7, гл. II. Мы привели доказательство, опирающееся на теорему 2, желая обратить внимание на связь вопроса о представлении чисел формами дискриминанта D с вопросом о разложении на множители в соответствующем квадратичном поле.

Полученный результат дает нам, однако, не совсем то, что мы хотели бы получить. Действительно, нам желательно было бы иметь критерий представимости числа a формами из заданного класса собственно эквивалентных форм, а теорема 3 дает нам условие представимости a формами из какого-нибудь класса. В связи с этим возникает следующий вопрос. Нельзя ли классы форм так разбить на непересекающиеся группы (по возможности более мелкие), чтобы для любого a все формы, представляющие это число a (если конечно, они существуют), содержались в некоторой одной определенной группе? Такое разбиение классов форм на группы было найдено Гауссом. Оно связано с рассмотрением рациональной эквивалентности квадратичных форм.

Определение. *Говорят, что две примитивные бинарные квадратичные формы данного дискриминанта D принадлежат одному роду, если они рационально эквивалентны.*

Так как целочисленно эквивалентные формы тем самым и рационально эквивалентны, то все формы одного и того же класса входят в один род. Таким образом, каждый род является объединением нескольких классов форм. Отсюда, в частности, следует, что число родов форм (данного дискриминанта D) конечно.

В п. 5 § 7 гл. I для бинарных рациональных неособенных форм f были введены инварианты $e_p(f)$, где p — простое число или символ ∞. В нашем случае примитивных форм f дискриминанта D определитель равен $-\frac{1}{4}D$, поэтому $e_p(f)=\left(\frac{a, D}{p}\right)$, где $a\neq 0$ — произвольное число, рационально представимое формой f.

Пусть G — некоторый род форм. Так как все формы из G имеют одни и те же инварианты, то мы можем положить $e_p(G)=e_p(f)$, где f — произвольная форма из рода G.

Пусть a — отличное от нуля число, представимое формой f. Согласно второму утверждению теоремы 3 мы имеем $e_p(f)=\left(\frac{a, D}{p}\right)=1$ для всех простых p, не входящих в D. Далее, $e_\infty(f)=1$, так как в случае $D<0$ мы рассматриваем только положительно определенные формы. Следовательно, для любого рода G форм дискриминанта D мы имеем

$$e_p(G)=1 \quad \text{при} \quad p\nmid D \quad \text{и} \quad p=\infty. \tag{6}$$

Каждый род G однозначно определен, таким образом, инвариантами $e_p(G)$, где p пробегает все простые делители дискриминанта D.

Условие представимости чисел формами некоторого фиксированного рода G может быть сформулировано следующим образом.

Теорема 4. *Для того чтобы целое $a>0$ допускало целочисленное представление некоторой формой рода G, необходимо и достаточно, чтобы при всех p выполнялось равенство*

$$\left(\frac{a, D}{p}\right)=e_p(G).$$

Доказательство. Необходимость условия очевидна. Если же для некоторого a мы имеем $\left(\frac{a, D}{p}\right)=e_p(G)$ при всех p, то ввиду (6) $\left(\frac{a, D}{p}\right)=1$ при всех $p\nmid D$. Но в таком случае согласно теореме 3 число a представляется некоторой формой f дискриминанта D, а так как $e_p(f)=\left(\frac{a, D}{p}\right)=e_p(G)$, то f принадлежит роду G, и теорема 4 доказана.

Утверждение теоремы 4 интересно в том отношении, что оно характеризует представимость числа a некоторой формой из рода

G лишь вычетом числа a по модулю $|D|$ (при условии, что a вообще представимо какой-нибудь формой дискриминанта D, т. е. при условии, что $\left(\frac{a, D}{p}\right) = 1$ при всех $p \nmid D$). Действительно, все значения $\left(\frac{a, D}{p}\right)$ для $p \mid D$ зависят только от вычета a по модулю $|D|$. В случае, когда разбиение форм на роды совпадает с разбиением на классы (т. е. когда каждый род состоит только из одного класса), теорема 4 дает нам, следовательно, идеальный ответ на вопрос о представлении чисел бинарными формами.

В общем же случае этот результат улучшить нельзя. Это значит, что, какой бы дискриминант D (максимального порядка) мы ни взяли и какую бы совокупность классов форм этого дискриминанта ни рассмотрели, если эта совокупность не состоит целиком из нескольких родов, то не существует такого модуля m, что представимость числа какой-нибудь формой нашей совокупности зависит только от вычета этого числа по модулю m. В частности, если род состоит не из одного класса, то не существует характеристики чисел, представимых классом, в терминах их вычетов по некоторому модулю. Доказательства этих фактов вытекают из теории полей классов и основываются на том, что (если ограничиться простыми числами) представимость простого числа формами некоторой совокупности классов можно интерпретировать в терминах типа разложения этого числа на простые дивизоры в некотором поле L. Это поле L только в том случае будет иметь абелеву группу Галуа над полем рациональных чисел, когда наша совокупность классов состоит из нескольких родов (см. по этому поводу работу [78]).

Займемся теперь исследованием вопроса о числе родов. Пусть $p_1, \ldots, p_t$ — все попарно различные простые делители дискриминанта D. Согласно (6) каждый род однозначно определяется набором инвариантов $e = e_{p_i}(G)$. Эти инварианты не могут быть произвольны, так как, выбрав форму $f \in G$ и число $a \neq 0$, представимое формой f, мы имеем (формула (17) § 7 гл. I)

$$e_1 \ldots e_t = \prod_p e_p(G) = \prod_p \left(\frac{a, D}{p}\right) = 1$$

(в произведениях p пробегает все простые числа и символ ∞).

Покажем, что полученное нами соотношение

$$e_1 \ldots e_t = 1 \tag{7}$$

между числами $e_i = \pm 1$ является не только необходимым, но и достаточным, для того чтобы эти числа являлись инвариантами некоторого рода G.

Обозначим через k_t показатель степени, с которым p_t входит в D (k_t равно 1 для всех $p_i \neq 2$ и равно 2 или 3 для $p_i = 2$). Для каждого $i = 1, \ldots, t$ выберем целое a_i, не делящееся на p_i, для

которого $\left(\frac{a_i, D}{p_i}\right) = e_i$, а затем определим целое a из системы сравнений

$$a \equiv a_i \pmod{p_i^{k_i}} \qquad (1 \leqslant i \leqslant t).$$

Для любого a, удовлетворяющего этим сравнениям, мы имеем (в силу свойств символа Гильберта)

$$\left(\frac{a, D}{p_i}\right) = \left(\frac{a_i, D}{p_i}\right) = e_i.$$

Наша задача состоит сейчас в том, чтобы среди значений a найти такое, для которого $\left(\frac{a, D}{p}\right) = 1$ при всех $p \nmid D$. Воспользуемся для этой цели теоремой Дирихле о простых числах в арифметической прогрессии (см. § 3 гл. V). Так как все значения a взаимно просты с D и образуют класс вычетов по модулю $|D| = \prod p_i^{k_i}$, то по теореме Дирихле среди них найдется нечетное простое число q. Для него мы имеем:

$$\left(\frac{q, D}{p_i}\right) = \left(\frac{a, D}{p_i}\right) = e_i;$$

$$\left(\frac{q, D}{p}\right) = 1 \quad \text{при} \quad p \nmid D, \quad p \neq 2 \quad \text{и} \quad p \neq q;$$

$$\left(\frac{q, D}{2}\right) = (-1)^{\frac{q-1}{2}\cdot\frac{D-1}{2}} = 1 \quad \text{при} \quad 2 \nmid D.$$

Соотношение $\prod_{\wp} \left(\frac{q, D}{p}\right) = 1$ дает нам, следовательно, равенство $e_1 \ldots e_t \left(\frac{q, D}{q}\right) = 1$, откуда ввиду (7) следует, что значение символа $\left(\frac{q, D}{q}\right)$ также равно 1.

Таким образом, существует натуральное a (и даже простое), для которого

$$\left(\frac{a, D}{p_i}\right) = e_i \quad (1 \leqslant i \leqslant t) \qquad \text{и} \qquad \left(\frac{a, D}{p}\right) = 1 \quad \text{при} \quad p \nmid D.$$

По теореме 3 число a представляется некоторой формой f дискриминанта D. Если эта форма принадлежит роду G, то

$$e_{\wp_i}(G) = \left(\frac{a, D}{p_i}\right) = e_i \qquad (1 \leqslant i \leqslant t).$$

Этим и доказано наше утверждение о существовании рода с наперед заданными инвариантами (удовлетворяющими, конечно, со-

отношению (7)). Так как число всех возможных наборов значений $e_i = \pm 1$ с условием (7) равно 2^{t-1}, то, следовательно, число всех родов форм дискриминанта D также равно 2^{t-1}. Сформулируем полученный результат.

Теорема 5. *Пусть $p_1, \ldots, p_t$ — все попарно различные простые делители дискриминанта D квадратичного поля $\mathbb{Q}(\sqrt{d})$. Для любого набора значений $e_i = \pm 1$ $(1 \leqslant i \leqslant t)$ с условием $e_1 \ldots e_t = 1$ существует род G форм дискриминанта D, для которого $e_{\mathfrak{p}_i}(G) = e_i$. Число всех родов форм дискриминанта D равно 2^{t-1}.*

Замечание 1. Изложенная в этом пункте теория родов для форм, дискриминант которых совпадает с дискриминантом D максимального порядка квадратичного поля, может быть развита также и для форм дискриминанта Df^2.

Замечание 2. Если каждый род форм отрицательного дискриминанта Df^2 состоит только из одного класса, то для числа представлений целых чисел, взаимно простых с f, фиксированной формой дискриминанта Df^2 может быть указана простая формула (см. задачу 18). Таблица известных значений дискриминантов $Df^2 < 0$ с одноклассными родами приведена в конце книги. Вопрос о том, исчерпывает ли эта таблица все значения отрицательных дискриминантов, для которых каждый род форм состоит из одного класса, к настоящему времени не решен. Доказано только, что число таких дискриминантов конечно. Для четных Df^2 из приведенной таблицы числа $-\frac{1}{4}Df^2$ были найдены еще Эйлером и названы им *удобными* числами. Удобные числа применялись Эйлером для разыскания больших простых чисел на основе следующего их свойства: если произведение ab взаимно простых натуральных чисел a и b равно одному из удобных чисел и если форма $ax^2 + by^2$ представляет число q существенно одним способом (при взаимно простых x и y), то это число q простое (см. задачу 19). Например, разность $3049 - 120y^2$ только при $y = 5$ является квадратом, значит, число 3049 представляется формой $x^2 + 120y^2$ единственным образом: $3049 = 7^2 + 120 \cdot 5^2$, и поэтому оно простое. Этим приемом Эйлеру удалось установить простоту многих больших по тому времени простых чисел. Ясно, что, чем больше удобное число, тем меньше требуется испытаний для выяснения вопроса о единственности представления.

4. Роды дивизоров. Полученные в п. 3 результаты о родах форм позволяют сделать некоторые заключения о строении группы классов (в узком смысле) дивизоров квадратичного поля. Перенесем для этого определение родов на дивизоры.

Согласно теореме 6 § 6 каждому дивизору $\mathfrak{a}$ (целому или дробному) взаимно однозначно соответствует идеал $\mathfrak{a}$, состоящий из тех чисел поля, которые делятся на $\mathfrak{a}$. В случае квадратичного поля каждому базису $\{\alpha, \beta\}$ модуля $\mathfrak{a}$, удовлетворяющему

условию (10) § 7 гл. II, соответствует примитивная форма

$$f(x, y) = \frac{N(\alpha x + \beta y)}{N(\mathfrak{a})}. \tag{8}$$

При переходе к другому базису модуля $\bar{\mathfrak{a}}$ (с тем же условием (10) § 7 гл. II) форма f заменяется собственно эквивалентной формой. Равенство (8) сопоставляет, стало быть, дивизору $\mathfrak{a}$ целый класс собственно эквивалентных форм. Это отображение и устанавливает взаимно однозначное соответствие между классами дивизоров в узком смысле и классами собственно эквивалентных форм дискриминанта D, о котором уже говорилось в начале п. 3.

Определение. *Два дивизора квадратичного поля принадлежат одному роду, если соответствующие им классы форм содержатся в одном и том же роде форм* (*т. е. рационально эквивалентны*).

Так как эквивалентным в узком смысле дивизорам соответствует один и тот же класс форм, то каждый род дивизоров является объединением нескольких классов дивизоров (в узком смысле).

Род дивизоров, соответствующий роду форм G, мы будем обозначать той же буквой G. Под инвариантами $e_p(G)$ рода дивизоров G подразумеваются аналогичные инварианты соответствующего класса форм. Для инвариантов $e_p(G)$ имеет место формула

$$e_p(G) = \left(\frac{N(\mathfrak{a}), D}{p}\right), \tag{9}$$

где $\mathfrak{a}$ — произвольный дивизор из рода G. В самом деле, по определению инвариантов $e_p(G) = \left(\frac{a, D}{p}\right)$, где a — отличное от нуля рациональное число, представимое формулой $f(x, y)$ вида (8), соответствующей дивизору $\mathfrak{a}$. Но форма $N(\alpha x + \beta y)$ представляет все квадраты рациональных чисел, в частности она представляет $N(\mathfrak{a})^2$. Следовательно, $f(x, y)$ представляет $N(\mathfrak{a})$, а это и доказывает формулу (9).

Род дивизоров G_0, все инварианты которого равны 1, называется главным родом. Все дивизоры $\mathfrak{a}$ из главного рода характеризуются условием $\left(\frac{N(\mathfrak{a}), D}{p}\right) = 1$ при всех p. Отсюда следует, что главный род является группой относительно умножения дивизоров — подгруппой группы всех дивизоров. Очевидно, далее, что произвольный род дивизоров G является смежным классом $\mathfrak{a}G_0$ по подгруппе G_0, где $\mathfrak{a}$ — произвольный дивизор из рода G. Но совокупность всех смежных классов по подгруппе G_0 является естественным образом группой — фактор-группой группы всех дивизоров по подгруппе G_0. Мы можем, следовательно, совокупность всех родов рассматривать как группу. Она называется *груп-*

пой родов. Согласно теореме 5 порядок группы родов равен 2^{t-1}, где t — число различных простых делителей дискриминанта D.

Дадим характеристику рода дивизоров в терминах самих дивизоров (без привлечения форм).

Теорема 6. *Два дивизора* $\mathfrak{a}$ *и* $\mathfrak{a}_1$ *квадратичного поля принадлежат одному и тому же роду тогда и только тогда, когда в поле существует такое число* γ *с положительной нормой, что*

$$N(\mathfrak{a}_1) = N(\mathfrak{a})N(\gamma).$$

Доказательство. Выберем в идеалах $\bar{\mathfrak{a}}$ и $\bar{\mathfrak{a}}_1$ базисы $\{\alpha, \beta\}$ и $\{\alpha_1, \beta_1\}$, удовлетворяющие условию (10) § 7 гл. II. Тогда дивизорам $\mathfrak{a}$ и $\mathfrak{a}_1$ будут соответствовать формы

$$f(x, y) = \frac{N(\alpha x + \beta y)}{N(\mathfrak{a})}, \qquad f_1(x, y) = \frac{N(\alpha_1 x + \beta_1 y)}{N(\mathfrak{a}_1)}.$$

Согласно теореме 11 § 1 Дополнения формы f и f_1 рационально эквивалентны тогда и только тогда, когда существует хоть одно рациональное число $\neq 0$, представимое одновременно этими формами, т. е. когда

$$\frac{N(\xi)}{N(\mathfrak{a})} = \frac{N(\xi_1)}{N(\mathfrak{a}_1)} \qquad (\xi, \xi_1 \neq 0).$$

Отсюда и следует утверждение теоремы.

Для дивизоров главного рода мы имеем следующую важную характеристику.

Теорема 7. *Дивизор* $\mathfrak{a}$ *принадлежит главному роду тогда и только тогда, когда он эквивалентен в узком смысле квадрату дивизора.*

Доказательство. Пусть дивизор $\mathfrak{a}$ принадлежит главному роду. Так как единичный дивизор принадлежит главному роду, то по теореме 6 существует число γ, для которого $N(\mathfrak{a}) = N(\gamma)$. Заменив $\mathfrak{a}$ на эквивалентный ему дивизор $\mathfrak{a}(\gamma^{-1})$, мы можем считать, что $N(\mathfrak{a}) = 1$. Чтобы выяснить, при каком условии возможно это равенство, разложим дивизор $\mathfrak{a}$ в произведение простых дивизоров. При этом мы отделим простые дивизоры $\mathfrak{p}_i$, для которых существует другой простой дивизор $\mathfrak{p}_i'$ с той же нормой (первый тип разложения по терминологии п. 1), от всех остальных простых дивизоров $\mathfrak{q}_j$:

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{a_i} \mathfrak{p}_i'^{b_i} \prod_j \mathfrak{q}_j^{c_j}.$$

Так как $N(\mathfrak{p}_i) = N(\mathfrak{p}_i') = p_i$ и $N(\mathfrak{q}_i) = q_j^{r_j}$ (где r_j равно 2 или 1), то условие $N(\mathfrak{a}) = 1$ дает нам

$$\prod_i p_i^{a_i + b_i} \prod_j q_j^{r_j c_j} = 1.$$

Простые числа p_i и q_j попарно различны, поэтому $b_i = -a_i$ и $c_j = 0$, а значит,

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{a_i} \mathfrak{p}_i'^{-a_i}.$$

Но $\mathfrak{p}_i \mathfrak{p}_i' = p_i$, поэтому $\mathfrak{p}_i'^{-1} \sim \mathfrak{p}_i$, откуда следует, что

$$\mathfrak{a} \sim \left(\prod_i \mathfrak{p}_i^{a_i}\right)^2$$

(знак $\sim$ здесь означает эквивалентность дивизоров в узком смысле).

Обратно, если $\mathfrak{a} \sim \mathfrak{b}^2$, т. е. $\mathfrak{a} = \mathfrak{b}^2(\alpha)$, $N(\alpha) > 0$, то $N(\mathfrak{a}) = N(\beta)$, где $\beta = N(\mathfrak{b})\alpha$, а значит, по теореме 6 $\mathfrak{a}$ принадлежит главному роду.

Теорема 7 доказана.

Рассмотрим теперь группу $\mathfrak{C}$ классов дивизоров в узком смысле. Если каждому классу $C \in \mathfrak{C}$ мы поставим в соответствие тот род G, в котором этот класс содержится, то получим гомоморфизм группы классов $\mathfrak{C}$ на группу родов. Его ядром является совокупность тех классов, которые содержатся в главном роде G_0. По теореме 7 класс C' содержится в главном роде тогда и только тогда, когда он является квадратом некоторого класса из $\mathfrak{C}$. Таким образом, ядром гомоморфизма группы $\mathfrak{C}$ на группу родов является подгруппа $\mathfrak{C}^2$, состоящая из квадратов C^2 классов $C \in \mathfrak{C}$. Применяя теорему о гомоморфизме из теории групп и вспоминая, что группа родов имеет порядок 2^{t-1}, приходим к следующему результату.

Теорема 8. *Фактор-группа $\mathfrak{C}/\mathfrak{C}^2$ группы $\mathfrak{C}$ классов дивизоров в узком смысле по подгруппе квадратов имеет порядок 2^{t-1}, где t — число различных простых делителей дискриминанта D квадратичного поля.*

Значение теоремы 8 состоит в том, что она дает нам некоторые сведения о строении группы $\mathfrak{C}$. Согласно теореме 1 § 5 Дополнения группа $\mathfrak{C}$ может быть разложена в прямое произведение циклических подгрупп. Из теоремы 8 легко следует, что среди этих подгрупп ровно $t-1$ будут иметь четный порядок. В частности, мы получаем следующий факт.

Следствие. *Число классов дивизоров (в узком смысле) квадратичного поля нечетно тогда и только тогда, когда его дискриминат содержит только одно простое число.*

Такими полями являются $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}\sqrt{-2}$, $\mathbb{Q}(\sqrt{p})$ с простым p вида $4n+1$ и $\mathbb{Q}(\sqrt{-q})$ с простым q вида $4n+3$.

Приведенные нами факты принадлежат к очень небольшому числу известных результатов о строении группы классов дивизоров.

Задачи

1. Доказать, что характер χ квадратичного поля с дискриминантом D в терминах символа Гильберта может быть выражен формулой

$$\chi(a) = \prod_{\mathfrak{p}|D} \left(\frac{a, D}{p}\right), \qquad (a, D) = 1.$$

2. Пусть дискриминант D квадратичного поля не делится на 8. Доказать, что тогда для всякого целого числа γ квадратичного поля, взаимно простого с D, сравнение

$$x^2 \equiv N(\gamma) \pmod{|D|}$$

разрешимо относительно целого рационального x.

3. Те классы чисел по модулю $|D|$, которые сравнимы с нормами целых чисел квадратичного поля, взаимно простых с дискриминантом D, образуют подгруппу H в группе G всех классов чисел mod $|D|$, взаимно простых с D. Доказать, что индекс $(G : H)$ равен 2^t, где t — число различных простых делителей дискриминанта D.

4. Пусть H^* обозначает группу тех классов вычетов по модулю $|D|$, которые сравнимы с нормами целых дивизоров квадратичного поля, взаимно простых с D. Доказать, что $(G : H^*) = 2$.

5. Доказать, что для любого числа γ с положительной нормой из квадратичного поля с дискриминантом D при всех p имеем $\left(\frac{N(\gamma), D}{p}\right) = 1$.

6. Доказать, что целые дивизоры $\mathfrak{a}$ и $\mathfrak{b}$, взаимно простые с D, тогда и только тогда принадлежат одному роду, когда при некотором целом γ выполнено сравнение

$$N(\mathfrak{a}) \equiv N(\gamma) N(\mathfrak{b}) \pmod{|D|}.$$

7. Показать, что в вещественном квадратичном поле, дискриминант которого содержит только одно простое число, норма основной единицы равна -1.

8. Показать, что нетождественный автоморфизм σ: $\alpha \to \alpha^\sigma$ квадратичного поля $\mathbb{Q}(\sqrt{d})$ однозначно определяет на группе дивизоров автоморфизм σ: $\mathfrak{a} \to \mathfrak{a}^\sigma$, для которого $(\alpha^\sigma) = (\alpha)^\sigma$ при всех $\alpha \neq 0$. Выяснить, как действует автоморфизм σ на простых дивизорах.

9. Автоморфизм σ группы дивизоров, определенный в задаче 8, естественным образом индуцирует автоморфизм σ: $C \to C^\sigma$ группы классов дивизоров $\mathfrak{C}$ (в узком смысле). Именно, если $\mathfrak{a} \in C$, то C^σ есть тот класс, который содержит $\mathfrak{a}^\sigma$. Класс C называется инвариантным, если $C^\sigma = C$. Доказать, что класс C инвариантен тогда и только тогда, когда C^2 есть главный класс.

10. Доказать, что подгруппа группы классов дивизоров $\mathfrak{C}$ (в узком смысле), состоящая из инвариантных классов, имеет порядок 2^{t-1} (t — число различных простых делителей дискриминанта).

11. Доказать, что если в квадратичном поле $N(\beta) = 1$, то существует такое α, что

$$N(\alpha) > 0, \qquad \beta = \pm \frac{\alpha^\sigma}{\alpha}.$$

12. Показать, что в каждом инвариантом классе C имеется дивизор $\mathfrak{a}$, для которого $\mathfrak{a}^\sigma = \mathfrak{a}$.

13. Пусть $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ — все попарно различные простые дивизоры, делящие дискриминант D. Показать, что в каждом инвариантом классе C имеется ровно два представителя вида

$$\mathfrak{p}_{i_1} \ldots \mathfrak{p}_{i_k}, \quad 1 \leqslant i_1 < \ldots < i_k \leqslant t, \quad k = 0, 1, \ldots, t.$$

14. Подгруппа тех инвариантных классов, которые содержатся в главном роде, раскладывается, очевидно, в прямое произведение нескольких циклических групп второго порядка. Доказать, что число этих циклических сомножителей равно числу инвариантов группы классов $\mathfrak{C}$ (в узком смысле), делящихся на 4 (относительно определения инвариантов конечной абелевой группы см. п. 1 § 5 Дополнения).

15. Показать, что число положительных делителей r дискриминанта D, свободных от квадратов и удовлетворяющих условию

$$\left(\frac{r, D}{p}\right) = 1 \quad \text{при всех } p,$$

равно числу вида 2^u. Показать, далее, что число инвариантов группы классов $\mathfrak{C}$, делящихся на 4, равно $u - 1$.

16. Пусть m — натуральное число, взаимно простое с индексом f порядка $\mathfrak{O}_f$ в максимальном порядке квадратичного поля $\mathbb{Q}(\sqrt{d})$. Доказать, что число модулей в $\mathbb{Q}(\sqrt{d})$ с кольцом множителей $\mathfrak{O}_f$, содержащихся в $\mathfrak{O}_f$ и имеющих норму m, равно числу целых дивизоров поля $\mathbb{Q}(\sqrt{d})$ с нормой m.

17. Доказать, что число целых дивизоров квадратичного поля $\mathbb{Q}(\sqrt{d})$ с нормой m равно $\sum_{r|m} \chi(r)$, где χ — характер поля $\mathbb{Q}(\sqrt{d})$, а r пробегает все делители натурального числа m.

18. Пусть $g_1(x, y), \ldots, g_s(x, y)$ — полная система попарно неэквивалентных положительных примитивных квадратичных форм дискриминанта $Df^2 < 0$ (D — дискриминант максимального порядка поля $\mathbb{Q}(\sqrt{d})$), и пусть m — натуральное число, взаимно простое с f. Доказать для числа N всех представлений числа m всеми формами $g_1, \ldots, g_s$ формулу

$$N = \varkappa \sum_{r|m} \chi(r),$$

где

$$\varkappa = \begin{cases} 6 & \text{при} \quad D = -3, \quad f = 1, \\ 4 & \text{при} \quad D = -4, \quad f = 1, \\ 2 & \text{при} \quad Df^2 < -4. \end{cases}$$

19. Пусть $g(x, y)$ — положительная форма дискриминанта $Df^2 < -4$ и q — натуральное число, взаимно простое с Df^2. Предположим, что каждый род форм дискриминанта Df^2 состоит из одного класса. Доказать, что если уравнение $g(x, y) = q$ имеет ровно 4 решения в целых взаимно простых x и y, то число q простое.

20. В обозначениях задачи 11 § 7 гл. II доказать, что для числа h_f классов подобных модулей квадратичного поля (в обычном смысле), принадлежащих порядку $\mathfrak{O}_f$, имеет место формула

$$h_f = h \frac{f}{e_f} \prod_{p|f} \left(1 - \frac{\chi(p)}{p}\right),$$

где χ — характер квадратичного поля (p пробегает все простые делители числа f).

21. Показать, что простое число представляется формой $x^2 + 3y^2$ тогда и только тогда, когда оно имеет вид $3n + 1$.

22. Показать, что форма $x^2 - 5y^2$ представляет все простые числа вида $10n \pm 1$ и не представляет простых чисел вида $10n \pm 3$.

23. Показать, что натуральное m представляется формой $x^2 + 2y^2$ со взаимно простыми x и y тогда и только тогда, когда оно имеет вид

$$m = 2^{\alpha} p_1^{\alpha_1} \ldots p_r^{\alpha_r},$$

где $\alpha = 0$ или 1, а каждое простое нечетное p_i имеет вид $8n+1$ или $8n+3$.

24. Доказать существование квадратичных полей (вещественных и мнимых) со сколь угодно большим числом классов дивизоров.

25. Пусть $p_1, \ldots, p_s$ — все попарно различные простые числа, входящие в дискриминант D квадратичного поля $\mathbb{Q}(\sqrt{d})$. Равенства

$$\left(\frac{p_i, D}{p_j}\right) = (-1)^{a_{ij}}, \qquad 1 \leqslant i, j \leqslant s,$$

определяют матрицу (a_{ij}) с элементами из поля вычетов по модулю 2. Обозначим через ρ ранг этой матрицы (в поле $GF(2)$). Доказать, что число инвариантов группы классов дивизоров поля $\mathbb{Q}(\sqrt{d})$ (в узком смысле), делящихся на 4, равно $s - \rho - 1$.

26. Пусть p и q — простые числа, причем $p \neq 2$ и $q \not\equiv p \pmod 4$. Доказать, что число классов дивизоров поля $\mathbb{Q}(\sqrt{-pq})$ делится на 4 тогда и только тогда, когда $\left(\frac{q}{p}\right) = 1$.

27. Пусть $p_1, \ldots, p_s$ — различные простые числа вида $4n+1$, и пусть $d = p_1 \ldots p_s \equiv 1 \pmod 8$. Доказать, что каждый род дивизоров поля $\mathbb{Q}(\sqrt{-d})$ состоит из четного числа классов.

28. Пусть $\mathbb{Q}(\sqrt{d})$ — вещественное квадратичное поле, в дискриминант которого не входят простые числа вида $4n+3$, и ε — основная единица поля $\mathbb{Q}(\sqrt{d})$. Доказать, что если главный род дивизоров поля $\mathbb{Q}(\sqrt{d})$ состоит из нечетного числа классов (в узком смысле), то $N(\varepsilon) = -1$.

29. Пусть p — простое число вида $8n+1$. Доказать, что число классов дивизоров поля $\mathbb{Q}(\sqrt{-p})$ делится на 4.

Добавление при корректуре

В статьях [159], [160] показано, что первый случай теоремы Ферма справедлив для бесконечного числа простых показателей l. Более того, если через $s(N)$ мы обозначим число тех $l \leqslant N$, для которых справедлив первый случай теоремы Ферма, и через $\pi(N)$ — число всех простых $l \leqslant N$, то $s(N)/\pi(N) \to 1$ при $N \to \infty$. Можно сказать, другими словами, что первый случай теоремы Ферма справедлив для «почти всех» l. С другой стороны, из доказанной недавно теоремы Фалтингса очень просто вытекает, что теорема Ферма верна для «почти всех» натуральных показателей. (См. [161].)

Глава IV

ЛОКАЛЬНЫЙ МЕТОД

В § 7 гл. I нами была доказана теорема Минковского — Хассе о представлениях нуля рациональными квадратичными формами. Как сама формулировка этой теоремы, так и ее доказательство требуют вложения поля рациональных чисел $\mathbb{Q}$ в поле p-адических чисел $\mathbb{Q}_p$ и в поле вещественных чисел $\mathbb{Q}_\infty$, т. е. вложения во все пополнения поля $\mathbb{Q}$. Метод решения задач теории чисел, использующий вложения рассматриваемого основного поля в его пополнения, носит название *локального метода*. Этот метод приводит к особенно важным арифметическим следствиям, когда он применяется не только к полю рациональных чисел, но и к произвольному полю алгебраических чисел. Локальный метод является также одним из основных инструментов при изучении полей алгебраических функций.

В этой главе мы изложим ряд общих фактов, связанных с локальным методом в случае произвольного основного поля, а затем в качестве применения локального метода приведем доказательство одного из самых глубоких фактов, относящихся к представлению чисел неполными разложимыми формами (см. определение п. 3 § 1 гл. II). Речь идет о замечательной теореме Туэ, гласящей, что неопределенное уравнение $f(x, y) = c$, где $f(x, y)$ — целочисленный неприводимый однородный многочлен степени $\geqslant 3$, имеет лишь конечное число решений в целых числах. Сам Туэ доказал эту теорему с помощью теории рациональных приближений к алгебраическим числам. Доказательство, основанное на привлечении локального метода, принадлежит Сколему. В доказательстве Сколема приходится, правда, наложить одно небольшое ограничение на многочлен $f(x, y)$, зато это доказательство более прозрачно, чем первоначальное доказательство Туэ.

§ 1. Поля, полные относительно показателей

1. Пополнение поля по показателю. В § 4 гл. I мы видели, что каждому простому числу p, т. е. каждому простому дивизору поля рациональных чисел $\mathbb{Q}$, соответствует p-адическая метрика φ_p поля $\mathbb{Q}$, пополнение по которой приводит нас к полю p-адических чисел $\mathbb{Q}_p$. При определении метрики φ_p мы не используем никаких свойств поля $\mathbb{Q}$, кроме факта существования p-адического показателя ν_p (см. формулу (1) § 4 гл. I). Поэтому построение аналогичных пополнений возможно и для произвольного по-

ля k, если в нем имеется теория дивизоров. Действительно, если простому дивизору $\mathfrak{p}$ поля k соответствует показатель $\nu_{\mathfrak{p}} = \nu$, то, выбрав вещественное ρ, $0 < \rho < 1$, мы можем на k определить метрику $\varphi = \varphi_{\mathfrak{p}}$, полагая

$$\varphi(x) = \rho^{\nu(x)}, \qquad x \in k, \tag{1}$$

а затем, следуя методу п. 1 § 4 гл. I, построить пополнение $\bar{k} = \bar{k}_{\mathfrak{p}}$ поля k по этой метрике. (То, что функция (1) является метрикой, проверяется очевидным образом.) Поле $\bar{k}_{\mathfrak{p}}$ называется $\mathfrak{p}$-*адическим пополнением* поля k. Пополнение $\bar{k} = \bar{k}_{\mathfrak{p}}$, очевидно, не зависит от того, какая рассматривается на k теория дивизоров. Оно вполне определено заданием лишь одного показателя $\nu = \nu_{\mathfrak{p}}$. В силу этого мы его будем называть также *пополнением* k *по показателю* ν. В настоящем параграфе мы изучим некоторые свойства таких пополнений, а также их конечных расширений.

Пусть $\bar{k}$ — пополнение поля k по показателю ν. Покажем, что показатель ν может быть естественным образом продолжен до показателя $\bar{\nu}$ поля $\bar{k}$. В самом деле, в п. 1 § 4 гл. I мы видели, что метрика φ поля k (см. (1)) может быть продолжена до метрики $\bar{\varphi}$ поля $\bar{k}$ так, что если $\alpha \in \bar{k}$ и $\alpha = \lim\limits_{n\to\infty} a_n$, где $a_n \in k$, то $\bar{\varphi}(\alpha) = \lim\limits_{n\to\infty} \varphi(a_n)$. Но в нашем случае нуль является единственной предельной точкой для множества значений $\varphi(a)$, $a \in k$, поэтому последовательность $\{\varphi(a_n)\}$ либо сходится к нулю (если $\alpha = 0$), либо, начиная с некоторого места, стабилизируется (если $\alpha \neq 0$). Следовательно, последовательность $\{\nu(a_n)\}$ стремится к бесконечности при $\alpha = 0$ и также стабилизируется при $\alpha \neq 0$. Мы можем поэтому положить $\bar{\nu}(\alpha) = \lim\limits_{n\to\infty} \nu(\alpha_n)$. Легко проверяется теперь, что так определенная функция $\bar{\nu}(\alpha)$ (значения которой не зависят, очевидно, от выбора последовательности $\{a_n\}$) является показателем поля $\bar{k}$, причем $\bar{\nu}(a) = \nu(a)$ для всех $a \in k$. Очевидно также, что метрика $\bar{\varphi}$ поля $\bar{k}$ связана с показателем $\bar{\nu}$ соотношением

$$\bar{\varphi}(\alpha) = \rho^{\bar{\nu}(\alpha)}, \qquad \alpha \in \bar{k}.$$

В дальнейшем аналогично тому, как это мы уже делали в случае поля p-адических чисел (см. п. 4 § 3 гл. I), сходимость в поле $\bar{k}$ будет выражаться в терминах показателя $\bar{\nu}$ (вместо метрики $\bar{\varphi}$).

Пусть $\mathfrak{o}$ — кольцо показателя ν, т. е. кольцо тех элементов $a \in k$, для которых $\nu(a) \geqslant 0$ (см. п. 1 § 4 гл. III). Покажем, что замыкание $\bar{\mathfrak{o}}$ кольца $\mathfrak{o}$ в поле $\bar{k}$ совпадает с кольцом показателя $\bar{\nu}$ (замыканием $\bar{A}$ любого подмножества $A \subset \bar{k}$ называется совокуп-

ность всех тех элементов из $\bar{k}$, которые являются пределами последовательностей элементов из A). В самом деле, если $a \in \bar{\mathfrak{o}}$, то $\alpha = \lim\limits_{n\to\infty} a_n$, где $a_n \in \mathfrak{o}$, откуда $\bar{v}(\alpha) = \lim\limits_{n\to\infty} v(a_n) \geqslant 0$. Обратно, пусть $\bar{v}(\alpha) \geqslant 0$. Так как α является пределом последовательности элементов из k, то для всякого натурального n найдется такой элемент $a_n \in k$, что $\bar{v}(\alpha - a_n) \geqslant n$. Тогда $\alpha = \lim\limits_{n\to\infty} a_n$, причем

$$v(a_n) = \bar{v}(\alpha - (\alpha - a_n)) \geqslant \min(\bar{v}(\alpha), \bar{v}(\alpha - a_n)) \geqslant 0,$$

т. е. $a_n \in \mathfrak{o}$. Наше утверждение, таким образом, доказано.

Согласно теореме 2 § 4 гл. III в кольце $\mathfrak{o}$ с точностью до ассоциированности имеется только один простой элемент π, характеризуемый условием $v(\pi) = 1$. Он же будет простым элементом и в кольце $\bar{\mathfrak{o}}$ (так как $\bar{v}(\pi) = 1$). Обозначим через Σ_v и $\Sigma_{\bar{v}}$ поля вычетов показателей v и $\bar{v}$ соответственно (см. конец п. 1 § 4 гл. III). Так как сравнение в кольце $\mathfrak{o}$ по модулю π равносильно аналогичному сравнению и в кольце $\bar{\mathfrak{o}}$, то мы имеем естественный изоморфизм поля Σ_v в поле $\Sigma_{\bar{v}}$. С другой стороны, для всякого $\alpha \in \bar{\mathfrak{o}}$ существует элемент $a \in \mathfrak{o}$, для которого $\bar{v}(\alpha - a) \geqslant 1$, т. е. $\alpha \equiv a \pmod{\pi}$. Последнее означает, что отображение $\Sigma_v \to \Sigma_{\bar{v}}$ является изоморфизмом на все поле $\Sigma_{\bar{v}}$. В силу этого изоморфизма поле вычетов $\Sigma_{\bar{v}}$ обычно отождествляют с Σ_v.

2. Представление элементов в виде рядов. В этом пункте мы будем считать, что k — полное поле относительно показателя v (т. е. полное поле относительно метрики (1)). Кольцо $\mathfrak{o}$ показателя v называется в этом случае *кольцом целых элементов* поля k. Через π мы обозначим какой-нибудь фиксированный простой элемент кольца $\mathfrak{o}$.

Поле вычетов Σ показателя v мы будем в этом случае называть также *полем вычетов* поля k.

Для рядов в поле k справедливо, очевидно, все то, что было сказано в п. 4 § 3 гл. I о p-адических рядах; в частности, справедлива теорема 8 § 3 гл. I.

Выбрав произвольно целые α_n $(m \leqslant n < \infty)$, рассмотрим ряд

$$\sum_{n=m}^{\infty} \alpha_n \pi^n. \tag{2}$$

Так как $v(\alpha_n \pi^n) = v(\alpha_n) + n \geqslant n$, то $\alpha_n \pi^n \to 0$ при $n \to \infty$, т. е. общий член ряда (2) стремится к нулю. Следовательно, ряд (2) сходится и его сумма равна некоторому элементу из k. В связи с этим возникает вопрос, нельзя ли всякий элемент из k представить в виде суммы (2), и если это возможно, то нельзя ли (подобно случаю поля p-адических чисел, теорема 10 § 3 гл. I) ука-

зать для элементов из k некоторые канонические представления такого рода. Ответ оказывается утвердительным.

Выберем в кольце $\mathfrak{o}$ какую-нибудь полную систему вычетов S по модулю π. Относительно системы S мы будем предполагать, что $0 \in S$, т. е. что в классе элементов кольца $\mathfrak{o}$, делящихся на π, в качестве представителя взят нуль.

Теорема 1. *Пусть k — полное поле с показателем ν, $\mathfrak{o}$ — кольцо целых элементов поля k, π — простой элемент в $\mathfrak{o}$ и S — полная система вычетов (содержащая нуль) кольца $\mathfrak{o}$ по модулю π. Тогда всякий элемент $\alpha \in k$ может быть представлен в виде суммы ряда*

$$\alpha = \sum_{i=m}^{\infty} a_i \pi^i, \tag{3}$$

в котором $a_i \in S$ $(m \leqslant i < \infty)$, и такое представление единственно (при фиксированной системе вычетов S и фиксированном π).

Доказательство. Для $\alpha = 0$ имеем представление $0 = \sum_{i=0}^{\infty} 0 \cdot \pi^i$. Пусть $\alpha \neq 0$. Если $\nu(\alpha) = m$, то $\nu(\alpha\pi^{-m}) = 0$. Элемент $\alpha\pi^{-m}$ из $\mathfrak{o}$ сравним по модулю π с некоторым элементом из S, скажем с a_m. Так как $\alpha\pi^{-m} - a_m = \pi\xi$, где $\xi \in \mathfrak{o}$, то

$$\alpha = a_m \pi^m + \xi\pi^{m+1}.$$

Предположим, что для некоторого $n > m$ нами найдено представление

$$\alpha = a_m\pi^m + \ldots + a_{n-1}\pi^{n-1} + \eta_n\pi^n,$$

где $a_i \in S$ $(m \leqslant i \leqslant n-1)$, $\eta_n \in \mathfrak{o}$. Выберем такое $a_n \in S$, что $\eta_n \equiv a_n \pmod{\pi}$. Так как $\eta_n = a_n + \eta_{n+1}\pi$, где $\eta_{n+1} \in \mathfrak{o}$, то для α получаем представление

$$\alpha = a_m\pi^m + \ldots + a_n\pi^n + \eta_{n+1}\pi^{n+1}.$$

Продолжим этот процесс до бесконечности. Так как $\nu(\eta_n\pi^n) \geqslant n$, то $\eta_n\pi^n \to 0$ при $n \to \infty$, а значит, $\alpha = \sum_{i=m}^{\infty} a_i\pi^i$.

Если в ряде (3) не все коэффициенты a_n равны нулю, то можно считать, что $a_m \neq 0$. В этом случае $\nu(a_m) = 0$, так как в кольце $\mathfrak{o}$ все элементы, не делящиеся на π, являются единицами. Но тогда

$$\nu\left(\sum_{i=m}^{\infty} a_i\pi^i\right) = \nu(a_m\pi^m) = m.$$

Отсюда следует единственность представления для $\alpha = 0$. Предположим теперь, что для $\alpha \neq 0$ мы имеем два представления:

$$\alpha = \sum_{i=m}^{\infty} a_i\pi^i = \sum_{i=m'}^{\infty} a'_i\pi^i, \qquad a_i, a'_i \in S.$$

Если в этих представлениях $a_m \neq 0$ и $a'_{m'} \neq 0$, то по только что доказанному $m = m'$. Пусть уже установлено, что $a_i = a'_i$ для $m \leqslant i < n$ $(n \geqslant m)$. Умножим равенство $\sum_{i=n}^{\infty} a_i \pi^i = \sum_{i=n}^{\infty} a'_i \pi^i$ на π^{-n}. Переходя к сравнению по модулю π, мы получим, что $a_n \equiv a'_n \pmod{\pi}$, а так как $a_n \in S$ и $a'_n \in S$, то $a_n = a'_n$. Этим теорема 1 доказана.

Заметим, что в случае, когда $k = \mathbb{Q}_p$, $\pi = p$ и $S = (0, 1, \ldots, p-1)$, теорема 1 превращается в теорему 10 § 3 гл. I.

Следствие. *В обозначениях теоремы 1 каждый целый элемент $\alpha \in k$ однозначно представляется в виде*

$$\alpha = a_0 + a_1\pi + \ldots + a_n\pi^n + \ldots, \qquad a_n \in S. \tag{4}$$

Легко видеть, что для рядов в поле k справедлива теорема 9 § 3 гл. I. В силу этого сходящиеся ряды в k можно перемножать по обычным правилам анализа. В частности, с рядами вида (2) мы можем обращаться как со степенными рядами от π. Но при выполнении действий над рядами вида (3) по правилам степенных рядов надо иметь в виду, что при сложении и умножении двух таких рядов в результате может получиться ряд вида (2), в котором коэффициенты α_n уже не принадлежат системе вычетов S. В этом случае полученный ряд мы должны преобразовать к виду (3), заменяя последовательно каждый коэффициент $\alpha_n \in \mathfrak{o}$ его вычетом $a_n \in S$, определяемым равенством $\alpha_n = a_n + \pi\gamma_n$, и присоединяя на каждом шаге элемент $\gamma_n \in \mathfrak{o}$ к следующему коэффициенту.

Замечание 1. Представление элементов в полном поле с показателем в виде рядов (3) зависит, конечно, от выбора системы представителей S. Среди множества различных систем представителей во многих важных случаях существуют «наилучшие» системы, обладающие свойством мультипликативной замкнутости или даже являющиеся подполями поля k (см. по этому поводу задачи 7—11).

Замечание 2. Полученные нами здесь результаты являются обобщениями аналогичных фактов для случая поля p-адических чисел (см. п. 4 § 3 гл. I). Следует предупредить, однако, что теорема 6 § 3 гл. I для произвольных полных полей с показателем перестает быть справедливой. Она сохраняется только для тех полей k, для которых поле вычетов Σ кольца $\mathfrak{o}$ по простому элементу π конечно. Так же обстоит дело и с теоремами 1 и 2 § 5 гл. I (в которых под F надо понимать многочлен с коэффициентами из $\mathfrak{o}$). Что касается теоремы 3 § 5 гл. I, то она вместе с доказательством почти дословно переносится на случай произвольного полного поля k с показателем. В дальнейшем мы воспользуемся следствием этой теоремы в следующей форме: *если для многочлена $F(X)$ с целыми коэффициентами из k и для целого*

$\xi \in k$ мы имеем $F(\xi) \equiv 0 \pmod{\pi}$ и $F'(\xi) \not\equiv 0 \pmod{\pi}$, то в k существует целый элемент θ, для которого $\xi \equiv \theta \pmod{\pi}$ и $F(\theta) = 0$.

3. Конечные расширения полного поля с показателем. Пусть k — полное поле относительно показателя ν_0. Над этим полем существует достаточно много конечных расширений (см. задачу 9 § 3 гл. III). Пусть K — расширение поля k степени n. По теореме 5 § 4 гл. III на поле K существует показатель ν, являющийся продолжением ν_0. Нашей целью является доказательство того, что продолжение ν *в данном случае* существует только *одно*, а также, что относительно показателя ν поле K полно.

Пусть L — подмножество поля K, являющееся линейным пространством над полем k, и $\omega_1, \ldots, \omega_s$ — базис L над k. Каждый элемент α из L однозначно представляется тогда в виде

$$\alpha = a_1\omega_1 + \ldots + a_s\omega_s, \qquad a_i \in k. \tag{5}$$

Если $\nu_0(a_i) \geqslant N$ $(i = 1, \ldots, s)$, то по свойствам показателей

$$\nu(\alpha) \geqslant \min \nu(a_i\omega_i) \geqslant eN + \min \nu(\omega_i),$$

где e обозначает индекс ветвления показателя ν относительно ν_0 (см. определение п. 3 § 4 гл. III). Покажем, что и, обратно, все коэффициенты a_i в разложении (5) будут сколь угодно малыми относительно ν_0, если только элемент $\alpha \in L$ будет достаточно мал относительно ν. (Напомним, что «малые» элементы относительно метрики вида (1) характеризуются большим значением показателя ν.) Более точно это означает, что для любого N можно найти такое M, что неравенства $\nu_0(a_i) \geqslant N$ $(i = 1, \ldots, s)$ будут справедливы всякий раз, когда $\nu(\alpha) \geqslant M$. При $s = 1$ это утверждение очевидно. Доказательство его в общем случае проведем индукцией по s. Пусть $s \geqslant 2$, и пусть вопреки нашему утверждению для некоторого N существуют элементы $\alpha \in L$ со сколь угодно большим значением $\nu(\alpha)$, для которых хоть один коэффициент a_i в разложении (5) удовлетворяет неравенству $\nu_0(a_i) < N$. Можно считать, очевидно, что этому неравенству каждый раз удовлетворяет первый коэффициент a_1. Для любого натурального r мы можем тогда выбрать элемент $\alpha_r \in L$, для которого $\nu(\alpha_r) \geqslant r + eN$ и в то же время коэффициент $a_1^{(r)}$ в разложении

$$\alpha_r = a_1^{(r)}\omega_1 + \ldots + a_s^{(r)}\omega_s, \qquad a_i^{(r)} \in k,$$

удовлетворяет неравенству $\nu_0(a_1^{(r)}) < N$. Рассмотрим последовательность $\{\beta_r\}$, где

$$\beta_r \doteq \alpha_r a_1^{(r)-1} = \omega_1 + b_2^{(r)}\omega_2 + \ldots + b_s^{(r)}\omega_s. \tag{6}$$

Так как $\nu(\beta_r) = \nu(\alpha_r) - e\nu_0(a_1^{(r)})$, то $\nu(\beta_r) > r$. Разности

$$\beta_{r+1} - \beta_r = \sum_{i=2}^{s} (b_i^{(r+1)} - b_i^{(r)})\omega_i$$

все принадлежат подпространству размерности $s-1$ (порожденному элементами $\omega_2, \ldots, \omega_s$), и для них

$$v(\beta_{r+1}-\beta_r) \geqslant \min(v(\beta_{r+1}), v(\beta_r)) > r,$$

т. е. $v(\beta_{r+1}-\beta_r) \to \infty$ при $r \to \infty$. Но тогда по индуктивному предположению при любом $i=2, \ldots, s$ мы имеем также

$$v\left(b_i^{(r+1)} - b_i^{(r)}\right) \to \infty \quad \text{при} \quad r \to \infty.$$

Следовательно, в силу полноты поля k (см. теорему 7 § 3 гл. I) последовательность $\{b_i^{(r)}\}_{r=1}^{\infty}$ сходится к некоторому элементу $b_i \in k$. Переходя теперь в равенстве (6) к пределу при $r \to \infty$ и замечая, что $\beta_r \to 0$, получаем равенство

$$\omega_1 + b_2\omega_2 + \ldots + b_s\omega_s = 0,$$

которое противоречит, однако, линейной независимости элементов $\omega_1, \ldots, \omega_s$ над полем k. Полученное противоречие и доказывает наше утверждение.

Возьмем теперь в качестве L все поле K. Если последовательность $\{\alpha_r\}$ элементов из K фундаментальна, т. е. $v(\alpha_{r+1}-\alpha_r) \to \infty$ при $r \to \infty$, то по доказанному все последовательности $\{a_i^{(r)}\}_{r=1}^{\infty}$, определяемые разложениями

$$\alpha_r = a_1^{(r)}\omega_1 + \ldots + a_n^{(r)}\omega_n, \qquad a_i^{(r)} \in k \tag{7}$$

(здесь $\omega_1, \ldots, \omega_n$ — базис K над k), будут сходящимися в поле k. Но тогда вместе с ними сходящейся будет и последовательность $\{\alpha_r\}$. Это доказывает полноту поля K относительно показателя v. Кроме того, мы видим, что сходимость в поле K по показателю v однозначно определена сходимостью в поле k (относительно показателя v_0).

Из последнего факта легко вытекает единственность продолжения показателя v_0 на поле K. В самом деле, пусть помимо v существует другое продолжение v', отличное от v. По независимости показателей в поле K существует тогда элемент α, для которого $v(\alpha) > 0$ и $v'(\alpha) = 0$. Последовательность $\{\alpha^r\}$ будет, очевидно, сходиться к нулю относительно показателя v, но не будет сходящейся относительно показателя v' (поскольку $v'(\alpha^{r+1}-\alpha^r) = v'(\alpha-1)$ не стремится к бесконечности). Этим получено противоречие, так как по доказанному сходимость в K не зависит от продолжения показателя v_0 на поле K.

Нами получена, таким образом, следующая теорема.

Теорема 2. *Пусть k — полное поле относительно показателя v_0 и K — его конечное расширение. Для показателя v_0 существует только одно продолжение v на поле K. Поле K полно относительно v, и для любого базиса $\omega_1, \ldots, \omega_n$ расширения K/k последовательность $\{\alpha_r\}$, $\alpha_r \in K$, будет сходящейся тогда и только*

тогда, когда все последовательности $\{a_i^{(\nu)}\}$ $(1 \leqslant i \leqslant n)$, *определенные разложениями* (7), *сходятся в поле* k.

4. Целые элементы. Обратимся к изучению взаимоотношений между кольцом $\mathfrak{o}$ целых элементов полного поля k относительно показателя v_0 и кольцом $\mathfrak{O}$ целых элементов конечного расширения K/k. Так как для показателя v_0 мы имеем только одно продолжение v на поле K, то по теореме 6 § 4 гл. III кольцо $\mathfrak{O}$ (т. е. кольцо показателя v) совпадает с целым замыканием кольца $\mathfrak{o}$ в поле K. Следовательно, для любого элемента $\alpha \in \mathfrak{O}$ его норма $N(\alpha) = N_{K/k}(\alpha)$ принадлежит $\mathfrak{o}$, и, значит, норма $N(\varepsilon)$ всякой единицы ε кольца $\mathfrak{O}$ является единицей в кольце $\mathfrak{o}$. Пусть теперь $\alpha \notin \mathfrak{O}$. Так как $\alpha^{-1} \in \mathfrak{O}$ и не является единицей в $\mathfrak{O}$, то $N(\alpha^{-1}) = N(\alpha)^{-1}$ принадлежит $\mathfrak{o}$ и не является единицей в $\mathfrak{o}$. Но в таком случае $N(\alpha) = (N(\alpha)^{-1})^{-1}$ не принадлежит кольцу $\mathfrak{o}$. Этим доказана следующая теорема.

Теорема 3. *Для того чтобы элемент* α *из конечного расширения* K/k *полного поля с показателем был целым, необходимо и достаточно, чтобы его норма* $N_{K/k}(\alpha)$ *была целым элементом в* k.

Следствие. *Элемент* $\varepsilon \in K$ *является единицей кольца* $\mathfrak{O}$ *тогда и только тогда, когда его норма* $N(\varepsilon)$ *есть единица кольца* $\mathfrak{o}$.

Кольца $\mathfrak{o}$ и $\mathfrak{O}$ мы можем рассматривать, конечно, как кольца, в которых имеется теория дивизоров. Обозначим через $\mathfrak{p}$ и $\mathfrak{P}$ (единственные) простые дивизоры этих колец. Степень инерции f дивизора $\mathfrak{P}$ относительно $\mathfrak{p}$, т. е. степень $(\Sigma : \Sigma_0)$ поля вычетов Σ поля K над полем вычетов Σ_0 поля k, называется в данном случае также *степенью инерции расширения* K/k. Аналогично индекс ветвления e дивизора $\mathfrak{P}$ относительно $\mathfrak{p}$ называется *индексом ветвления расширения* K/k. Если π_0 и π — простые элементы колец $\mathfrak{o}$ и $\mathfrak{O}$ соответственно, то, как мы знаем,

$$\pi_0 = \pi^e \varepsilon, \tag{8}$$

где ε — единица кольца $\mathfrak{O}$.

Пусть S_0 — некоторая полная система вычетов в кольце $\mathfrak{o}$ по модулю π_0. Как и ранее, мы будем предполагать, что $0 \in S_0$. Легко видеть, что если классы вычетов $\omega_1, \ldots, \omega_f$ из Σ образуют базис расширения Σ/Σ_0, то совокупность S, состоящая из линейных комбинаций

$$a_1\omega_1 + \ldots + a_f\omega_f, \tag{9}$$

где $a_1, \ldots, a_f$ независимо друг от друга пробегают все элементы из S_0, является полной системой вычетов в кольце $\mathfrak{O}$ по модулю π.

Определение. *Базис* $\theta_1, \ldots, \theta_n$ *поля* K *над* k *называется фундаментальным, если все* θ_i *целые и в разложении*

$$\alpha = a_1\theta_1 + \ldots + a_n\theta_n, \qquad a_i \in k$$

любого целого $\alpha \in K$ *все коэффициенты* a_i *являются целыми в* k.

Теорема 4. *Пусть k — полное поле относительно показателя v_0 и K — его конечное расширение индекса ветвления e и степени инерции f. Пусть, далее, Σ_0 и Σ — поля вычетов полей k и K, соответственно. Если π — простой элемент кольца целых элементов поля K, а $\bar{\omega}_1, \ldots, \bar{\omega}_f$ — классы вычетов из Σ, образующие базис Σ над Σ_0, то система элементов*

$$\omega_i \pi^j, \quad i = 1, \ldots, f; \quad j = 0, 1, \ldots, e-1, \tag{10}$$

является фундаментальным базисом расширения K/k.

Доказательство. Докажем прежде всего, что элементы (10) линейно независимы относительно k. Допуская противное, предположим, что $\sum_{i=1}^{f} \sum_{j=0}^{e-1} a_{ij} \omega_i \pi^j = 0$, где a_{ij} — элементы из k, не равные нулю одновременно. Мы можем считать, что все a_{ij} целые и хоть один из них есть единица в $\mathfrak{o}$ (если это не так, то наше соотношение надо умножить на подходящую степень простого элемента $\pi_0 \in \mathfrak{o}$). Пусть j_0 $(0 \leqslant j_0 \leqslant e-1)$ есть наименьший индекс, для которого существует такое i_0 $(1 \leqslant i_0 \leqslant f)$, что $a_{i_0 j_0}$ — единица в $\mathfrak{o}$. Следовательно, если $j < j_0$, то $v_0(a_{ij}) \geqslant 1$ для всех i. Так как $\sum_{i=1}^{f} \bar{a}_{ij_0} \bar{\omega}_i \neq \bar{0}$, то сумма $\sum_{i=1}^{f} a_{ij_0} \omega_i$ не делится на π, а поэтому для элемента

$$\gamma = \sum_{i=1}^{f} a_{ij_0} \omega_i \pi^{j_0}$$

мы имеем $v(\gamma) = j_0 + v\left(\sum_{i=1}^{f} a_{ij_0} \omega_i\right) = j_0$. С другой стороны,

$$\gamma = -\sum_{i=1}^{f} \sum_{j \neq j_0} a_{ij} \omega_i \pi^j.$$

Если $j < j_0$, то $v(a_{ij} \omega_i \pi^j) = j + v(a_{ij}) \geqslant e v_0(a_{ij}) \geqslant e > j_0$. Если же $j > j_0$, то $v(a_{ij} \omega_i \pi^j) = j + v(a_{ij}) \geqslant j > j_0$. Следовательно,

$$v(\gamma) \geqslant \min_{j \neq j_0} v(a_{ij} \omega_i \pi^j) > j_0.$$

Полученное противоречие и доказывает линейную независимость элементов (10) над полем k.

Пусть теперь α — произвольный элемент из $\mathfrak{O}$. В силу следствия теоремы 1 мы имеем сравнение

$$\alpha \equiv \xi_0 + \xi_1 \pi + \ldots + \xi_{e-1} \pi^{e-1} \pmod{\pi^e},$$

где ξ_i — элементы из некоторой фиксированной системы вычетов S в кольце $\mathfrak{O}$ по модулю π. В качестве S мы возьмем систему вычетов, состоящую из чисел вида (9). Так как π_0 и π^e ассоцииро-

ваны в $\mathfrak{O}$ (см. равенство (8)), то сравнения в кольце $\mathfrak{O}$ по модулям π_0 и π^e эквивалентны. Мы имеем, следовательно, сравнение

$$\alpha \equiv \sum_{i=1}^{f}\sum_{j=0}^{e-1} a_{ij}^{(0)}\omega_i\pi^j \pmod{\pi_0}, \qquad a_{ij}^{(0)} \in S_0,$$

а значит,

$$\alpha = \sum_{i=1}^{f}\sum_{j=0}^{e-1} a_{ij}^{(0)}\omega_i\pi^j + \pi_0\alpha_1, \qquad \alpha_1 \in \mathfrak{O}.$$

Аналогично

$$\alpha_1 = \sum_{i=1}^{f}\sum_{j=0}^{e-1} a_{ij}^{(1)}\omega_i\pi^j + \pi_0\alpha_2, \qquad \alpha_2 \in \mathfrak{O}, \qquad a_{ij}^{(1)} \in S_0.$$

Продолжая этот процесс до бесконечности, получим последовательность равенств

$$\alpha_n = \sum_{i=1}^{f}\sum_{j=0}^{e-1} a_{ij}^{(n)}\omega_i\pi^j + \pi_0\alpha_{n+1}, \qquad \alpha_{n+1} \in \mathfrak{O}, \qquad a_{ij}^{(n)} \in S_0.$$

При фиксированных i и j имеем бесконечную последовательность $\{a_{ij}^{(n)}\}$. Рассмотрим ряд $\sum_{n=0}^{\infty} a_{ij}^{(n)}\pi_0^n$. Поскольку $a_{ij}^{(n)}$ целые, то этот ряд сходится и его сумма a_{ij} есть целый элемент поля k, т. е. $a_{ij} \in \mathfrak{o}$. Докажем, что

$$\alpha = \sum_{i=1}^{f}\sum_{j=0}^{e-1} a_{ij}\omega_i\pi^j. \tag{11}$$

Действительно, по построению элементов $\alpha_1, \alpha_2 \ldots$ мы имеем

$$\alpha = \sum_{r=0}^{n-1}\left(\sum_{i=1}^{f}\sum_{j=0}^{e-1} a_{ij}^{(r)}\omega_i\pi^j\right)\pi_0^r + \pi_0^n\alpha_n,$$

откуда следует, что разность $\alpha - \left(\sum_{i=1}^{f}\sum_{j=0}^{e-1} a_{ij}\omega_i\pi^j\right)$ делится на π_0^n (в кольце $\mathfrak{O}$). Поскольку это верно для любого n, то эта разность должна быть равна нулю, и равенство (11) доказано.

Если β — произвольный элемент из K, то при некотором m элемент $\beta\pi_0^m$ будет целым. Представив его в виде (11), мы видим, что β является линейной комбинацией элементов (10) с коэффициентами из k. Таким образом, система (10) есть базис поля K над k, а так как для целого $\alpha \in K$ в представлении (11) все коэффициенты a_{ij} принадлежат $\mathfrak{o}$, то этот базис фундаментальный. Теорема 4 доказана.

Так как число элементов в базисе (10) равно fe, то мы имеем также следующий результат.

Теорема 5. *Индекс ветвления e и степень инерции f конечного расширения K/k полного поля с показателем связаны со степенью $n=(K:k)$ соотношением $fe=n$.*

Положим $N_{K/k}(\pi)=\pi_0^m u$, где u — единица кольца $\mathfrak{o}$. Переходя в равенстве (8) к нормам, мы получим

$$N_{K/k}(\pi_0)=\pi_0^n=N_{K/k}(\pi^e\varepsilon)=\pi_0^{me}u^eN_{K/k}(\varepsilon)=\pi_0^{me}v,$$

где v — также единица в $\mathfrak{o}$. Отсюда следует, что $n=me$ (и $v=1$), а значит, $m=f$. Таким образом, степень инерции f расширения K/k может быть определена также равенством

$$f=v_0(N_{K/k}(\pi)), \tag{12}$$

где π — простой элемент кольца целых элементов поля K. Отсюда легко получаем, что для любого α из поля K справедлива формула

$$v_0(N_{K/k}(\alpha))=fv(\alpha). \tag{13}$$

Заметим, что равенство (12) и теорема 5 являются также непосредственными следствиями теоремы 5 и формулы (12) из § 5 гл. III.

Определение. *Если $e=1$, то расширение K/k называется неразветвленным. Если же $e=n$, то K/k называется вполне разветвленным.*

Из теоремы 5 следует, что степень инерции неразветвленного расширения совпадает со степенью этого расширения. Для вполне разветвленных расширений поле вычетов Σ совпадает с Σ_0 (в смысле естественного отождествления), т. е. каждый целый элемент из K сравним по модулю π с целым элементом из k.

Можно показать (задача 12), что в случае, когда поле вычетов Σ поля K сепарабельно над полем вычетов Σ_0 поля k для расширения K/k, существует однозначно определенное промежуточное поле T, такое, что расширение T/k не разветвлено, а K/T вполне разветвлено. Поле T называется *полем инерции* расширения K/k.

5. Поля формальных степенных рядов. К числу полных полей относительно показателя относятся поля формальных степенных рядов. Эти поля конструируются следующим образом.

Пусть k_0 — произвольное поле. Совокупность $\mathfrak{o}$ всех формальных рядов вида

$$a_0+a_1t+a_2t^2+\ldots+a_nt^n+\ldots, \qquad a_n\in k_0, \tag{14}$$

от переменной t относительно обычных действий над степенными рядами образует коммутативное кольцо с единицей 1. Это кольцо не имеет делителей нуля, и единицами в нем являются, как легко видеть, те и только те ряды (14), у которых $a_0\neq 0$. Поле отношений кольца $\mathfrak{o}$ и называется *полем формальных степенных рядов* от t над полем k_0. Оно обозначается через $k_0\{t\}$. Аналогично случаю поля p-адических чисел (см. п. 3 § 3 гл. I) всякий отличный

от нуля элемент ξ поля $k_0\{t\}$ однозначно представляется в виде

$$\xi = t^m(c_0 + c_1 t + \ldots + c_n t^n + \ldots), \qquad c_n \in k_0, \quad c_0 \neq 0,$$

с некоторым целым m (положительным, отрицательным или равным нулю). Полагая $\nu(\xi) = m$ при $\xi \neq 0$ и $\nu(0) = \infty$, мы получаем показатель ν, относительно которого поле $k_0\{t\}$, как легко проверяется, полно. Кольцо показателя ν совпадает, очевидно, с кольцом o рядов вида (14). В качестве простого элемента в o можно взять t. Так как два ряда вида (14) сравнимы по модулю t тогда и только тогда, когда их свободные члены совпадают, то получаем, что в каждом классе вычетов кольца o по модулю t имеется единственный представитель из k_0. Таким образом, поле вычетов Σ_0 поля $k_0\{t\}$ естественным образом изоморфно полю k_0.

Легко видеть, что поле формальных степенных рядов $k_0\{t\}$ есть не что иное, как пополнение поля рациональных функций $k_0(t)$ по показателю, соответствующему неприводимому многочлену t из кольца $k_0[t]$ (см. задачу 7 § 4 гл. I).

Так как $k_0 \subset k_0\{t\}$ и $k_0 \approx \Sigma_0$, то характеристика поля формальных степенных рядов совпадает с характеристикой его поля вычетов. Это свойство, оказывается, и характеризует поля формальных степенных рядов среди всех полных полей относительно показателей. Именно, если характеристика полного (относительно показателя) поля k совпадает с характеристикой его поля вычетов, то в k существует подполе k_0, элементы которого образуют полную систему вычетов по модулю простого элемента π. Но при такой системе вычетов действия над рядами (3) будут производиться по правилам действий над степенными рядами, а значит, k будет полем формальных степенных рядов от π с коэффициентами из k_0. Доказательство существования подполя k_0 в общем случае довольно сложно, и мы проводить его не будем.

(Два частных случая, в которых доказательство сравнительно нетрудно, указаны в задачах 7 и 11.)

Если k_0' — расширение поля k_0, то $k_0'\{t\}$ является, очевидно, расширением поля $k_0\{t\}$, при этом, если k_0'/k_0 конечно, то $k_0'\{t\}/k_0\{t\}$ также конечно и имеет ту же степень. Другой способ построения конечных расширений поля $k_0\{t\}$ состоит в его изоморфном вложении в поле $k_0\{u\}$, при котором $t \to u^n$ (n натуральное). Если мы отождествим поле $k_0\{t\}$ с его образом при этом отображении, т. е. положим $t = u^n$, то $k_0\{u\}$ будет конечным расширением $k_0\{t\}$ степени n. Ясно, что $k_0\{u\}$ получается из $k_0\{t\}$ присоединением корня n-й степени из t.

В случае полей характеристики нуль к этим двум типам расширений сводятся любые конечные расширения поля $k_0\{t\}$. Точнее, имеет место следующий факт.

Теорема 6. *Пусть k_0 — поле характеристики нуль. Каждое конечное расширение K/k поля формальных степенных рядов*

$k = k_0\{t\}$ индекса ветвления e является подполем расширения вида $k_0'\{u\}$, где k_0' — конечное расширение над k_0 и $u^e = t$.

Доказательство. Обозначим через Σ_0 и Σ поля вычетов полей k и K соответственно, через f — степень инерции расширения K/k, через π — какой-нибудь простой элемент поля K и для любого целого $\xi \in K$ через $\bar{\xi}$ — класс вычетов из Σ, содержащий ξ в качестве представителя. Элементы поля k_0 образуют, как мы видели, естественную систему представителей для классов вычетов из Σ_0. Покажем прежде всего, что и в поле K существует подполе S, содержащее k_0 и являющееся полной системой представителей для классов вычетов из Σ. Так как всякое конечное расширение поля нулевой характеристики является простым, то $\Sigma = \Sigma_0(\bar{\xi})$, где $\bar{\xi}$ — некоторый класс вычетов из Σ. Обозначим через $\bar{F}$ минимальный многочлен элемента $\bar{\xi}$ над Σ_0. Заменяя все коэффициенты многочлена $\bar{F}$ (являющиеся классами вычетов из Σ_0) соответствующими вычетами из k_0, мы получим неприводимый над k_0 многочлен F степени f, для которого

$$F(\xi) \equiv 0 \pmod{\pi} \qquad \text{и} \qquad F'(\xi) \not\equiv 0 \pmod{\pi}.$$

Согласно замечанию 2, сделанному в конце п. 2, в поле K существует такой целый элемент θ, что $\bar{\theta} = \bar{\xi}$ и $F(\theta) = 0$. Рассмотрим подполе $S = k_0(\theta)$ поля K. Так как θ является корнем неприводимого многочлена степени f с коэффициентами из k_0, то $(S : k_0) = f$ и каждый элемент из S однозначно представляется в виде

$$a_0 + a_1\theta + \ldots + a_{f-1}\theta^{f-1}, \qquad a_i \in k_0.$$

Соответствующие этим элементам классы вычетов по модулю π (ввиду равенства $\bar{\theta} = \bar{\xi}$) совпадают с классами вычетов $\bar{a}_0 + \bar{a}_1\bar{\xi} + \ldots + \bar{a}_{f-1}\bar{\xi}^{f-1}$. Но поскольку $\Sigma = \Sigma_0(\bar{\xi})$ и $(\Sigma : \Sigma_0) = f$, то такие линейные комбинации исчерпывают собой без повторений все классы вычетов из Σ. Этим и доказано, что элементы подполя S (являющегося конечным расширением поля k_0) составляют полную систему представителей из классов вычетов Σ.

Согласно теореме 1 поле K является полем формальных степенных рядов от π с коэффициентами из S, т. е. $K = S\{\pi\}$. Теорема 6 была бы доказана (причем в более сильной форме), если бы удалось показать, что простой элемент π можно выбрать так, чтобы он был корнем степени e из t. Однако такой выбор π в самом поле K не всегда возможен, и нам надо будет поэтому перейти к некоторому конечному расширению k_0' поля коэффициентов S.

Ввиду (8) мы имеем равенство

$$t = \pi^e\varepsilon, \tag{15}$$

где ε — единица кольца целых элементов поля K. Обозначим через α тот элемент из S, для которого $\alpha \equiv \varepsilon \pmod{\pi}$, и через k_0' поле $S\left(\sqrt[e]{\alpha}\right)$ (если $\alpha = \gamma^e$ при некотором $\gamma \in S$, то $k_0' = S$). Поле формальных степенных рядов $K' = k_0'\{\pi\}$ содержит, очевидно, K в качестве подполя и является конечным расширением k. Покажем, что оно уже может быть представлено в виде $k_0'\{u\}$, где $u^e = t$. Рассмотрим многочлен $G(X) = X^e - \varepsilon$. Так как в поле K' мы имеем

$$G(\gamma) \equiv 0 \pmod{\pi} \qquad \text{и} \qquad G'(\gamma) \not\equiv 0 \pmod{\pi},$$

где через γ обозначен корень $\sqrt[e]{\alpha}$, то в K' существует единица η, для которой $\eta \equiv \gamma \pmod{\pi}$ и $\eta^e = \varepsilon$ (здесь мы опять применили упоминавшееся уже замечание из п. 2). Заменим теперь простой элемент π поля K' элементом $u = \pi\eta$. Тогда K' может рассматриваться также как поле формальных степенных рядов от u над полем k_0', т. е. $K' = k_0'\{u\}$, при этом $u^e = t$ ввиду (15). Доказательство теоремы 6 окончено.

Замечание. Теорема 6 перестает быть справедливой для произвольных конечных расширений поля формальных степенных рядов $k = k_0\{t\}$ характеристики $p \neq 0$. Однако она сохраняется как легко видеть, для тех расширений K/k, для которых поле вычетов Σ сепарабельно над Σ_0 и индекс ветвления e не делится на p.

Задачи

1. Нетривиальная метрика φ поля k называется *дискретной*, если для ее значений $\varphi(x)$, $x \in k$, нуль является единственной предельной точкой. Доказать, что всякая дискретная метрика связана с некоторым показателем ν поля k соотношением (1).

2. Пусть k — полное поле с показателем, K/k — конечное расширение и $\theta_1, \ldots, \theta_n$ — фундаментальный базис поля K над k. Показать, что элементы

$$\theta_i' = \sum_{j=1}^{n} a_{ij}\theta_j, \qquad a_{ij} \in k,$$

также образуют фундаментальный базис K над k тогда и только тогда, когда все a_{ij} целые и определитель $\det(a_{ij})$ является единицей в k.

3. Пусть сохраняются обозначения теоремы 4. Для произвольного элемента $\alpha = \sum_{i=1}^{f}\sum_{j=0}^{e-1} a_{ij}\omega_i\pi^j$ $(a_{ij} \in k)$ из K положим $m = \min \nu_0(a_{ij})$. Показать, что если j_0 есть наименьшее значение индекса j, для которого существует такое $i = i_0$, что $\nu_0(a_{i_0 j_0}) = m$, то $\nu(\alpha) = j_0 + em$, где ν — показатель поля K.

4. Доказать, что каждый элемент из поля формальных степенных рядов $k_0\{t\}$, не принадлежащий k_0, трансцендентен над полем k_0.

5. Доказать, что в условиях теоремы 6 подполе $S \subset K$, содержащее k_0 и являющееся полной системой представителей из классов вычетов поля K, определено однозначно.

6. Доказать, что если поле k_0 алгебраически замкнуто и имеет характеристику нуль, то для поля формальных степенных рядов $k = k_0\{t\}$ при любом натуральном n существует только одно конечное расширение степени n, а именно $k\left(\sqrt[n]{t}\right)$. (Единственность понимается с точностью до изоморфизма, оставляющего элементы из k на месте.)

7. Доказать, что если характеристика поля вычетов Σ полного поля K с показателем равна нулю, то в K существует подполе S, являющееся полной системой представителей для классов вычетов из Σ, и, следовательно, $K = S\{\pi\}$, где π — произвольный простой элемент в кольце целых элементов поля K. (При доказательстве использовать тот факт, что всякое поле может быть получено из простого подполя чисто трансцендентным расширением с последующим алгебраическим расширением.)

8. Показать, что в условиях задачи 7 подполе S единственно, если поле вычетов Σ алгебраично над простым подполем.

9. Пусть K — полное поле с показателем и Σ — его поле вычетов. Доказать, что если Σ есть совершенное поле характеристики p (в котором возведение в степень p является автоморфизмом), то в K существует, и притом единственная «мультипликативно замкнутая» система представителей S из классов вычетов $\bar{\xi} \in \Sigma$, обладающая тем свойством, что если $\alpha \in S$ и $\beta \in S$, то $\alpha\beta \in S$. (Представителем $\alpha \in S$ класса $\bar{\xi}$ является предел $\alpha = \lim\limits_{n\to\infty} \alpha_n^{p^n}$, где α_n — представители классов $\bar{\xi}^{p^{-n}}$.)

10. Сохраняя те же обозначения, предположим, что Σ есть конечное поле из p^f элементов. Доказать, что в поле K многочлен $t^{p^f} - t$ раскладывается на линейные множители и все его корни образуют мультипликативно замкнутую систему представителей S для классов вычетов из Σ.

11. Предположим, что поле K задачи 9 имеет ту же характеристику p, что и его совершенное поле вычетов Σ. Доказать, что тогда мультипликативно замкнутая система представителей S будет и «аддитивно замкнутой» и, значит, будет подполем поля K, так что $K = S\{\pi\}$, где π — простой элемент поля K.

12. Пусть K — конечное расширение полного поля k с показателем. Предположим, что поле вычетов Σ поля K сепарабельно над полем вычетов Σ_0 поля k. Показать, что тогда среди промежуточных полей L, $k \subset L \subset K$, не разветвленных над k, существует максимальное поле T (содержащее в себе все другие не разветвленные над k промежуточные поля). Поле вычетов поля T совпадает с Σ, и его степень $(T : k)$ равна $(\Sigma : \Sigma_0)$.

13. Пусть $f(X) = X^m + a_1X^{m-1} + \ldots + a_m$ — неприводимый многочлен с коэффициентами из полного поля с показателем. Доказать, что если свободный член a_m целый, то все остальные коэффициенты $a_1, \ldots, a_{m-1}$ также целые.

14. Пусть ζ — первообразный корень степени p^s из 1 ($s \geqslant 1$). Доказать, что поле $\mathbb{Q}_p(\zeta)$ имеет степень $(p-1)p^{s-1}$ над полем p-адических чисел $\mathbb{Q}_p$. Доказать, далее, что расширение $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ вполне разветвлено.

15. Пусть ζ — первообразный корень степени p из 1. Доказать, что $\mathbb{Q}_p(\zeta) = \mathbb{Q}_p\left(\sqrt[p-1]{-p}\right)$.

16. Пусть k — полное поле с показателем, K/k — его конечное расширение, Σ и Σ_0 — поля вычетов K и k соответственно. Доказать, что если расширение Σ/Σ_0 сепарабельно, то для K/k существует степенной фундаментальный базис (т. е. $\mathfrak{O} = \mathfrak{o}[\theta]$, $\theta \in \mathfrak{O}$, где $\mathfrak{O}$ и $\mathfrak{o}$ — кольца целых элементов K и k).

Указание. Доказать, что если $\Sigma = \Sigma_0(\bar{\theta})$, то представитель $\theta \in \mathfrak{O}$ можно выбрать так, что $f(\theta)$ будет простым элементом кольца $\mathfrak{O}$. Здесь многочлен $f(t) \in \mathfrak{o}[t]$ таков, что $\bar{f}(t) \in \Sigma_0[t]$ является минимальным многочленом элемента $\bar{\theta} \in \Sigma$.

17. Доказать, что в полном поле с показателем бесконечное произведение $\prod_{n=1}^{\infty}(1+a_n)$, $a_n \neq -1$, сходится тогда и только тогда, когда $a_n \to 0$ при $n \to \infty$.

§ 2. Конечные расширения поля с показателем

Пусть k — произвольное поле с показателем $\nu_\mathfrak{p}$ и K/k — его конечное расширение. Кольцо $\mathfrak{o} = \mathfrak{o}_\mathfrak{p}$ показателя $\nu_\mathfrak{p}$ мы будем рассматривать как кольцо, в котором имеется теория дивизоров с единственным простым дивизором $\mathfrak{p}$. Согласно теореме 1 § 5 гл. III в целом замыкании $\mathfrak{O}$ кольца $\mathfrak{o}$ в поле K мы имеем теорию дивизоров с конечным числом простых дивизоров $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ (все они являются делителями $\mathfrak{p}$).

Пусть $\mathfrak{P}$ — один из простых дивизоров кольца $\mathfrak{O}$ и $K_\mathfrak{P}$ — пополнение поля K по показателю $\nu_\mathfrak{P}$. Те элементы из $K_\mathfrak{P}$, которые являются пределами элементов из k, образуют подполе, топологически изоморфное пополнению $k_\mathfrak{p}$ поля k по показателю $\nu_\mathfrak{p}$. В силу изоморфного вложения $k_\mathfrak{p} \to K_\mathfrak{P}$ будем в дальнейшем считать, что $k_\mathfrak{p}$ является подполем поля $K_\mathfrak{P}$. Пусть $K = k(\alpha_1, \ldots, \alpha_r)$. Элементы $\alpha_i \in K$ принадлежат также и $K_\mathfrak{P}$, и, будучи алгебраичными над k, они алгебраичны и над $k_\mathfrak{p}$. Следовательно, расширение $k_\mathfrak{p}(\alpha_1, \ldots, \alpha_r)/k_\mathfrak{p}$ конечно (причем его степень не превосходит степени K/k), а значит, по теореме 2 § 1 поле $k_\mathfrak{p}(\alpha_1, \ldots, \alpha_r)$ полно. Каждый элемент из $K_\mathfrak{P}$ является пределом последовательности элементов из K, поэтому из включения $K \subset k_\mathfrak{p}(\alpha_1, \ldots, \alpha_r)$ и полноты $k_\mathfrak{p}(\alpha_1, \ldots, \alpha_r)$ следует, что $K_\mathfrak{P} \subset k_\mathfrak{p}(\alpha_1, \ldots, \alpha_r)$, а так как справедливо и обратное включение, то $K_\mathfrak{P} = k_\mathfrak{p}(\alpha_1, \ldots, \alpha_r)$. Этим мы доказали, что расширение $K_\mathfrak{P}/k_\mathfrak{p}$ конечно, при этом

$$(K_\mathfrak{P} : k_\mathfrak{p}) \leqslant (K : k).$$

Так как поля вычетов показателей $\nu_\mathfrak{p}$ и $\nu_\mathfrak{P}$ совпадают с полями вычетов пополнений $k_\mathfrak{p}$ и $K_\mathfrak{P}$ (см. конец п. 1 § 1), то степень инерции $f_\mathfrak{P}$ дивизора $\mathfrak{P}$ относительно $\mathfrak{p}$ совпадает со степенью инерции расширения $K_\mathfrak{P}/k_\mathfrak{p}$. Очевидно также, что индекс ветвления $e_\mathfrak{P}$ дивизора $\mathfrak{P}$ относительно $\mathfrak{p}$ совпадает с индексом ветвления $K_\mathfrak{P}/k_\mathfrak{p}$. Согласно теореме 5 § 1 числа $f_\mathfrak{P}$ и $e_\mathfrak{P}$ связаны со степенью $n_\mathfrak{P} = (K_\mathfrak{P} : k_\mathfrak{p})$ соотношением $f_\mathfrak{P} e_\mathfrak{P} = n_\mathfrak{P}$.

Далее в этом параграфе мы предположим, что расширение K/k сепарабельно, и в этом предположении изучим связи между

пополнениями $K_{\mathfrak{P}_1}, \ldots, K_{\mathfrak{P}_m}$ поля K по всем продолжениям показателя $\nu_\mathfrak{p}$.

Пусть $\omega_1, \ldots, \omega_n$ — базис расширения K/k. Если для элемента $\alpha \in K$ в представлении

$$\alpha = a_1\omega_1 + \ldots + a_n\omega_n, \qquad a_j \in k, \tag{1}$$

все коэффициенты a_j будут малы относительно $\mathfrak{p}$ (т. е. малы относительно показателя $\nu_\mathfrak{p}$), то этот элемент α будет, очевидно, мал относительно каждого простого дивизора $\mathfrak{P}_s$. Справедливо и обратное утверждение.

Лемма 1. *Для любого целого N можно указать такое M, что для всех коэффициентов a_j в разложении* (1) *будут выполняться неравенства $\nu_\mathfrak{p}(a_j) \geqslant N$, если только $\nu_{\mathfrak{P}_s}(\alpha) \geqslant M$ при всех $s = 1, \ldots, m$.*

Доказательство. Пусть $\omega_1^*, \ldots, \omega_n^*$ — взаимный базис для базиса $\omega_1, \ldots, \omega_n$ (см. п. 3 § 2 Дополнения; здесь мы воспользовались сепарабельностью расширения K/k). Тогда

$$a_j = \mathrm{Sp}_{K/k}(\alpha\omega_j^*) = \mathrm{Sp}\,\alpha\omega_j^*.$$

Обозначим через e_s индекс ветвления $\mathfrak{P}_s$ относительно $\mathfrak{p}$ и через p простой элемент в кольце $\mathfrak{o}_\mathfrak{p}$ показателя $\nu_\mathfrak{p}$, так что $e_s = \nu_{\mathfrak{P}_s}(p)$. Положим $M = \max\limits_{s,f}\left(e_sN - \nu_{\mathfrak{P}_s}(\omega_j^*)\right)$. Если теперь $\nu_{\mathfrak{P}_s}(\alpha) \geqslant M$ при всех s, то при фиксированном j имеем

$$\nu_{\mathfrak{P}_s}(\alpha\omega_j^*) \geqslant e_sN = \nu_{\mathfrak{P}_s}(p^N),$$

а значит, $\alpha\omega_j^* = p^N\gamma$, где $\nu_{\mathfrak{P}_s}(\gamma) \geqslant 0$ $(1 \leqslant s \leqslant m)$. По теореме 6 § 4 гл. III элемент γ принадлежит целому замыканию кольца $\mathfrak{o}_\mathfrak{p}$ в поле K, поэтому $\mathrm{Sp}\,\gamma \in \mathfrak{o}_\mathfrak{p}$, т. е. $\nu_\mathfrak{p}(\mathrm{Sp}\,\gamma) \geqslant 0$, откуда

$$\nu_\mathfrak{p}(a_j) = \nu_\mathfrak{p}\left(\mathrm{Sp}(\alpha\omega_j^*)\right) = \nu_\mathfrak{p}(p^N\,\mathrm{Sp}\,\gamma) \geqslant N,$$

и лемма 1 доказана.

Следствие. *Если последовательность $\{\alpha_r\}$ элементов поля K является фундаментальной относительно каждого простого дивизора $\mathfrak{P}_s$ $(s = 1, \ldots, m)$, то все последовательности $\{a_j^{(r)}\}_{r=1}^\infty$, определяемые разложениями*

$$\alpha_r = a_1^{(r)}\omega_1 + \ldots + a_n^{(r)}\omega_n, \qquad a_j^{(r)} \in k,$$

фундаментальны относительно $\mathfrak{p}$.

Рассмотрим теперь пополнения $K_{\mathfrak{P}_1}, \ldots, K_{\mathfrak{P}_m}$ поля K по всем простым дивизорам $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ и составим прямую сумму $K_{\mathfrak{P}_1} \oplus \ldots \oplus K_{\mathfrak{P}_m}$, которую мы обозначим через $K_\mathfrak{p}$. Элементами

этой прямой суммы являются последовательности $\xi = (\xi_1, \ldots, \xi_m)$, где $\xi_1 \in K_{\mathfrak{P}_1}, \ldots, \xi_m \in K_{\mathfrak{P}_m}$. Определим сложение и умножение таких последовательностей покомпонентно. Этим мы превратим $K_\mathfrak{p}$ в кольцо. Для любого $\gamma \in k_\mathfrak{p}$ положим

$$\gamma(\xi_1, \ldots, \xi_m) = (\gamma\xi_1, \ldots, \gamma\xi_m).$$

Кольцо $K_\mathfrak{p}$ становится теперь линейным пространством над полем $k_\mathfrak{p}$. Если степень $K_{\mathfrak{P}_s}$ над $k_\mathfrak{p}$ мы обозначим через n_s, то размерность пространства $K_\mathfrak{p}$ над $k_\mathfrak{p}$ будет, очевидно, равна

$$n_1 + \ldots + n_m. \tag{2}$$

В кольце $K_\mathfrak{p}$ естественным образом можно определить понятие сходимости. Именно, будем говорить, что последовательность $\{(\xi_1^{(r)}, \ldots, \xi_m^{(r)})\}_{r=1}^{\infty}$, $\xi_s^{(r)} \in K_{\mathfrak{P}_s}$, сходится к элементу $(\xi_1, \ldots, \xi_m)$, если при любом s последовательность $\{\xi_s^{(r)}\}$ сходится к ξ_s согласно сходимости в поле $K_{\mathfrak{P}_s}$. Легко видеть, что относительно этого понятия сходимости операция умножения в кольце $K_\mathfrak{p}$ на элементы из $k_\mathfrak{p}$ непрерывна. Другими словами, если $\gamma = \lim\limits_{r\to\infty} \gamma^{(r)}$, $\gamma^{(r)} \in k_\mathfrak{p}$ и $\xi = \lim\limits_{r\to\infty} \xi^{(r)}$, $\xi^{(r)} \in K_\mathfrak{p}$, то

$$\lim_{r\to\infty} \gamma^{(r)}\xi^{(r)} = \gamma\xi. \tag{3}$$

Определим теперь отображение $K \to K_\mathfrak{p}$, полагая

$$\widehat{\alpha} = (\alpha, \ldots, \alpha) \in K_\mathfrak{p}, \qquad \alpha \in K.$$

Так как $K \subset K_{\mathfrak{P}_s}$ при любом s, то последовательность $(\alpha, \ldots, \alpha)$ является элементом из $K_\mathfrak{p}$. Ясно, что отображение $\alpha \to \widehat{\alpha}$ определяет изоморфизм поля K в кольцо $K_\mathfrak{p}$. Образ поля K при этом изоморфизме мы обозначим через $\widehat{K}$.

Во избежание недоразумений заметим, что компоненты произведения $\gamma\widehat{\alpha} = (\gamma\alpha, \ldots, \gamma\alpha)$, $\gamma \in k_\mathfrak{p}$, которые по виду представляются одинаковыми, на самом деле, как правило, различны, так как произведение $\gamma\alpha$ зависит от того, в каком поле $K_{\mathfrak{P}_s}$ мы его рассматриваем, и для различных $K_{\mathfrak{P}_s}$ оно имеет, вообще говоря, разные значения, даже когда $\alpha\gamma \in k_\mathfrak{p}$.

Теорема 1. *Если $\omega_1, \ldots, \omega_n$ — базис сепарабельного расширения K/k, то $\widehat{\omega}_1, \ldots, \widehat{\omega}_n$ образуют базис кольца $K_\mathfrak{p}$ как линейного пространства над $k_\mathfrak{p}$.*

Доказательство. Покажем сначала, что $\widehat{K}$ всюду плотно в $K_{\mathfrak{p}}$, т. е. что каждый элемент из $K_{\mathfrak{p}}$ является пределом последовательности элементов из $\widehat{K}$. Пусть $\xi=(\xi_1, \ldots, \xi_n)$ — произвольный элемент из $K_{\mathfrak{p}}$, $\xi_s \in K_{\mathfrak{P}_s} (s=1, \ldots, m)$. Так как K всюду плотно в $K_{\mathfrak{P}_s}$, то для любого натурального r существует такой элемент $\alpha_s^{(r)} \in K$, что $v_{\mathfrak{P}_s}(\xi_s - \alpha_s^{(r)}) \geqslant r$. Согласно теореме 4 § 4 гл. III в K найдется элемент $\alpha^{(r)}$, для которого $v_{\mathfrak{P}_s}(\alpha_s^{(r)} - \alpha^{(r)}) \geqslant r$ при всех $s=1, \ldots, m$. Для элемента $\alpha^{(r)}$ мы имеем

$$v_{\mathfrak{P}_s}(\xi_s - \alpha^{(r)}) \geqslant r, \qquad s=1, \ldots, m,$$

а это и означает, очевидно, что последовательность $\{\widehat{\alpha}^{(r)}\}_{r=1}^{\infty}$ элементов из $\widehat{K}$ сходится в кольце $K_{\mathfrak{p}}$ к элементу ξ.

Представим каждый элемент $\alpha^{(r)}$ в виде

$$\alpha^{(r)} = a_1^{(r)}\omega_1 + \ldots + a_n^{(r)}\omega_n, \qquad a_j^{(r)} \in k.$$

Так как последовательность $\{\alpha^{(r)}\}$ фундаментальна относительно каждого простого дивизора $\mathfrak{P}_s$, то по следствию леммы 1 последовательности $\{a_j^{(r)}\}_{r=1}^{\infty}$ все фундаментальны относительно $\mathfrak{p}$, а поэтому имеют пределы в $k_{\mathfrak{p}}$. Положим $\gamma_j = \lim\limits_{r\to\infty} a_j^{(r)}$ $(j=1, \ldots, n)$. Так как для всякого $a \in k \subset k_{\mathfrak{p}}$ и любого $\xi \in K_{\mathfrak{p}}$, очевидно,

$$a\xi = \widehat{a}\xi, \tag{4}$$

то $\widehat{\alpha}^{(r)} = \sum\limits_{j=1}^{n} \widehat{a}_j^{(r)}\widehat{\omega}_j = \sum\limits_{j=1}^{n} a_j^{(r)}\widehat{\omega}_j$. Переходя в этом равенстве к пределу при $r \to \infty$ и учитывая свойство (3), мы получаем, что

$$\xi = \lim_{r\to\infty} \widehat{\alpha}^{(r)} = \sum_{j=1}^{n} \gamma_j \widehat{\omega}_j.$$

Этим доказано, что элементы $\widehat{\omega}_j$ составляют систему образующих линейного пространства $K_{\mathfrak{p}}$. Остается проверить, что они линейно независимы над $k_{\mathfrak{p}}$. Пусть

$$\gamma_1\widehat{\omega}_1 + \ldots + \gamma_n\widehat{\omega}_n = 0, \qquad \gamma_j \in k_{\mathfrak{p}}.$$

Так как k всюду плотно в $k_{\mathfrak{p}}$, то $\gamma_j = \lim\limits_{r\to\infty} a_j^{(r)}$, где $a_j^{(r)} \in k$. Положим

$$\alpha^{(r)} = a_1^{(r)}\omega_1 + \ldots + a_n^{(r)}\omega_n \in K.$$

Тогда $\lim\limits_{r\to\infty} \widehat{\alpha}^{(r)} = \lim\limits_{r\to\infty} \sum\limits_j a_j^{(r)}\widehat{\omega}_j = \sum\limits_j \gamma_j\widehat{\omega}_j = 0$. Это значит, что в поле K последовательность $\{\alpha^{(r)}\}$ является нулевой относительно

всех простых дивизоров $\mathfrak{P}_s$ $(s=1, \ldots, m)$. Но в таком случае по следствию леммы 1 нулевыми относительно $\mathfrak{p}$ будут все последовательности $\{a_j^{(r)}\}$ в поле k, а значит, $\gamma_1=0, \ldots, \gamma_n=0$.

Доказательство теоремы 1 закончено.

Замечание. В терминах тензорного произведения алгебр теорема 1 означает, что алгебра $K_\mathfrak{p}$ над полем $k_\mathfrak{p}$ изоморфна тензорному произведению $K\otimes_k k_\mathfrak{p}$, т. е. может быть получена из K (как алгебры над k) расширением основного поля k до $k_\mathfrak{p}$.

По доказанному размерность линейного пространства $K_\mathfrak{p}$ над $k_\mathfrak{p}$ равна $n=(K:k)$. С другой стороны, эта размерность равна сумме (2). Сопоставляя это с тем, что $n_s=n_{\mathfrak{P}_s}=e_{\mathfrak{P}_s}f_{\mathfrak{P}_s}$, мы приходим к равенству $\sum\limits_{\mathfrak{P}} e_\mathfrak{P} f_\mathfrak{P}=n$ ($\mathfrak{P}$ пробегает все простые дивизоры кольца $\mathfrak{O}$). Нами получено, таким образом, другое доказательство теоремы 7 § 5 гл. III.

Теорема 2. *Обозначим через $\varphi(X)$ характеристический многочлен элемента $\alpha\in K$ относительно сепарабельного расширения K/k и через $\varphi_\mathfrak{P}(X)$ его характеристический многочлен относительно расширения $K_\mathfrak{P}/k_\mathfrak{p}$. Тогда*

$$\varphi(X)=\prod_{\mathfrak{P}}\varphi_\mathfrak{P}(X).$$

Доказательство. В линейном пространстве $K_\mathfrak{p}$ рассмотрим линейное преобразование $\xi\to\widehat{\alpha}\xi$ $(\xi\in K_\mathfrak{p})$.

Если $\alpha\omega_r=\sum\limits_{l=1}^{n} a_{rl}\omega_l$, $a_{rl}\in k$, то в силу (4) имеем также

$$\widehat{\alpha}\widehat{\omega}_r=\sum_l a_{rl}\widehat{\omega}_l.$$

Это показывает, что характеристический многочлен нашего преобразования совпадает с характеристическим многочленом матрицы (a_{rl}), т. е. совпадает с $\varphi(X)$. Рассмотрим теперь в $K_\mathfrak{p}$ другой базис (над $k_\mathfrak{p}$). Пусть β_{sj} $(j=1, \ldots, n_s)$ — какой-нибудь базис расширения $K_{\mathfrak{P}_s}/k_\mathfrak{p}$ $(s=1, \ldots, m)$. Если через $\overline{\beta}_{sj}$ мы обозначим тот элемент из $K_\mathfrak{p}$, у которого s-я компонента равна β_{sj}, а все прочие равны нулю, то совокупность элементов

$$\overline{\beta}_{sj}, \qquad s=1, \ldots, m;\ j=1, \ldots, n_s \tag{5}$$

составит, очевидно, новый базис кольца $K_\mathfrak{p}$ (над $k_\mathfrak{p}$). Пусть

$$\alpha\beta_{sj}=\sum_{l=1}^{n_s}\gamma_{jl}^{(s)}\beta_{sl}, \qquad \gamma_{jl}^{(s)}\in k_{\mathfrak{p}s}$$

так что $\varphi_{\mathfrak{P}_s}(X)$ — это характеристический многочлен матрицы $(\gamma_{jl}^{(s)})$. Легко видеть теперь, что матрицей линейного преобразования $\xi \to \widehat{\alpha}\xi$ в базисе (5) будет клеточно диагональная матрица с клетками $(\gamma_{jl}^{(s)})$ на главной диагонали. Это и доказывает теорему 2.

Для элементов α из K введем понятие локальной нормы $N_{\mathfrak{P}}(\alpha)$ и локального следа $\mathrm{Sp}_{\mathfrak{P}}(\alpha)$:

$$N_{\mathfrak{P}}(\alpha) = N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(\alpha), \qquad \mathrm{Sp}_{\mathfrak{P}}(\alpha) = \mathrm{Sp}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(\alpha).$$

Из теоремы 2 очевидным образом вытекают следующие формулы:

$$N_{K/k}(\alpha) = \prod_{\mathfrak{P}|\mathfrak{p}} N_{\mathfrak{P}}(\alpha), \qquad \mathrm{Sp}_{K/k}(\alpha) = \sum_{\mathfrak{P}|\mathfrak{p}} \mathrm{Sp}_{\mathfrak{P}}(\alpha). \tag{6}$$

Первая из этих формул вместе с равенством (13) § 1 дает нам соотношение

$$v_{\mathfrak{p}}(N_{K/k}(\alpha)) = \sum_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}} v_{\mathfrak{P}}(\alpha), \tag{7}$$

которое в § 5 гл. III было доказано другим способом.

Теорема 3. *Выберем в поле K (сепарабельном над k) примитивный элемент θ, так что $K = k(\theta)$, и обозначим через $\varphi(X)$ его минимальный многочлен относительно k. Все простые дивизоры $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ поля K, делящие $\mathfrak{p}$, находятся во взаимно однозначном соответствии с множителями из разложения*

$$\varphi(X) = \varphi_1(X) \ldots \varphi_m(X)$$

на неприводимые множители в кольце $k_{\mathfrak{p}}[X]$. Для простого дивизора $\mathfrak{P}_s$ соответствующий ему многочлен $\varphi_s(X)$ совпадает с минимальным многочленом элемента $\theta \in K_{\mathfrak{P}_s}$ над полем $k_{\mathfrak{p}}$.

Доказательство. По теореме 2 многочлен $\varphi(X)$, являясь характеристическим многочленом для θ относительно K/k, равен произведению $\varphi_1(X) \ldots \varphi_m(X)$, где $\varphi_s(X)$ — характеристический многочлен для θ относительно $K_{\mathfrak{P}_s}/k_{\mathfrak{p}}$. Множитель $\varphi_s(X)$ однозначно определен, таким образом, простым дивизором $\mathfrak{P}_s$. Но, как мы видели в начале пункта, $K_{\mathfrak{P}_s} = k_{\mathfrak{p}}(\theta)$, $\theta \in K \subset K_{\mathfrak{P}_s}$, поэтому каждый из многочленов $\varphi_s(X)$ неприводим над $k_{\mathfrak{p}}$, и теорема 3 доказана.

Замечание. Предположим, что кольцо $\mathfrak{o}$ (с полем отношений k) есть произвольное кольцо с теорией дивизоров и $\mathfrak{p}$ — один из простых дивизоров кольца $\mathfrak{o}$. В случае конечного сепарабельного расширения K/k теорема 3 дает нам, очевидно, описание всех простых дивизоров $\mathfrak{P}$ в целом замыкании $\mathfrak{O}$ кольца $\mathfrak{o}$ в K, делящих $\mathfrak{p}$ (точнее, дает их число m и произведения $e_{\mathfrak{P}} f_{\mathfrak{P}}$).

§ 3. Разложение многочленов на множители в полном поле с показателем

В связи с теоремой 3 § 2 важно иметь удобный прием для разложения многочленов на неприводимые множители в полном поле с показателем. В этом параграфе мы покажем, что в таких полях разложение многочлена с целыми коэффициентами вполне определяется его разложением по модулю некоторой степени простого элемента.

Лемма. *Пусть* $\mathfrak{o}$ *— подкольцо произвольного поля* k, *и пусть* $g(X)$ *и* $h(X)$ *— многочлены степеней* m *и* n *соответственно с коэффициентами из* $\mathfrak{o}$. *Если результант* $\rho = R(g, h)$ *многочленов* g *и* h *отличен от нуля, то для любого многочлена* $l(X) \in \mathfrak{o}[X]$ *степени* $\leqslant m+n-1$ *в кольце* $\mathfrak{o}[X]$ *существуют такие многочлены* $\varphi(X)$ *и* $\psi(X)$ *степеней* $\leqslant n-1$ *и* $\leqslant m-1$ *соответственно, что*

$$\rho l(X) = g(X)\varphi(X) + h(X)\psi(X). \tag{1}$$

Доказательство. Положим

$$g(X) = \sum_{i=0}^{m} a_i X^{m-i}, \quad h(X) = \sum_{i=0}^{n} b_i X^{n-i}, \quad l(X) = \sum_{i=0}^{m+n-1} c_i X^{m+n-1-i},$$

$$\varphi(X) = \sum_{i=0}^{n-1} u_i X^{n-1-i}, \quad \psi(X) = \sum_{i=0}^{m-1} v_i X^{m-1-i}.$$

Для определения $m+n$ неизвестных $u_0, \ldots, u_{n-1}; v_0, \ldots, v_{m-1}$ приравняем в равенстве (1) коэффициенты при одинаковых степенях X. Мы получим систему $m+n$ уравнений:

$$\sum_{r+s=i} a_r u_s + \sum_{r+s=i} b_r v_s = \rho c_i, \qquad i = 0, 1, \ldots, m+n-1.$$

Определитель этой системы равен

$$\begin{vmatrix}
a_0 & & & & b_0 & & & \\
a_1 & a_0 & & & b_1 & b_0 & & \\
\cdot & \cdot & & & \cdot & \cdot & & \\
\cdot & & \cdot & & \cdot & & \cdot & \\
\cdot & & & \cdot & \cdot & & & \cdot \\
\cdot & & & a_0 & \cdot & & & b_0 \\
a_m & a_{m-1} & & a_1 & b_n & b_{n-1} & & b_1 \\
 & a_m & & \cdot & & b_n & & \cdot \\
 & & \cdot & \cdot & & & \cdot & \cdot \\
 & & & \cdot & & & & \cdot \\
 & & & a_m & & & & b_n
\end{vmatrix}
\begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix}
\tag{2}$$

$$\underbrace{\qquad\qquad}_{n} \quad \underbrace{\qquad\qquad}_{m}$$

(на свободных местах стоят нули), т. е. равен результанту $\rho = R(g, h)$. По условию $\rho \neq 0$, поэтому система имеет (единственное) решение, и так как все ее свободные члены ρc_i делятся на

ρ, то значения неизвестных u_i и v_i будут принадлежать кольцу $\mathfrak{o}$. Лемма доказана.

Пусть теперь k — полное поле относительно показателя ν, $\mathfrak{o}$ — кольцо целых элементов из k и π — простой элемент в $\mathfrak{o}$. Два многочлена $f(X)$ и $f_1(X)$ из кольца $\mathfrak{o}[X]$ называем сравнимыми по модулю π^h и пишем $f(X) \equiv f_1(X) \pmod{\pi^h}$, если сравнимы по тому же модулю их коэффициенты при одинаковых степенях X.

Теорема 1. *Пусть для многочлена $f(X) \in \mathfrak{o}[X]$ степени $m+n$ в кольце $\mathfrak{o}[X]$ существуют такие многочлены $g_0(X)$ и $h_0(X)$ степеней m и n соответственно, что*: 1) *старшие коэффициенты f и g_0h_0 совпадают*, 2) *результант $R(g_0, h_0)$ отличен от нуля* и 3) *если $\nu(R(g_0, h_0)) = r$, то*

$$f(X) \equiv g_0(X)h_0(X) \pmod{\pi^{2r+1}}. \tag{3}$$

Тогда в $\mathfrak{o}[X]$ существуют многочлены $g(X)$ степени m и $h(X)$ степени n, для которых

$$f(X) = g(X)h(X);\ g(X) \equiv g_0(X),\ h(X) \equiv h_0(X) \pmod{\pi^{r+1}}$$

и старшие коэффициенты $g(X)$ и $h(X)$ совпадают со старшими коэффициентами $g_0(X)$ и $h_0(X)$ соответственно.

Доказательство. Для каждого $k \geqslant 1$ мы индуктивно построим многочлены $\varphi_k \in \mathfrak{o}[X]$ степени $\leqslant m-1$ и $\psi_k \in \mathfrak{o}[X]$ степени $\leqslant n-1$ так, чтобы для многочленов

$$g_k = g_0 + \pi^{r+1}\varphi_1 + \ldots + \pi^{r+k}\varphi_k,$$
$$h_k = h_0 + \pi^{r+1}\psi_1 + \ldots + \pi^{r+k}\psi_k$$

выполнялось сравнение

$$f \equiv g_k h_k \pmod{\pi^{2r+k+1}}. \tag{4}$$

Пусть многочлены $\varphi_1, \ldots, \varphi_{k-1}$ и $\psi_1, \ldots, \psi_{k-1}$ с требуемыми свойствами уже построены, так что

$$f = g_{k-1}h_{k-1} + \pi^{2r+k}l, \tag{5}$$

где $l(X) \in \mathfrak{o}[X]$. Многочлены g_0 и g_{k-1}, а также h_0 и h_{k-1} имеют одинаковые старшие коэффициенты, поэтому в силу первого условия $l(X)$ имеет степень $\leqslant m+n-1$. Далее, $g_{k-1} \equiv g_0$, $h_{k-1} \equiv h_0 \pmod{\pi^{r+1}}$, поэтому

$$R(g_{k-1}, h_{k-1}) \equiv R(g_0, h_0) \pmod{\pi^{r+1}},$$

а значит, $\nu(R(g_{k-1}, h_{k-1})) = r$. По лемме в кольце $\mathfrak{o}[X]$ существуют многочлены φ_k и ψ_k степеней $\leqslant m-1$ и $\leqslant n-1$ соответственно, для которых

$$\pi^r l = g_{k-1}\psi_k + h_{k-1}\varphi_k. \tag{6}$$

Проверим, что φ_k и ψ_k удовлетворяют необходимым требованиям.

Так как $g_k = g_{k-1} + \pi^{r+k}\varphi_k$, $h_k = h_{k-1} + \pi^{r+k}\psi_k$, то ввиду (5) и (6)

$$f - g_k h_k = \pi^{2r+k} l - \pi^{r+k}(g_{k-1}\psi_k + h_{k-1}\varphi_k) - \pi^{2r+2k}\varphi_k\psi_k = -\pi^{2r+2k}\varphi_k\psi_k,$$

откуда и следует сравнение (4) (ибо $2k \geqslant k+1$).

Рассмотрим теперь в $\mathfrak{o}[X]$ многочлены

$$g(X) = g_0 + \sum_{k=1}^{\infty} \pi^{r+k}\varphi_k, \qquad h(X) = h_0 + \sum_{k=1}^{\infty} \pi^{r+k}\psi_k,$$

коэффициенты которых (кроме старших) являются суммами сходящихся рядов. Так как $g \equiv g_k$ и $h \equiv h_k \pmod{\pi^{r+k+1}}$, то

$$gh \equiv g_k h_k \pmod{\pi^{r+k+1}},$$

а значит, в силу (4)

$$f \equiv gh \pmod{\pi^{r+k+1}}.$$

Поскольку последнее сравнение верно при любом k, то $f = gh$, и теорема 1 доказана.

Замечание. Из доказательства теоремы 1 легко следует, что если g_0 и h_0 вместо (3) удовлетворяют условию $f \equiv g_0 h_0 \pmod{\pi^s}$, $s \geqslant 2r+1$, то g и h могут быть выбраны так, чтобы выполнялись сравнения $g \equiv g_0$, $h \equiv h_0 \pmod{\pi^{s-r}}$.

Рассмотрим один важный частный случай теоремы 1.

Многочлен $f(X) \in \mathfrak{o}[X]$ будем называть *примитивным*, если хоть один из его коэффициентов является единицей в $\mathfrak{o}$. Пусть Σ — поле вычетов кольца $\mathfrak{o}$ по простому элементу π. Заменяя в многочлене $f \in \mathfrak{o}[X]$ все его коэффициенты соответствующими классами вычетов из Σ, мы получим многочлен $\bar{f}$ с коэффициентами из поля Σ. Предположим, что в кольце $\Sigma[X]$ для $\bar{f}$ имеет место разложение

$$\bar{f} = \bar{g}_0 \bar{h}_0, \tag{7}$$

в котором сомножители $\bar{g}_0$ и $\bar{h}_0$ взаимно просты. Многочлены g_0 и h_0 из кольца $\mathfrak{o}[X]$ мы можем, конечно, выбрать так, чтобы, во-первых, степень g_0 совпадала со степенью $\bar{g}_0$ и, во-вторых, чтобы совпадали степени и старшие коэффициенты многочленов f и $g_0 h_0$. Рассмотрим результант $R(g_0, h_0)$ многочленов g_0 и h_0, т. е. определитель вида (2). Заменяя в этом определителе все элементы на соответствующие классы вычетов по модулю π, мы получим определитель, который будет равен, очевидно, результанту $R(\bar{g}_0, \bar{h}_0)$ многочленов $\bar{g}_0$ и $\bar{h}_0$ (старший коэффициент $\bar{h}_0$, возможно, равен нулю). Результант $R(\bar{g}_0, \bar{h}_0)$ отличен от нуля, так как по выбору g_0 старший коэффициент $\bar{g}_0$ отличен от нуля и многочлены $\bar{g}_0$ и $\bar{h}_0$ по условию взаимно просты. (Напомним, что для двух многочленов с произвольными старшими коэффициентами результант равен нулю тогда и только тогда, когда эти многочлены имеют общий множитель или же когда их старшие коэффициенты оба равны нулю.) Следовательно, $R(g_0, h_0) \not\equiv 0 \pmod{\pi}$,

т. е. $\nu(R(g_0, h_0)) = r = 0$. Равенство (7) равносильно сравнению $f \equiv g_0 h_0 \pmod{\pi}$. Мы видим, таким образом, что для g_0 и h_0 выполнены все условия теоремы 1 (при $r = 0$), а потому можно сформулировать следующее утверждение.

Теорема 2 (лемма Хензеля). *Пусть $f(X)$ — примитивный многочлен с коэффициентами из кольца $\mathfrak{o}$ целых элементов полного поля с показателем. Если в поле вычетов Σ кольца $\mathfrak{o}$ по простому элементу для многочлена $\bar{f} \in \Sigma[X]$ имеет место разложение*

$$\bar{f} = \bar{g}_0 \bar{h}_0, \qquad g_0, h_0 \in \mathfrak{o}[X]$$

со взаимно простыми $\bar{g}_0$ и $\bar{h}_0$, то в $\mathfrak{o}[X]$ существуют такие многочлены g и h, что

$$f(X) = g(X)h(X),$$

причем $\bar{g} = \bar{g}_0$, $\bar{h} = \bar{h}_0$ и степень g равна степени $\bar{g}_0$.

При помощи полученной нами теоремы 1 мы можем теперь решить вопрос о разложении многочленов с коэффициентами из полного поля k с показателем на неприводимые множители. Ограничимся рассмотрением многочленов $f(X)$ с целыми коэффициентами и со старшим коэффициентом 1 (если старший коэффициент многочлена из $\mathfrak{o}[X]$ степени n равен a, то мы можем умножить этот многочлен на a^{n-1} и взять aX за новую переменную). Так как для кольца $\mathfrak{o}[X]$ сохраняется известная теорема Гаусса о разложении многочленов с целыми коэффициентами, то все неприводимые делители таких многочленов $f(X)$, старшие коэффициенты которых равны 1, будут также принадлежать кольцу $\mathfrak{o}[X]$.

Если многочлен $f(X)$ не имеет кратных корней (в конечных расширениях поля k), то его дискриминант $D(f) = \pm R(f, f')$ отличен от нуля. Пусть $d = \nu(D(f))$, и пусть в кольце $\mathfrak{o}[X]$ имеет место сравнение

$$f \equiv \varphi_1 \varphi_2 \dots \varphi_m \pmod{\pi^{d+1}}, \tag{8}$$

в котором старшие коэффициенты многочленов φ_s (так же, как и f) все равны 1. Положим $h_1 = \varphi_2 \dots \varphi_m$. Так как для дискриминанта произведения двух многочленов имеет место формула

$$D(\varphi\psi) = D(\varphi)D(\psi)R(\varphi, \psi)^2,$$

и $D(f) \equiv D(\varphi_1 h_1) \pmod{\pi^{d+1}}$, так что $\nu(D(\varphi_1 h_1)) = d$, то $d \geqslant 2r$, где $r = \nu(R(\varphi_1, h_1))$. По теореме 1 (см. замечание в конце ее доказательства) в кольце $\mathfrak{o}[X]$ существуют такие многочлены $g_1(X)$ и $f_1(X)$, что $f = g_1 f_1$ и $f_1 \equiv \varphi_2 \dots \varphi_m \pmod{\pi^{d-r+1}}$. Но $d - r \geqslant d - 2r \geqslant d_1 = \nu(D(f_1))$, поэтому аналогичным образом для многочлена f_1 найдем разложение $f_1 = g_2 f_2$ и т. д. В конце концов мы получим разложение

$$f(X) = g_1(X) \dots g_m(X), \tag{9}$$

в котором многочлены $g_s \in \mathfrak{o}[X]$ имеют те же степени, что и φ_s.

Если разложение (8) выбрано с наибольшим возможным m, то все многочлены g_s, очевидно, неприводимы над полем k, и мы получаем следующий результат.

Теорема 3. *Если для многочлена $f(X)$ разложение* (8) *по модулю π^{d+1} выбрано с наибольшим возможным значением m, то разложение этого многочлена на неприводимые в k множители имеет вид* (9), *где каждый из многочленов g_s имеет ту же степень, что и соответствующий ему многочлен φ_s.*

Для теоремы 3 также особо отметим тот частный случай, когда $d = 0$, т. е. когда $D(f)$ является единицей в $\mathfrak{o}$. В этом случае разложение (8) (при переходе к полю вычетов Σ) совпадает с разложением

$$\bar{f} = \bar{\varphi}_1 \dots \bar{\varphi}_m \tag{10}$$

на неприводимые множители в кольце $\Sigma[X]$. Поэтому мы имеем следующее

Следствие. *Если для многочлена $f(X) \in \mathfrak{o}[X]$ дискриминант $D(f)$ является единицей в $\mathfrak{o}$ и если в кольце $\Sigma[X]$ разложение $\bar{f}$ на неприводимые множители имеет вид* (10), *то в $\mathfrak{o}[X]$ существуют такие неприводимые над k многочлены $g_1, \dots, g_m$, что $f = g_1 \dots g_m$ и $\bar{g}_1 = \bar{\varphi}_1, \dots, \bar{g}_m = \bar{\varphi}_m$.*

Это утверждение, конечно, очевидным образом вытекает также из теоремы 2.

Задачи

1. Пусть k — полное поле с показателем, K/k — конечное сепарабельное расширение с индексом ветвления e, $\mathfrak{o}$ и $\mathfrak{O}$ — кольца целых элементов полей k и K соответственно, π_0 и π — их простые элементы. Доказать, что если элемент $\alpha \in \mathfrak{O}$ делится на π, то $\mathrm{Sp}_{K/k}(\alpha)$ делится на π_0. Вывести отсюда, что $\mathrm{Sp}_{K/k}(\pi^{1-e}\mathfrak{O}) \subset \mathfrak{o}$. Перенести, далее, утверждения задач 12 и 16 § 2 гл. II на рассматриваемый случай и доказать, что в случае $e > 1$ для каждого элемента $\theta \in \mathfrak{O}$ с характеристическим многочленом $f(t)$ значение $f'(0)$ делится на π.

2. Пусть k — конечное расширение поля p-адических чисел, e — его индекс ветвления над $\mathbb{Q}_p$ и π — простой элемент поля k. Предположим, что k содержит первообразный корень степени p из 1, так что e делится на $p-1$ (задача 14 § 1). Доказать, что всякое целое $\alpha \in k$, которое $\equiv 1 \pmod{\pi^{m+1}}$, где $m = pe/(p-1) = ps = e + s$, является p-й степенью некоторого элемента из k. (Воспользоваться тем, что если $\beta = 1 + \pi^{e+r}\gamma$ (γ целое), $r > s$, $p = \pi^e\varepsilon^{-1}$, то $\beta \equiv (1 + \pi^r\gamma\varepsilon)^p \pmod{\pi^{e+r+1}}$. Применить затем задачу 17 § 1.)

3. В условиях задачи 2 предположим, что целое α сравнимо с 1 по модулю π^m, но не является p-й степенью элемента из k. Доказать, что тогда $k\left(\sqrt[p]{\alpha}\right)/k$ является неразветвленным расширением степени p. (Найти характеристический многочлен $f(t)$ элемента $\theta = \pi^{-s}\left(\sqrt[p]{\alpha} - 1\right)$ и убедиться, что $f'(0)$ является единицей; применить затем последнее утверждение задачи 1.)

4. Сохраняя условия задачи 2, предположим, что целое $\alpha \in k$ удовлетворяет условиям: $\alpha \equiv 1 \pmod{\pi^h}$, $\alpha \not\equiv 1 \pmod{\pi^{h+1}}$, $(h, p) = 1$, $h < m = ep/(p-1)$. Доказать, что тогда α не является p-й степенью элемента

из k и что расширение $k\left(\sqrt[p]{\alpha}\right)/k$ вполне разветвлено. (Рассмотреть показатель степени, с которым простой элемент поля $k\left(\sqrt[p]{\alpha}\right)$ входит в разность $1-\alpha=\prod_{i=0}^{p-1}\left(1-\zeta^i\sqrt[p]{\alpha}\right)$, где ζ — первообразный корень степени p из 1.)

§ 4. Метрики поля алгебраических чисел

1. Описание метрик. В п. 2 § 4 гл. I нами было выяснено, что всевозможные пополнения поля рациональных чисел $\mathbb{Q}$ — это поля p-адических чисел $\mathbb{Q}_p$ и поле вещественных чисел $\mathbb{Q}_\infty$. Теперь мы решим это вопрос для случая произвольного поля алгебраических чисел k. Согласно сказанному в начале § 1 каждому простому дивизору $\mathfrak{p}$ поля k соответствует $\mathfrak{p}$-адическое пополнение $k_\mathfrak{p}$, т. е. пополнение по метрике $\varphi_\mathfrak{p}(x)=\rho^{\nu_\mathfrak{p}(x)}$, $x\in k\,(0<\rho<1)$. Метрику $\varphi_\mathfrak{p}$ мы будем называть *$\mathfrak{p}$-адической метрикой* поля k. Для ответа на интересующий нас вопрос о возможных пополнениях поля k нам следует, очевидно, выяснить, какие еще метрики помимо $\mathfrak{p}$-адических имеются в полях алгебраических чисел.

Пусть φ — произвольная нетривиальная метрика поля алгебраических чисел k. Рассматривая ее лишь на рациональных числах, мы получаем метрику φ_0 поля $\mathbb{Q}$. Покажем прежде всего, что вместе с φ метрика φ_0 также нетривиальна. Выберем в k какой-нибудь базис $\omega_1, \ldots, \omega_n$ над $\mathbb{Q}$. Для любого $\xi=a_1\omega_1+\ldots+a_n\omega_n\,(a_i\in\mathbb{Q})$ мы имеем

$$\varphi(\xi)\leqslant\varphi_0(a_1)\varphi(\omega_1)+\ldots+\varphi_0(a_n)\varphi(\omega_n).$$

Если бы метрика φ_0 была тривиальной, то, поскольку $\varphi_0(a_i)\leqslant 1$, имело бы место неравенство

$$\varphi(\xi)\leqslant\sum_{i=1}^{n}\varphi(\omega_i)$$

при всех $\xi\in k$. Но это невозможно, так как все значения нетривиальной метрики не могут быть ограничены.

Согласно теореме 3 § 4 гл. I метрика φ_0 совпадает либо с p-адической метрикой $\varphi_p(x)=\rho^{\nu_p(x)}$, $0<\rho<1$, либо с метрикой $|x|^\rho$, $0<\rho\leqslant 1$ $(x\in\mathbb{Q})$. Разберем сначала первый случай. Обозначим через $\mathfrak{o}_p$ кольцо p-целых рациональных чисел (кольцо показателя ν_p) и через $\mathfrak{O}_p$ его целое замыкание в k. Если $\omega_1, \ldots, \omega_n$ — фундаментальный базис поля k, то всякое $\alpha\in\mathfrak{O}_p$ представляется в виде $\alpha=a_1\omega_1+\ldots+a_n\omega_n$ с коэффициентами a_i из $\mathfrak{o}_p$. Но $\varphi_p(a_i)\leqslant 1$, поэтому

$$\varphi(\alpha)\leqslant\sum_{i=1}^{n}\varphi(\omega_i),$$

а так как вместе с α все степени α^k $(k \geqslant 0)$ также принадлежат $\mathfrak{O}_p$, то $\varphi(\alpha) \leqslant 1$. Отсюда легко теперь следует, что $\varphi(\varepsilon) = 1$ для всех единиц кольца $\mathfrak{O}_p$. Согласно теореме 7 § 4 гл. III каждое отличное от нуля число $\xi \in k$ однозначно представляется в виде

$$\xi = \varepsilon \pi_1^{k_1} \dots \pi_m^{k_m}, \tag{1}$$

где ε — единица в $\mathfrak{O}_p$, а $\pi_1, \dots, \pi_m$ — некоторая фиксированная система попарно не ассоциированных простых элементов. (Число ξ принадлежит $\mathfrak{O}_p$ тогда и только тогда, когда $k_i \geqslant 0$.) Если бы $\varphi(\pi_i) = 1$ при всех i, то $\varphi(\xi)$ было бы равно 1 при всех $\xi \neq 0$ из k. Это, однако, противоречит нетривиальности φ. Предположим, что $\varphi(\pi_i) < 1$ и $\varphi(\pi_j) < 1$ для двух различных индексов i и j. Выберем натуральные k и l так, чтобы $\varphi(\pi_i)^k + \varphi(\pi_j)^l < 1$. Числа π_i^k и π_j^l взаимно просты в кольце $\mathfrak{O}_p$, поэтому согласно лемме 2 § 6 гл. III в $\mathfrak{O}_p$ существуют такие α и β, что

$$1 = \alpha \pi_i^k + \beta \pi_j^l.$$

Но тогда

$$1 = \varphi(1) \leqslant \varphi(\alpha)\varphi(\pi_i)^k + \varphi(\beta)\varphi(\pi_j)^l \leqslant \varphi(\pi_i)^k + \varphi(\pi_j)^l < 1,$$

и мы опять получили противоречие. Таким образом, существует только один простой элемент π_i, для которого $\varphi(\pi_i) < 1$. Обозначим через $\mathfrak{p}$ и $\nu_\mathfrak{p}$ соответствующие ему простой дивизор и показатель. Так как в разложении (1) показатель k_i равен $\nu_\mathfrak{p}(\xi)$, то, обозначая через ρ_1 значение $\varphi(\pi_i)$, будем иметь

$$\varphi(\xi) = \rho_1^{\nu_\mathfrak{p}(\xi)}. \tag{2}$$

Взяв здесь $\xi = p$, находим, что $\rho = \rho_1^e$, где e — индекс ветвления простого дивизора $\mathfrak{p}$. Полученная формула (2) показывает, что метрика φ совпадает с $\mathfrak{p}$-адической метрикой $\varphi_\mathfrak{p}$, соответствующей простому дивизору $\mathfrak{p}$.

Перейдем теперь к изучению случая, когда $\varphi_0(x) = |x|^\rho$, $0 < \rho \leqslant 1$ $(x \in \mathbb{Q})$.

Пополнение поля $\mathbb{Q}$ по метрике $|x|^\rho$ дает, как мы знаем, поле вещественных чисел (независимо от значения ρ). Как и в п. 2 § 7 гл. I, обозначим его через $\mathbb{Q}_\infty$. Продолжением метрики $|x|^\rho$, $x \in \mathbb{Q}$, на поле $\mathbb{Q}_\infty$ будет, очевидно, метрика $|\alpha|^\rho$, $\alpha \in \mathbb{Q}_\infty$. Присоединяя к полю $\mathbb{Q}_\infty$ корень $i = \sqrt{-1}$, мы получаем поле комплексных чисел $\mathbb{C}$. Покажем, что метрика $|\alpha|^\rho$ поля $\mathbb{Q}_\infty$ может быть продолжена на поле $\mathbb{C}$ единственным образом, а именно с помощью метрики $|\xi|^\rho$, где $|\xi|$ обозначает модуль комплексного числа ξ. Пусть ψ — какое-нибудь продолжение. Тогда $\psi(\xi) = 1$ для всех $\xi \in \mathbb{C}$ с условием $|\xi| = 1$. В самом деле, если бы это было не так, то для некоторого $\xi \in \mathbb{C}$ мы имели бы $\psi(\xi) > 1$ и

$|\xi| = 1$. Выбрав натуральное число n и положив $\xi^n = \alpha + \beta i$ ($\alpha, \beta \in \mathbb{Q}_\infty$), мы получили бы

$$\psi(\xi^n) \leqslant \psi(\alpha) + \psi(\beta)\psi(i) \leqslant 1 + \psi(i),$$

поскольку $\psi(\alpha) = |\alpha|^\rho \leqslant 1$ и аналогично $\psi(\beta) \leqslant 1$. Но это невозможно, так как $\psi(\xi)^n > 1 + \psi(i)$, если только n достаточно велико. Пусть теперь ξ — произвольное отличное от нуля комплексное число. По доказанному $\psi(\xi/|\xi|) = 1$. Следовательно, $\psi(\xi) = \psi(|\xi|) = |\xi|^\rho$, что и требовалось доказать.

Каждое поле алгебраических чисел k степени $n = s + 2t$ (см. п. 1 § 3 гл. II) имеет n различных изоморфизмов в поле комплексных чисел $\mathbb{C}$ (s вещественных и t пар комплексных). Пусть σ — какой-нибудь один из них. Если для любого $\xi \in k$ мы положим

$$\varphi_\sigma(\xi) = |\sigma(\xi)|^\rho,$$

то функция φ_σ будет, очевидно, метрикой поля k, причем $\varphi_\sigma(x) = |x|^\rho$ при $x \in \mathbb{Q}$. Если σ и $\bar{\sigma}$ — сопряженные изоморфизмы, то $|\bar{\sigma}(\xi)| = |\overline{\sigma(\xi)}| = |\sigma(\xi)|$, а значит, соответствующие им метрики φ_σ и $\varphi_{\bar{\sigma}}$ совпадают. Мы имеем, таким образом, $s + t$ метрик поля k, совпадающих на $\mathbb{Q}$ с метрикой $|x|^\rho$.

Пусть теперь φ — произвольная метрика поля k, совпадающая на $\mathbb{Q}$ с метрикой $|x|^\rho$. На пополнении $\bar{k}_\varphi$ поля k по этой метрике однозначно определена непрерывная метрика $\bar{\varphi}$, совпадающая на k с φ. Ясно, что замыкание $\bar{\mathbb{Q}}$ поля рациональных чисел в $\bar{k}_\varphi$ топологически изоморфно полю вещественных чисел $\mathbb{Q}_\infty$. Если через σ мы обозначим (единственный) топологический изоморфизм $\bar{\mathbb{Q}}$ на $\mathbb{Q}_\infty$, то для всякого $\gamma \in \bar{\mathbb{Q}}$ будем иметь $\bar{\varphi}(\gamma) = |\sigma(\gamma)|^\rho$. Выберем в k примитивное число θ, так что $k = \mathbb{Q}(\theta)$, и обозначим через $f(X)$ минимальный многочлен числа θ над $\mathbb{Q}$. При разложении $f(X)$ на неприводимые множители в поле вещественных чисел мы имеем s линейных и t квадратных множителей. Следовательно, и в поле $\bar{\mathbb{Q}}$ имеет место разложение

$$f(X) = (X - \theta_1) \ldots (X - \theta_s)(X^2 + p_1 X + q_1) \ldots (X^2 + p_t X + q_t).$$

Так как $f(\theta) = 0$, то θ должно быть корнем одного из этих сомножителей.

Предположим сначала, что $\theta = \theta_1$. Так как $\theta \in \bar{\mathbb{Q}}$ и, следовательно, $K = \mathbb{Q}(\theta) \subset \bar{\mathbb{Q}}$, то изоморфизм $\sigma\colon \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_\infty$ индуцирует на k вещественный изоморфизм $\sigma\colon k \to \mathbb{C}$, при этом, если $\xi \in k$, то

$$\varphi(\xi) = \bar{\varphi}(\xi) = |\sigma(\xi)|^\rho.$$

Метрика φ совпадает, таким образом, с φ_σ. Кроме того, мы видим, что в этом случае $\bar{k}_\varphi = \bar{\mathbb{Q}}$, т. е. пополнение $\bar{k}_\varphi$ топологически изоморфно полю вещественных чисел.

Предположим теперь, что θ — корень одного из квадратных трехчленов. В этом случае $(\overline{\mathbb{Q}}(\theta)\colon \overline{\mathbb{Q}}) = 2$, а поэтому изоморфизм $\sigma\colon \overline{\mathbb{Q}} \to \mathbb{Q}_\infty$ может быть продолжен (двумя способами) до изоморфизма $\sigma\colon \overline{\mathbb{Q}}(\theta) \to \mathbb{C}$. Индуцированное этим изоморфизмом вложение $\sigma\colon k \to \mathbb{C}$ будет, очевидно, комплексным изоморфизмом k в поле комплексных чисел $\mathbb{C}$. По доказанному на $\mathbb{C}$ существует только одна метрика, совпадающая на $\mathbb{Q}_\infty$ с метрикой $|\alpha|^\rho$, а именно $|\eta|^\rho$, $\eta \in \mathbb{C}$. Следовательно, для любого $\xi \in k$ мы имеем

$$\varphi(\xi) = \overline{\varphi}(\xi) = |\sigma(\xi)|^\rho,$$

т. е. $\varphi = \varphi_\sigma$ при комплексном изоморфизме σ; поле $\bar{k}_\varphi$ (совпадающее с $\overline{\mathbb{Q}}(\theta)$) топологически изоморфно полю всех комплексных чисел.

Нами доказана, таким образом,

Теорема 1. *Всякая нетривиальная метрика φ поля алгебраических чисел k степени $n = s + 2t$ совпадает либо с $\mathfrak{p}$-адической метрикой*

$$\varphi_\mathfrak{p}(\xi) = \rho^{\nu_\mathfrak{p}(\xi)}, \qquad 0 < \rho < 1, \qquad \xi \in k,$$

соответствующей простому дивизору $\mathfrak{p}$, либо с одной из $s + t$ метрик вида

$$\varphi_\sigma(\xi) = |\sigma(\xi)|^\rho, \qquad 0 < \rho \leqslant 1, \qquad \xi \in k,$$

где σ — изоморфизм поля k в поле всех комплексных чисел $\mathbb{C}$.

Определение. *Пополнение $k_\mathfrak{p}$ поля алгебраических чисел k по метрике $\varphi_\mathfrak{p}$ называется полем $\mathfrak{p}$-адических чисел.*

Из теоремы 1 следует теперь, что все пополнения поля алгебраических чисел k исчерпываются полями $\mathfrak{p}$-адических чисел, полем вещественных чисел (при $s > 0$) и полем комплексных чисел (при $t \geqslant 0$).

Чтобы подчеркнуть аналогию между метриками $\varphi_\mathfrak{p}$ и φ_σ, полю алгебраических чисел k степени $n = s + 2t$ приписывают $s + t = r$ новых объектов $\mathfrak{p}_{1,\infty}, \ldots, \mathfrak{p}_{r,\infty}$, называемых *бесконечными простыми дивизорами*, которые взаимно однозначно соответствуют всем метрикам вида φ_σ. Обычные простые дивизоры, чтобы отличать их от бесконечных, называют тогда *конечными простыми дивизорами*. Бесконечный простой дивизор $\mathfrak{p} = \mathfrak{p}_{i,\infty}$ называется *вещественным*, если он соответствует метрике φ_σ с вещественным изоморфизмом σ, и называется *комплексным*, если связанная с ним метрика $\varphi_\sigma = \varphi_{\overline{\sigma}}$ отвечает паре сопряженных комплексных изоморфизмов σ и $\overline{\sigma}$.

В случае поля рациональных чисел $\mathbb{Q}$ существует единственный бесконечный (вещественный) простой дивизор p_∞, который мы фактически уже ввели в п. 2 § 7 гл. I и обозначали там сим-

волом ∞. Все простые дивизоры $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ поля k, соответствующие продолжениям p-адического показателя v_p на k, являются делителями числа p (которое мы можем рассматривать как дивизор поля $\mathbb{Q}$). Аналогично этому бесконечные простые дивизоры $\mathfrak{p}_{1,\infty}, \ldots, \mathfrak{p}_{r,\infty}$ называются делителями p_∞, так как соответствующие им метрики являются продолжениями метрики $|x|^\rho$ поля рациональных чисел.

Рассматривавшееся в § 2 кольцо $K_\mathfrak{p}$ в применении к расширению $k/\mathbb{Q}$ и к простому рациональному числу p совпадает с кольцом k_p последовательностей $(\xi_1, \ldots, \xi_m)$, где $\xi \in k_{\mathfrak{p}_i}$. Размерность кольца k_p как линейного пространства над полем p-адических чисел $\mathbb{Q}_p$ равна $n = (k:\mathbb{Q})$ (теорема 1 § 2). Аналогичным понятием в случае бесконечного простого дивизора p_∞ является кольцо k_{p_∞}, состоящее из последовательностей $(\xi_1, \ldots, \xi_s, \xi_{s+1}, \ldots, \xi_{s+t})$, где ξ_i $(1 \leqslant i \leqslant s)$ принадлежат полю вещественных чисел, а ξ_{s+j} $(1 \leqslant j \leqslant t)$ — полю комплексных чисел. Кольцо k_{p_∞}, являющееся линейным пространством размерности $n = (k:\mathbb{Q})$ над полем вещественных чисел $\mathbb{Q}_\infty$, совпадает, таким образом, с кольцом $\mathfrak{L}^{s,t}$, которое мы рассматривали в гл. II и которое являлось основным инструментом при изучении группы единиц и классов модулей поля алгебраических чисел k. Не меньшую роль кольцо k_{p_∞} будет играть в § 1 гл. V.

2. Соотношение между метриками. Для каждого простого дивизора $\mathfrak{p}$ поля k (как конечного, так и бесконечного) введем понятие связанной с ним *нормированной метрики* $\varphi_\mathfrak{p}$, определяемой специальным выбором значения ρ. Если $\mathfrak{p}$ — конечный простой дивизор, то нормированная метрика $\varphi_\mathfrak{p}$ определяется равенством

$$\varphi_\mathfrak{p}(\xi) = (1/N(\mathfrak{p}))^{v_\mathfrak{p}(\xi)}, \qquad \xi \in k,$$

где $N(\mathfrak{p})$ — норма дивизора $\mathfrak{p}$. Для бесконечного вещественного $\mathfrak{p}$, соответствующего вещественному изоморфизму $\sigma\colon k \to \mathbb{C}$, полагаем

$$\varphi_\mathfrak{p}(\xi) = |\sigma(\xi)|, \qquad \xi \in k.$$

Наконец, если $\mathfrak{p}$ — бесконечный комплексный простой дивизор, соответствующий паре сопряженных комплексных изоморфизмов σ и $\bar{\sigma}$, то нормированная метрика $\varphi_\mathfrak{p}$ определяется формулой

$$\varphi_\mathfrak{p}(\xi) = |\sigma(\xi)|^2 = |\bar{\sigma}(\xi)|^2 = \sigma(\xi)\bar{\sigma}(\xi).$$

Относительно последнего случая следует отметить, что функция $|\sigma(\xi)|^2$, строго говоря, не является метрикой в смысле определения п. 1 § 4 гл. I, так как для нее неравенство треугольника 2° не соблюдается. Однако ввиду того, что $|\sigma(\xi)|^2$ является квадратом метрики, эта функция также может быть использована для

определения сходимости на поле k, а потому может рассматриваться нами наравне с метриками.

Для любого $\xi \neq 0$ из k мы имеем, очевидно, только конечное число простых дивизоров $\mathfrak{p}$, для которых $\varphi_{\mathfrak{p}}(\xi) \neq 1$. В силу этого имеет смысл формально бесконечное произведение $\prod_{\mathfrak{p}} \varphi_{\mathfrak{p}}(\xi)$.

Теорема 2. *Для любого $\xi \neq 0$ из поля алгебраических чисел k значения $\varphi_{\mathfrak{p}}(\xi)$ всех нормированных метрик удовлетворяют соотношению*

$$\prod_{\mathfrak{p}} \varphi_{\mathfrak{p}}(\xi) = 1 \tag{3}$$

($\mathfrak{p}$ пробегает все простые дивизоры поля k, как конечные, так и бесконечные).

Доказательство. Обозначим через P и P' произведения значений $\varphi_{\mathfrak{p}}(\xi)$, распространенные соответственно на все бесконечные и на все конечные $\mathfrak{p}$, так что произведение, стоящее в левой части равенства (3), равно PP'. По определению нормированных метрик для бесконечных $\mathfrak{p}$ мы имеем

$$P = \prod_{\sigma} |\sigma(\xi)| = \left|\prod_{\sigma} \sigma(\xi)\right| = |N(\xi)|$$

(здесь σ пробегает все $n = s + 2t$ изоморфизмов k в поле $\mathbb{C}$). С другой стороны, по формуле (1) § 7 гл. III норма главного дивизора $(\xi) = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\xi)}$ (здесь $\mathfrak{p}$ пробегает все конечные простые дивизоры) равна

$$|N(\xi)| = N\left(\prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\xi)}\right) = \prod_{\mathfrak{p}} N(\mathfrak{p})^{\nu_{\mathfrak{p}}(\xi)} = \frac{1}{P'},$$

что и доказывает теорему.

Задачи

1. Пусть $\varphi_1, \ldots, \varphi_r$ $(r = s + t)$ — метрики поля алгебраических чисел k степени $n = s + 2t$, соответствующие бесконечным простым дивизорам. Доказать, что для любого $i = 1, \ldots, r$ в k существует число ξ_i, для которого $\varphi_i(\xi_i) > 1$. $\varphi_j(\xi_i) < 1$, $j \neq i$. Показать, далее, что метрики $\varphi_1, \ldots, \varphi_r$ определяют различные сходимости на k.

2. Показать, что всякое соотношение вида

$$\prod_{\mathfrak{p}} \varphi_{\mathfrak{p}}(\xi)^{m_{\mathfrak{p}}} = 1, \qquad \xi \in k^*,$$

между нормированными метриками $\varphi_{\mathfrak{p}}$ поля алгебраических чисел k является следствием соотношения (3), т. е. что это равенство выполняется для всех $\xi \in k^*$ лишь при условии $m_{\mathfrak{p}} = m$ при любом $\mathfrak{p}$.

§ 5. Аналитические функции в полных полях

1. Степенные ряды. Некоторые сведения о рядах в полном поле k с показателем v нам уже известны (см. п. 2 § 1 этой главы и п. 4 § 3 гл. I). Так, мы знаем, что в поле k ряд $\sum_{n=1}^{\infty} a_n$ сходится тогда и только тогда, когда $a_n \to 0$ при $n \to \infty$; что сходящиеся ряды можно почленно складывать, вычитать и умножать на постоянный множитель; что для сходящихся рядов справедливо сочетательное свойство. Известно, далее, что при любой перестановке членов сходящегося ряда его сходимость не нарушается и сумма не меняется. Отсюда легко следует, что если произведения $a_i b_j$ членов двух сходящихся рядов $\sum_{i=1}^{\infty} a_i = s$ и $\sum_{j=1}^{\infty} b_j = t$ выписать в каком-нибудь порядке и составить из них ряд, то этот ряд будет сходящимся и его сумма будет равна st.

Отметим для дальнейшего одну простую теорему о двойном ряде. Напомним, что двойной ряд

$$\sum_{i,j=1}^{\infty} a_{ij} \tag{1}$$

называется сходящимся к сумме s, если $\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij} \to s$ при $m, n \to \infty$. Ряды

$$\sum_{i=1}^{\infty}\left(\sum_{j=1}^{\infty} a_{ij}\right), \qquad \sum_{j=1}^{\infty}\left(\sum_{i=1}^{\infty} a_{ij}\right)$$

называются повторными рядами двойного ряда (1).

Теорема 1. *Если для любого N почти для всех пар (i, j) имеем $v(a_{ij}) > N$, то двойной ряд* (1) *сходится и его сумма равна суммам обоих повторных рядов, которые также сходятся. Если из членов двойного ряда* (1) *образовать каким-нибудь способом простой ряд, то он тоже будет сходиться, и к той же сумме.*

Доказательство этой теоремы совсем просто, и мы предоставляем его читателю.

Степенным рядом в поле k называется ряд вида

$$f(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + \ldots + a_n x^n + \ldots, \tag{2}$$

где $a_n \in k$. Если ряд (2) сходится при $x = x_0 \in k$, то он сходится и для всех тех $x \in k$, для которых $v(x) \geqslant v(x_0)$. Действительно, для всех таких x мы имеем $v(a_n x^n) \geqslant v(a_n x_0^n)$, и поэтому вместе с $a_n x_0^n$ общий член $a_n x^n$ также стремится к нулю при $n \to \infty$. Таким образом, если через μ мы обозначим $\min v(x)$, где x пробе-

гает все значения из k, при которых ряд (2) сходится, то область сходимости этого ряда будет характеризоваться условием $v(x) \geqslant \mu$ (или он будет сходиться при всех x).

Если мы имеем два степенных ряда $f_1(x) = \sum_{n=0}^{\infty} a_n x^n$ и $f_2(x) = \sum_{n=0}^{\infty} b_n x^n$, то под их произведением $h(x)$ понимается степенной ряд, полученный формальным перемножением данных рядов, т. е. ряд $\sum_{n=0}^{\infty} c_n x^n$, где $c_n = \sum_{i+j=n} a_i b_j$. Пусть ряды $f_1(x)$ и $f_2(x)$ сходятся при $v(x) \geqslant \mu_1$ и $v(x) \geqslant \mu_2$ соответственно. Очевидно, что тогда $h(x)$ будет сходящимся при $v(x) \geqslant \max(\mu_1, \mu_2)$ и его сумма будет равна $f_1(x) f_2(x)$.

Степенной ряд $f(x)$ в своей области сходимости является непрерывной функцией от x. Действительно, все члены $a_n x^n$ при $n \geqslant 1$ будут сколь угодно малы, если только значение для x достаточно мало. Отсюда следует, что $f(x) \to a_0 = f(0)$ при $x \to 0$, т. е. функция $f(x)$ непрерывна в точке $x = 0$. Пусть теперь c — произвольное значение из области сходимости ряда $f(x)$. Заменим каждый член $a_n x^n$ выражением $a_n (c + y)^n$. Раскрыв здесь скобки и просуммировав все такие многочлены, мы получим степенной ряд $f_c(y)$. Это приводит нас к формуле

$$f(c + y) = f_c(y), \tag{3}$$

справедливой для любого y из области сходимости ряда $f(x)$. По доказанному $f_c(y) \to f_c(0)$ при $y \to 0$, поэтому $f(x) \to f(c)$ при $x \to c$, и непрерывность $f(x)$ при $x = c$ доказана.

Функция $f(x)$, определенная в некоторой области полного поля с показателем и представимая в этой области сходящимся степенным рядом, называется *аналитической функцией*.

Рассмотрим степенной ряд

$$g(y) = b_1 y + \ldots + b_n y^n + \ldots$$

без свободного члена. Результат формальной подстановки ряда $g(y)$ в ряд $f(x)$ (вместо x) будет степенным рядом $F(y)$ от y. Именно, если

$$a_n (g(y))^n = c_{nn} y^n + c_{n,\, n+1} y^{n+1} + \ldots, \tag{4}$$

то

$$F(y) = a_0 + c_{11} y + (c_{12} + c_{22}) y^2 + \ldots + (c_{1n} + c_{2n} + \ldots + c_{nn}) y^n + \ldots$$

Теорема 2 (о подстановке ряда в ряд). *Пусть ряд $f(x)$ сходится при $v(x) \geqslant \mu$. Если в указанных выше обозначениях для некоторого $y \in k$ ряд $g(y)$ сходится и $v(b_m y^m) \geqslant \mu$ при всех $m \geqslant 1$, то ряд $F(y)$ также сходится и*

$$F(y) = f(g(y)).$$

Доказательство. Рассмотрим двойной ряд

$$\sum_{i,j} c_{ij} y^j. \tag{5}$$

В силу (4) имеем $c_{nm}y^m = \sum_{\substack{\alpha_1,\ldots,\alpha_n \geqslant 1 \\ \alpha_1+\ldots+\alpha_n=m}} a_n b_{\alpha_1} y^{\alpha_1} \ldots b_{\alpha_n} y^{\alpha_n}$. Пусть $N = \min_m v(b_m y^m)$. Тогда

$$v(c_{nm}y^m) \geqslant \min_{\alpha_1,\ldots,\alpha_n} \left(v\left(a_n b_{\alpha_1} y^{\alpha_1} \ldots b_{\alpha_n} y^{\alpha_n}\right)\right) \geqslant v(a_n) + nN.$$

Так как $N = v(x_0)$ при некотором x_0 и при $x = x_0$ ряд $f(x)$ сходится, то $v(a_n) + nN = v\left(a_n x_0^n\right) \to \infty$, а значит, и $v(c_{nm}y^m) \to \infty$ при $n \to \infty$ равномерно для всех m. Далее, при фиксированном n ряд (4) сходится (как произведение сходящихся рядов), поэтому $v(c_{nm}y^m) \to \infty$ при $m \to \infty$. Этим доказано, что для двойного ряда (5) выполнено условие теоремы 1. В силу этой теоремы оба повторных ряда для (5) сходятся и имеют одну и ту же сумму. Теперь остается лишь заметить, что

$$F(y) = a_0 + \sum_j \left(\sum_i c_{ij} y^j\right) \quad \text{и} \quad f(g(y)) = a_0 + \sum_i \left(\sum_j c_{ij} y^j\right),$$

и теорема 2 доказана.

В следующих двух параграфах мы будем рассматривать также аналитические функции от n переменных, т. е. функции, представимые в виде степенных рядов

$$f(x_1, \ldots, x_n) = \sum_{\alpha_1,\ldots,\alpha_n \geqslant 0} a_{\alpha_1 \ldots \alpha_n} x_1^{\alpha_1} \ldots x_n^{\alpha_n}.$$

Предположим, что ряд $f(x_1, \ldots, x_n)$ в n-мерном пространстве над полным полем с показателем сходится в области $v(x_i) \geqslant N$ $(i = 1, \ldots, n)$. Если $c = (c_1, \ldots, c_n)$ — точка из этой области, то, аналогично случаю одной переменной (применив теорему 1), легко можно получить тождество

$$f(x_1 + c_1, \ldots, x_n + c_n) = f_c(x_1, \ldots, x_n),$$

справедливое для всех точек из области $v(x_i) \geqslant N$ (в этом тождестве степенной ряд f_c также сходится при $v(x_i) \geqslant N$).

2. Показательная и логарифмическая функция. В этом пункте мы предположим, что k есть конечное расширение поля p-адических чисел $\mathbb{Q}_p$. Через v мы обозначим показатель поля k, через e — индекс ветвления k относительно $\mathbb{Q}_p$ и через π — простой элемент кольца целых элементов в k.

Рассмотрим в поле k степенные ряды

$$\exp x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots + \frac{x^n}{n!} + \ldots, \tag{6}$$

$$\ln(1+x) = x - \frac{x^2}{2} + \ldots + (-1)^{n-1}\frac{x^n}{n} + \ldots \tag{7}$$

Выясним область сходимости ряда (6). Так как простое число p входит в $n!$ с показателем $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots$, то

$$v(n!) = e\left(\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots\right) < en\sum_{k=1}^{\infty}\frac{1}{p^k} = \frac{en}{p-1},$$

а значит,

$$v\left(\frac{x^n}{n!}\right) = nv(x) - v(n!) > n\left(v(x) - \frac{e}{p-1}\right). \tag{8}$$

Если теперь $v(x) > \frac{e}{p-1}$, то $v\left(\frac{x^n}{n!}\right) \to \infty$ при $n \to \infty$, и ряд (6) сходится. С другой стороны, при $v(x) \leqslant \frac{e}{p-1}$ и при $n = p^s$ мы имеем

$$v\left(\frac{x^n}{n!}\right) = nv(x) - e(p^{s-1} + \ldots + p + 1) =$$

$$= nv(x) - e\frac{n-1}{p-1} = n\left(v(x) - \frac{e}{p-1}\right) + \frac{e}{p-1} \leqslant \frac{e}{p-1},$$

а значит, для таких x общий член ряда (6) не стремится к нулю. Этим доказано, что ряд (6) сходится для тех n только тех x, для которых $v(x) \geqslant \varkappa$, где $\varkappa = \left[\frac{e}{p-1}\right] + 1$. Формальное перемножение степенных рядов $\exp x$ и $\exp y$ дает, как легко видеть, ряд $\exp(x+y)$, поэтому при $v(x) \geqslant \varkappa$ и $v(y) \geqslant \varkappa$ имеет место формула

$$\exp(x+y) = \exp x \cdot \exp y. \tag{9}$$

Обратимся теперь к ряду (7). Если $v(x) \leqslant 0$, то $v(x^n/n)$ не стремится к бесконечности при $n \to \infty$, и поэтому для таких x ряд (7) не сходится. Пусть теперь $v(x) \geqslant 1$. Если $n = p^a n_1$, $(n_1, p) = 1$, то $p^a \leqslant n$ и $v(n) = ea \leqslant e\frac{\ln n}{\ln p}$, откуда

$$v(x^n/n) = nv(x) - v(n) \geqslant nv(x) - e\frac{\ln n}{\ln p},$$

а значит, $v(x^n/n) \to \infty$ при $n \to \infty$. Таким образом, ряд (7) сходится тогда и только тогда, когда $v(x) \geqslant 1$.

Если $v(x) \geqslant 1$, то элемент $\varepsilon = 1 + x$ является, очевидно, единицей в кольце $\mathfrak{o}$ целых элементов поля k, при этом $\varepsilon \equiv 1 \pmod{\pi}$.

Обратно, если для единицы выполнено последнее сравнение, то она имеет вид $\varepsilon = 1 + x$, где $v(x) \geqslant 1$. Такие единицы кольца o называются главными единицами поля k. Ряд (7) определяет, таким образом, функцию $\ln \varepsilon$ на мультипликативной группе всех главных единиц поля k. Покажем, что для любых двух главных единиц ε_1 и ε_2 имеет место формула

$$\ln(\varepsilon_1 \varepsilon_2) = \ln \varepsilon_1 + \ln \varepsilon_2. \tag{10}$$

Пусть $\varepsilon_1 = 1 + x$, $\varepsilon_2 = 1 + y$, и пусть $v(y) \geqslant v(x)$, так что $y = tx$ с целым t и

$$(1 + x)(1 + y) = 1 + (t + 1)x + tx^2.$$

Будем рассматривать выражение $(t + 1)x + tx^2$ как степенной ряд от x, все члены которого принадлежат области сходимости ряда $\ln(1 + z)$. Так как формальная подстановка этого выражения в ряд $\ln(1 + z)$ дает нам $\ln(1 + x) + \ln(1 + tx)$, то ввиду теоремы 2 получаем равенство

$$\ln(1 + (t + 1)x + tx^2) = \ln(1 + x) + \ln(1 + tx),$$

которое и доказывает формулу (10).

Формальная подстановка ряда (7) в ряд (6), а также ряда $\exp x - 1$ в ряд (7) дает нам следующие формальные тождества:

$$\exp \ln(1 + x) = 1 + x, \tag{11}$$

$$\ln \exp x = x. \tag{12}$$

Поскольку здесь речь идет о формальных равенствах, то для их проверки мы можем считать x комплексной переменной и воспользоваться теоремой о подстановке ряда в ряд для комплексных степенных рядов (см., например, [17], с. 206—208). Чтобы выяснить, при каких условиях формальные тождества (11) и (12) можно рассматривать как равенства в поле k, обратимся к теореме 2. Согласно этой теореме равенство (11) будет справедливо, если все члены ряда $\ln(1 + x)$ удовлетворяют условию $v(x^n/n) \geqslant \varkappa$. При $n = 1$ это дает нам условие $v(x) \geqslant \varkappa$. Но если $v(x) \geqslant \varkappa$, то $v(x^n/n) \geqslant n\varkappa \geqslant \varkappa$ при $1 \leqslant n \leqslant p - 1$ и

$$v(x^n/n) - \varkappa \geqslant (n - 1)\varkappa - v(n) > $$

$$> (n - 1)\frac{e}{p - 1} - e\frac{\ln n}{\ln p} = \frac{e(n - 1)}{\ln p}\left(\frac{\ln p}{p - 1} - \frac{\ln n}{n - 1}\right) \geqslant 0$$

при $n \geqslant p \geqslant 2$ (здесь мы воспользовались тем, что функция $\dfrac{\ln t}{t - 1}$ при $t \geqslant 2$ монотонно убывает). Следовательно, равенство (11) справедливо при условии $v(x) \geqslant \varkappa$. Кроме того, мы видим, что при том же условии $v(\ln(1 + x)) \geqslant \varkappa$. Перейдем к формуле (12). Из (8) следует, что при $v(x) \geqslant \varkappa$ все члены ряда $\exp x - 1$ содержатся в области сходимости ряда $\ln(1 + x)$, а значит, формула (12) справедлива для всех тех x, для которых $\exp x$ имеет смысл.

Обозначим через A аддитивную группу всех тех $x \in k$, для которых $v(x) \geqslant \varkappa$, и через M — мультипликативную группу единиц $\varepsilon = 1 + x$, $x \in A$. По доказанному отображение $\varepsilon \to \ln \varepsilon$ ($\varepsilon \in M$) является гомоморфизмом группы M в группу A. Покажем, что отображение $x \to \exp x$ является гомоморфизмом A в M. Ввиду (9) мы должны, очевидно, лишь проверить, что $v(x^n/n!) \geqslant \varkappa$ при всех $x \in A$ и всех $n \geqslant 1$. Пусть $p^s \leqslant n < p^{s+1}$. Тогда

$$v\left(\frac{x^n}{n!}\right) - \varkappa \geqslant (n-1)\varkappa - e\left(\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^s}\right]\right) \geqslant$$

$$\geqslant \frac{(n-1)e}{p-1} - \frac{en}{p^s}\frac{p^s-1}{p-1} \geqslant 0,$$

что и требовалось получить. Формулы (11) и (12) показывают теперь, что отображения $\ln\colon M \to A$ и $\exp\colon A \to M$ взаимно однозначны и обратны друг другу. Мы доказали, таким образом, следующий результат.

Теорема 3. *Отображение $x \to \exp x$ является изоморфизмом аддитивной группы всех тех целых чисел поля k, которые делятся на $\pi^\varkappa\left(\varkappa = \left[\frac{e}{p-1}\right] + 1\right)$, на мультипликативную группу главных единиц ε, сравнимых с 1 по модулю $\pi^\varkappa$. Обратный изоморфизм осуществляется отображением $\varepsilon \to \ln \varepsilon$ (для $\varepsilon \equiv 1 \pmod{\pi^\varkappa}$).*

Что касается отображения $\varepsilon \to \log \varepsilon$ на всей группе главных единиц, то оно, вообще говоря, уже не является изоморфизмом (задача 5). Кроме того, значение $\ln \varepsilon$ не обязательно является целым.

Наряду с функцией e^x в вещественном анализе рассматривают также показательную функцию $a^x = e^{x \ln a}$. Ее аналогом в поле k является функция

$$\eta^x = \exp(x \ln \eta), \tag{13}$$

где η — главная единица поля k. Эта функция определена, очевидно, при условии $v(x) \geqslant \varkappa - v(\ln \eta)$. Если поэтому $\eta \equiv 1 \pmod{\pi^\varkappa}$, то η^x будет иметь смысл при всех целых x из k, при этом для значений η^x будет выполнено сравнение $\eta^x \equiv 1 \pmod{\pi^\varkappa}$. Для показательной функции (13) в случае $\eta \equiv 1 \pmod{\pi^\varkappa}$ при любых целых x и y имеют место формулы

$$\eta^{x+y} = \eta^x \eta^y, \quad (\eta^x)^y = \eta^{xy}. \tag{14}$$

Задачи

1. Доказать, что функция $f(x)$, аналитическая при $v(x) \geqslant \mu$ (в полном поле с показателем v) и имеющая бесконечно много нулей в области $v(x) \geqslant \mu$, тождественно равна нулю.

2. Пусть k — поле характеристики 0, полное относительно неархимедовой метрики φ (задача 4 § 4 гл. I). Предположим, что метрика φ такова, что $\varphi(p) < 1$ для некоторого простого рационального числа p. Доказать, что

область сходимости ряда $\ln(1+x)$ в поле k характеризуется условием $\varphi(x) < 1$, а область сходимости ряда $\exp x$ — условием $\varphi(x) < \sqrt[p-1]{\varphi(p)}$.

3. При тех же условиях определить область сходимости рядов

$$\sin x = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{x^{2n-1}}{(2n-1)!}, \qquad \cos x = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!}.$$

4. Найти ошибку в следующем доказательстве иррациональности числа π. Число π есть наименьшее положительное число, для которого $\sin \pi = 0$. Пусть π рационально. Так как $\pi > 3$, то его числитель должен делиться либо на нечетное простое число p, либо на 2^2 (в последнем случае положим $p = 2$). Отсюда следует, что ряды $\sin x$ и $\cos x$ в поле p-адических чисел $\mathbb{Q}_p$ сходятся при $x = \pi$. Но ввиду формулы

$$\sin(x+y) = \sin x \cos y + \cos x \sin y$$

из равенства $\sin \pi = 0$ вытекает, что $\sin n\pi = 0$ при любом натуральном n. Функция $\sin x$ имеет, таким образом, в своей области сходимости бесконечно много нулей. Следовательно, согласно задаче 1 она тождественно равна нулю, и мы получили противоречие.

5. Пусть k — конечное расширение поля p-адических чисел $\mathbb{Q}_p$ и ε — главная единица поля k. Показать, что $\ln \varepsilon = 0$ тогда и только тогда, когда ε есть корень степени p^s $(s \geqslant 0)$ из 1.

6. Сохраним все обозначения пункта 2. Главные единицы ε, которые $\equiv 1 \pmod{\pi^k}$, образуют, очевидно, мультипликативную группу M_k. Все целые числа поля k, делящиеся на π^k, образуют аддитивную группу A_k. Доказать, что при $k \geqslant \varkappa$ отображение $\varepsilon \to \ln \varepsilon$, $\varepsilon \in M_k$ является изоморфизмом группы M_k на группу A_k (обратным изоморфизмом будет отображение $x \to \exp x$, $x \in A_k$).

7. Доказать, что в полном поле с показателем область сходимости степенного ряда $f(x) = \sum_{n=0}^{\infty} a_n x^n$ содержится в области сходимости его производной $f'(x) = \sum n a_n x^{n-1}$. Показать на примере, что области сходимости рядов $f(x)$ и $f'(x)$ могут не совпадать (даже в случае поля нулевой характеристики).

8. Доказать, что в кольце 2-целых чисел сумма

$$2 + \frac{2^2}{2} + \frac{2^3}{3} + \ldots + \frac{2^n}{n}$$

делится на сколь угодно большую степень двойки, если только n достаточно велико.

9. Доказать, что все коэффициенты a_n ряда

$$E_p(x) = \exp\left(x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \ldots\right) = \sum_{n=0}^{\infty} a_n x^n$$

являются p-целыми рациональными числами (p простое).

Указание. Доказать, что число

$$T_n = a_n n! = \sum_{s \geqslant 1} \sum_{\substack{p^{\alpha_1} + \ldots + p^{\alpha_s} = n \\ \alpha_1 \geqslant 0, \ldots, \alpha_s \geqslant 0}} \frac{n!}{s! p^{\alpha_1} p^{\alpha_2} \ldots p^{\alpha_s}}$$

равно числу элементов в симметрической группе n-й степени, порядок которых есть степень p, и применить теорему о том, что для любого делителя d порядка конечной группы G число элементов $u \in G$, удовлетворяющих уравнению $u^d = 1$, делится на d.

10. Доказать, что $E_p(x) = \prod_{(m,p)=1} (1 - x^m)^{-\mu(m)/m}$ (m пробегает все натуральные числа, взаимно простые с p, $\mu(m)$ — функция Мёбиуса).

11. Пусть η — главная единица из конечного расширения поля p-адических чисел и x — целое p-адическое число. Выберем последовательность натуральных чисел $\{a_n\}$, сходящуюся к x. Доказать существование предела $\lim_{n\to\infty} \eta^{a_n}$ и его независимость от выбора $\{a_n\}$ (см. задачу 14 § 3 гл. I). Доказать, далее, что функция $\eta^x = \lim_{n\to\infty} \eta^{a_n}$ обладает свойствами (14) и в общей области определения совпадает с функцией (13).

12. Пусть k — конечное расширение поля p-адических чисел степени инерции f относительно $\mathbb{Q}_p$. Показать, что группа всех единиц в кольце целых элементов поля k есть прямое произведение содержащейся в k группы корней степени $p^f - 1$ из 1 и подгруппы главных единиц (использовать задачу 10 § 1).

Замечание. Функцию ln можно распространить на всю группу единиц кольца целых элементов поля k. Именно, если $\varepsilon = \theta\eta$, где θ — корень степени $p^f - 1$ из 1 и η — главная единица, то полагаем $\ln \varepsilon = \ln \eta$.

6. Метод Сколема

В этом параграфе мы изложим принадлежащий Сколему метод исследования неопределенных уравнений вида

$$F(x_1, \ldots, x_m) = c, \tag{1}$$

где F — неприводимая разложимая неполная форма (см. п. 3 § 1 гл. II), а c — рациональное число. Этот метод основан на применении простых свойств локальных аналитических многообразий над полем $\mathfrak{P}$-адических чисел, доказательства которых изложены в следующем параграфе.

1. Представление чисел неполными разложимыми формами. Согласно п. 3 § 1 гл. II уравнение (1) может быть записано в виде

$$N(x_1\mu_1 + \ldots + x_m\mu_m) = a \tag{2}$$

или

$$N(\alpha) = a, \qquad \alpha \in M, \tag{3}$$

где $\mu_1, \ldots, \mu_m$ — числа из некоторого поля алгебраических чисел k, а $M = \{\mu_1, \ldots, \mu_m\}$ — модуль, порожденный этими числами (a — рациональное число). Заменив, быть может, форму F целочисленно эквивалентной ей формой, мы можем добиться того, чтобы в представлении (2) образующие $\mu_1, \ldots, \mu_m$ модуля M были линейно независимыми над полем рациональных чисел $\mathbb{Q}$. По условию модуль M неполный, поэтому $m < n = (k : \mathbb{Q})$.

В гл. II мы видели, как находятся все решения уравнения (3), если M — полный модуль поля k. Естественно поэтому для реше-

ния уравнения (3) вложить модуль M в полный модуль $\overline{M}$ и найти, пользуясь методами гл. II, все решения уравнения $N(\alpha)=a$, $\alpha\in\overline{M}$, а затем отобрать из них те решения α, которые содержатся в M.

То, что любой модуль в k можно вложить в полный модуль, очевидно. Для этого достаточно дополнить любым образом систему линейно независимых чисел $\mu_1, \ldots, \mu_m$ до базиса $\mu_1, \ldots, \mu_n$ поля k и положить $\overline{M}=\{\mu_1, \ldots, \mu_n\}$.

Если все $\alpha\in\overline{M}$, для которых $N(\alpha)=a$, уже найдены, то мы получим все решения уравнения (3), если среди этих $\alpha\in\overline{M}$ выделим те, у которых в представлении

$$\alpha=x_1\mu_1+\ldots+x_n\mu_n$$

коэффициенты $x_{m+1}, \ldots, x_n$ равны нулю. Чтобы условия $x_{m+1}=0, \ldots, x_n=0$ выразить непосредственно через α, удобно воспользоваться взаимным базисом $\mu_1^*, \ldots, \mu_n^*$ для базиса $\mu_1, \ldots, \mu_n$ (см. Дополнение, § 2, п. 3). Так как след $\operatorname{Sp}\mu_j\mu_i^*$ равен 0 при $i\neq j$ и равен 1 при $i=j$, то $x_i=\operatorname{Sp}\alpha\mu_i^*$ $(1\leqslant i\leqslant n)$. Отсюда следует, что числа $\alpha\in\overline{M}$, принадлежащие подмодулю M, характеризуются условиями

$$\operatorname{Sp}\alpha\mu_i^*=0, \qquad i=m+1, \ldots, n. \tag{4}$$

Согласно теореме 1 § 5 гл. II все решения уравнения $N(\alpha)=a$, $\alpha\in\overline{M}$, записываются в виде

$$\alpha=\gamma_j\varepsilon_1^{u_1}\ldots\varepsilon_r^{u_r}, \qquad 1\leqslant j\leqslant h, \tag{5}$$

где $\gamma_1, \ldots, \gamma_h$ — некоторое конечное множество чисел модуля $\overline{M}$ с нормой a, $\varepsilon_1, \ldots, \varepsilon_r$ — система независимых единиц поля k и $u_1, \ldots, u_r$ — произвольные целые рациональные числа. В силу (4) решение уравнения (3) равносильно, таким образом, решению h систем уравнений вида

$$\operatorname{Sp}\left(\gamma\mu_i^*\varepsilon_1^{u_1}\ldots\varepsilon_r^{u_r}\right)=0, \qquad i=m+1, \ldots, n, \tag{6}$$

относительно целых рациональных $u_1, \ldots, u_r$ (здесь γ — одно из γ_j).

Пусть K — поле алгебраических чисел, содержащее все поля, сопряженные с k, и пусть $\sigma_1, \ldots, \sigma_n$ — все изоморфизмы k в K. Так как $\operatorname{Sp}\xi=\sigma_1(\xi)+\ldots+\sigma_n(\xi)$ для любого $\xi\in k$, то систему (6) можно переписать так:

$$\sum_{j=1}^{n}\sigma_j\left(\gamma\mu_i^*\right)\sigma_j(\varepsilon_1)^{u_1}\ldots\sigma_j(\varepsilon_r)^{u_r}=0, \qquad i=m+1, \ldots, n. \tag{7}$$

Ясно, что для доказательства конечности числа решений уравнения (3) нам достаточно показать, что каждая из систем вида (7) имеет лишь конечное число решений в целых рациональных числах $u_1, \ldots, u_r$.

Замечание. Совокупность чисел поля k, записываемых в виде $\varepsilon_1^{u_1} \dots \varepsilon_r^{u_r}$, где $u_1, \dots, u_r$ пробегают все целые рациональные числа, назовем мультипликативной подгруппой поля k и обозначим через U. Все решения уравнения (3) совпадают, очевидно, с числами из пересечений

$$M \cap \gamma_j U, \qquad j = 1, \dots, h. \tag{8}$$

Вместо любого из множеств (8) можно рассмотреть подобное ему множество $\gamma_j^{-1} M \cap U$. Мы видим, таким образом, что задача о нахождении решений уравнения (1) сводится к задаче о пересечении модуля и мультипликативной подгруппы поля k. Добавим к этому, что вместо модуля M в пересечениях (8) можно взять линейное пространство L (над полем $\mathbb{Q}$), натянутое на $\mu_1, \dots, \mu_m$. Действительно, так как $\gamma_j U \subset \overline{M}$ и $L \cap \overline{M} = M$, то $L \cap \gamma_j U = M \cap \gamma_j U$.

2. Связь с локальными аналитическими многообразиями. Идея метода Сколема заключается в том, что в некоторых случаях удается доказать конечность числа решений уравнения (1), показав, что система (7) имеет лишь конечное число решений даже в том случае, если неизвестные $u_1, \dots, u_r$ искать среди целых $\mathfrak{P}$-адических чисел (т. е. среди целых элементов пополнения $K_{\mathfrak{P}}$), где $\mathfrak{P}$ — произвольно выбранный простой дивизор поля K. При таком расширении области возможных значений неизвестных мы можем интерпретировать совокупность решений системы (7) как локальное аналитическое многообразие в r-мерном пространстве и для их исследования применить свойства этих многообразий.

Разрешая переменным $u_1, \dots, u_r$ в левых частях уравнений (7) принимать $\mathfrak{P}$-адические значения, мы сталкиваемся, однако, с тем затруднением, что показательная функция $\varepsilon^u = \exp(u \ln \varepsilon)$ определена для любого целого $\mathfrak{P}$-адического числа u только в случае, когда ε удовлетворяет сравнению $\varepsilon \equiv 1 \pmod{\mathfrak{P}^\varkappa}$ ($\varkappa$ — целое число, зависящее лишь от поля $K_{\mathfrak{P}}$; см. конец § 5). Эта трудность обходится следующим образом. Согласно задаче 6 § 7 гл. III существует такое натуральное число q, что для любого целого числа $\alpha \in K$, не делящегося на $\mathfrak{P}$, справедливо сравнение

$$\alpha^q \equiv 1 \pmod{\mathfrak{P}^\varkappa}. \tag{9}$$

Любой показатель u_i в формуле (5) можно записать в виде

$$u_i = \rho_i + q v_i, \qquad 0 \leqslant \rho_i < q, \qquad v_i \in \mathbb{Z},$$

и, следовательно, для единицы $\varepsilon = \varepsilon_1^{u_1} \dots \varepsilon_r^{u_r}$ имеет место представление $\varepsilon = \delta_l \varepsilon_1^{q v_1} \dots \varepsilon_r^{q v_r}$, $l = 1, \dots, q^r$, где δ_l — одно из q^r чисел $\varepsilon_1^{\rho_1} \dots \varepsilon_r^{\rho_r}$, $0 \leqslant \rho_i < q$.

Мы получаем, таким образом, для чисел α вида (5) новое представление, в котором вместо ε_i стоят ε_i^q, а вместо конечного мно-

жества чисел γ_j — конечное же множество чисел $\gamma_j\delta_l$. Так как ε_i являются единицами, то для них и для $\sigma_j(\varepsilon_i)$ выполнено сравнение (9), а следовательно, функция $\sigma_j(\varepsilon_i^q)^u$ определена для любого целого $\mathfrak{P}$-адического числа $u \in K_{\mathfrak{P}}$. Мы доказали следующий результат.

Лемма 1. *За счет, быть может, другого выбора чисел γ_j и ε_i в формулах* (5) *можно добиться того, чтобы функции $\sigma_j(\varepsilon_i)^u$ были определены для всех целых чисел и поля $K_{\mathfrak{P}}$.*

В дальнейшем мы будем предполагать это условие выполненным без дополнительных оговорок.

Вернемся к системе уравнений (7). Приняв во внимание формулы (9) и (13) § 5, мы можем эти уравнения переписать в виде

$$\sum_{j=1}^{n} A_{ij} \exp L_j(u_1, \ldots, u_r) = 0, \qquad i = m+1, \ldots, n, \tag{10}$$

где $L_j(u_1, \ldots, u_r) = \sum_{k=1}^{r} u_k \log \sigma_j(\varepsilon_k)$, $A_{ij} = \sigma_j(\gamma\mu_i^*)$. Так как левые части уравнений (10) представляются в виде степенных рядов, сходящихся для всех целых $\mathfrak{P}$-адических $u_1, \ldots, u_r$, и, следовательно, являются аналитическими функциями, то все решения системы (10) можно интерпретировать как локальное аналитическое многообразие (в окрестности произвольного решения) в смысле определения § 7.

Число неизвестных в системе (10) равно r, а число уравнений равно $n-m$. Естественно ожидать, что многообразие, определенное этой системой, состоит из конечного числа изолированных точек, если $n-m \geqslant r$. Вспомним, что число r появилось в связи с теоремой Дирихле о единицах и равно $s+t-1$, где s — число вещественных, а t — число пар комплексных изоморфизмов поля k в поле комплексных чисел. Так как $n = s+2t$, то условие $n-m \geqslant r$ равносильно условию $t \geqslant m-1$. В простейшем интересном случае $m=2$ это условие означает, что $t \geqslant 1$, т. е. что среди полей, сопряженных с k, имеется по крайней мере одна пара комплексных. Этот случай, приводящий к теореме Туэ, и будет разобран нами в следующем пункте.

Предположим, что система (10) имеет бесконечно много решений $(u_{1s}, \ldots, u_{rs})$, $s = 1, 2, \ldots$ Ввиду свойства компактности кольца целых $\mathfrak{P}$-адических чисел (см. теорему 6 § 3 гл. I и замечание 2 в конце п. 2 § 1 настоящей главы) из этой последовательности решений можно выделить сходящуюся подпоследовательность, предел которой мы обозначим через $u_1^*, \ldots, u_r^*$. Ясно, что точка $(u_1^*, \ldots, u_r^*$ также удовлетворяет системе (10) и, значит, лежит на многообразии, определяемом этими уравнениями, при этом она обладает тем свойством, что в любой ее окрестности лежит бесконечно много других точек многообразия. Вместо $u_1, \ldots, u_r$

введем новые переменные $v_1, \ldots, v_r$ по формулам

$$u_i = u_i^* + v_i, \qquad 1 \leqslant i \leqslant r.$$

Система (10) перепишется тогда в виде

$$\sum_{j=1}^{n} A_{ij}^* \exp L_j(v_1, \ldots, v_r) = 0, \quad i = m+1, \ldots, n, \tag{11}$$

где нами положено $A_{ij}^* = A_{ij} \exp L_j(u_1^*, \ldots, u_r^*)$. Свободные члены рядов, стоящих слева в уравнениях (11), равны нулю. Обозначим через V локальное аналитическое многообразие (в окрестности точки $(0, \ldots, 0)$), определяемое системой (11) (см. определение § 7). Так как это многообразие не сводится к одной точке (в любой окрестности начала содержится бесконечно много других точек многообразия), то по теореме 2 § 7 на V лежит аналитическая кривая, т. е. существует такая система формальных степенных рядов $\omega_1(t), \ldots, \omega_r(t)$ (не равных одновременно нулю и без свободных членов) с коэффициентами из конечного расширения поля $K_{\mathfrak{B}}$, что ряды

$$P_j(t) = L_j(\omega_1(t), \ldots, \omega_r(t)) \tag{12}$$

удовлетворяют тождественно соотношениям

$$\sum_{j=1}^{n} A_{ij}^* \exp P_j(t) = 0, \qquad i = m+1, \ldots, n.$$

Нами получен, таким образом, следующий результат.

Теорема 1. *Если уравнение* (1) *имеет бесконечное число решений, то хотя бы на одном из локальных аналитических многообразий вида* (11) (*для некоторого* $\gamma = \gamma_j$ *и некоторой точки* $(u_1^*, \ldots, u_r^*)$) *лежит аналитическая кривая.*

Эта теорема и является основой метода Сколема. Она сводит вопрос о конечности числа решений уравнения (1) к доказательству того, что система вида (11) не имеет решений в формальных степенных рядах от одной переменной, т. е. что на соответствующем локальном аналитическом многообразии нет аналитических кривых.

Заметим, что между n рядами $P_j(t)$, определенными равенствами (12), имеется $n-r$ линейных соотношений

$$\sum_{j=1}^{n} B_{ij} P_j(t) = 0, \qquad 1 \leqslant j \leqslant n-r,$$

так как они являются линейными комбинациями r степенных рядов $\omega_k(t)$. Таким образом, наличие на многообразии V аналитической кривой влечет за собой разрешимость (в степенных рядах

$P_i(t)$ без свободных членов) системы

$$\sum_{j=1}^{n} A_{ij}^{*} \exp P_j(t) = 0, \qquad m+1 \leqslant i \leqslant n,$$
$$\sum_{j=1}^{n} B_{ij} P_j(t) = 0, \qquad 1 \leqslant i \leqslant n-r = t+1, \tag{13}$$

в которой отдельно уравнения первой и второй групп линейно независимы. (Линейная независимость уравнений первой группы следует из того, что определитель $\det \sigma_j(\gamma\mu_i^{*})$, квадрат которого равен дискриминанту базиса $\gamma\mu_i^{*}$, отличен от нуля, а потому ранг матрицы (A_{ij}) $(m+1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$ и, следовательно, матрицы (A_{ij}^{*}) равен $n-m$.) Если мы предположим выполненным условие $n-m \geqslant r$, то общее число уравнений в системе (13) будет $\geqslant n$.

3. Теорема Туэ. Теорема Туэ гласит, что если форма $f(x, y) = a_0x^n + a_1x^{n-1}y + \ldots + a_ny^n$ от двух переменных с целыми рациональными коэффициентами неприводима и имеет степень $n \geqslant 3$, то уравнение

$$f(x, y) = c \tag{14}$$

имеет конечное число решений в целых числах. Так как форма от двух переменных всегда разложима и при $n > 2$ неполная, то уравнение (14) входит в класс рассматриваемых нами уравнений (1). Здесь $m = 2$, и поэтому условие $t \geqslant m-1$, при котором можно надеяться на применение метода Сколема, означает, как уже отмечалось, что $t \geqslant 1$, т. е. что уравнение $f(x, 1) = 0$ имеет хотя бы один комплексный корень. В таком случае говорят, что форма $f(x, y)$ имеет комплексный корень. В этом предположении мы и докажем теорему Туэ методом Сколема. Иначе говоря, мы докажем следующее утверждение.

Теорема 2. *Если целочисленная неприводимая форма $f(x, y)$ степени $n \geqslant 3$ имеет хотя бы один комплексный корень, то уравнение $f(x, y) = c$ имеет конечное число решений в целых числах.*

Доказательство. Будем считать, что у формы $f(x, y)$ коэффициент a_0 при x^n равен 1 (если это не так, то мы умножим уравнение (14) на a_0^{n-1} и заменим a_0x на x). Положим $k = \mathbb{Q}(\theta)$, $K = \mathbb{Q}(\theta_1, \ldots, \theta_n)$, где числа $\theta = \theta_1, \theta_2, \ldots, \theta_n$ определены разложением

$$f(x, 1) = (x+\theta_1)\ldots(x+\theta_n).$$

Для каждого $j = 1, \ldots, n$ через σ_j обозначим изоморфизм поля k в K, при котором $\theta \to \theta_j$. Так как $f(x, y) = N(x+y\theta)$ (N обозначает норму относительно расширения $k/\mathbb{Q}$), то уравнение (14) мы можем записать в виде (3), где под M надо понимать модуль $\{1, \theta\}$. Таким образом, в рассматриваемом случае $\mu_1 = 1$, $\mu_2 = \theta$ $(m = 2)$.

Предположим, что уравнение (3) для модуля $M = \{1, \theta\}$ имеет бесконечно много решений $\alpha = x + y\theta$. Тогда при некотором $\gamma = \gamma_j \in k$ бесконечно много этих решений представляется в виде (5), где независимые единицы $\varepsilon_1, \ldots, \varepsilon_r$ поля k подчинены требованию леммы 1. Соответствующие нашим решениям α показатели $u_1, \ldots, u_r$ в равенствах (5) будут удовлетворять системе (10). Выберем среди решений α последовательность $\alpha_1, \alpha_2, \ldots$ так, чтобы соответствующие им точки

$$(u_{1s}, \ldots, u_{rs}), \qquad s = 1, 2, \ldots, \tag{15}$$

сходились к некоторой точке $(u_1^*, \ldots, u_r^*)$. Согласно п. 2 локальное аналитическое многообразие V, определяемое уравнениями (11), содержит аналитическую кривую $\omega_1(t), \ldots, \omega_r(t)$ и для всякой такой кривой на V ряды (12) удовлетворяют некоторой системе вида (13).

Дальнейшее доказательство теоремы 2 основывается на следующем важном вспомогательном результате.

Лемма 2. *Пусть дана система уравнений*

$$\begin{aligned} \sum_{j=1}^{n} a_{ij} \exp P_j &= 0, \qquad i = 1, \ldots, n_1, \\ \sum_{j=1}^{n} b_{ij} P_j &= 0, \qquad i = 1, \ldots, n_2, \end{aligned} \tag{16}$$

в которой уравнения первой и второй групп в отдельности линейно независимы. Если $n_1 = n - 2$, $n_2 \geqslant 2$ и если система имеет решение в формальных степенных рядах $P_1(t), \ldots, P_n(t)$ без свободных членов, то $P_k(t) = P_j(t)$ по крайней мере для двух различных индексов k и j. (Коэффициенты a_{ij} и b_{ij}, а также коэффициенты степенных рядов $P_j(t)$ принадлежат произвольному полю характеристики 0.)

Доказательство этой леммы мы приведем ниже, а сейчас покажем, как из этой леммы вытекает теорема 2.

Согласно лемме 2 для всякой кривой $\omega_1(t), \ldots, \omega_r(t)$ на V по крайней мере для двух различных индексов k и j выполняется равенство $P_k(t) = P_j(t)$, т. е.

$$L_k(\omega_1(t), \ldots, \omega_r(t)) = L_j(\omega_1(t), \ldots, \omega_r(t)). \tag{17}$$

Рассмотрим в r-мерном пространстве точек $(v_1, \ldots, v_r)$ многообразие W, определенное уравнением

$$\prod_{1 \leqslant k < j \leqslant n} (L_k(v_1, \ldots, v_r) - L_j(v_1, \ldots, v_r)) = 0.$$

Из (17) следует, что всякая кривая, принадлежащая локальному аналитическому многообразию V, принадлежит также и W. Но тогда по теореме 3 § 7 $V \subset W$, т. е. все точки многообразия V,

содержащиеся в достаточно малой окрестности начала, принадлежат также и W.

С другой стороны, мы покажем сейчас, что среди точек $(v_{1s}, \ldots, v_{rs}) \in V$, $s = 1, 2, \ldots$, связанных с точками (15) соотношением $u_{is} = u_i^* + v_{is}$ и сходящихся к началу, имеется только конечное число точек, принадлежащих многообразию W. Это противоречие и докажет теорему 2.

Пусть $\alpha = x + y\theta$ и $\alpha' = x' + y'\theta$ — два числа из последовательности $\{\alpha_s\}$, для которых соответствующие точки из V принадлежат многообразию $L_k = L_j$. Если $\alpha = \gamma\varepsilon_1^{u_1} \ldots \varepsilon_r^{u_r}$ и $u_i = u_i^* + v_i$, то

$$\sigma_j(\alpha) = \sigma_j(\gamma)\,\sigma_j(\varepsilon_1)^{u_1^*} \ldots \sigma_j(\varepsilon_r)^{u_r^*}\,\sigma_j(\varepsilon_1)^{v_1} \ldots \sigma_j(\varepsilon_r)^{u_r} = c_j \exp L_j(v_1, \ldots, v_r)$$

и аналогично $\sigma_k(\alpha) = c_k \exp L_k(v_1, \ldots, v_r)$, откуда

$$\sigma_j(\alpha)/c_j = \sigma_k(\alpha)/c_k.$$

Точно таким же образом мы найдем, что

$$\sigma_j(\alpha')/c_j = \sigma_k(\alpha')/c_k.$$

Оба последних равенства вместе дают нам

$$\frac{x + y\theta_j}{x' + y'\theta_j} = \frac{x + y\theta_k}{x' + y'\theta_k},$$

откуда $(xy' - x'y)(\theta_k - \theta_j) = 0$, а так как $\theta_k \neq \theta_j$, то

$$xy' - x'y = 0.$$

Последнее означает, что $x + y\theta = d(x' + y'\theta)$ с некоторым рациональным d. Переходя к нормам и учитывая, что $N(\alpha) = N(\alpha')$, получаем равенство $d^n = 1$, откуда $d = \pm 1$ и, следовательно, $\alpha' = \pm\alpha$.

Итак, на каждом из $n(n-1)/2$ многообразий $L_k = L_j$, объединение которых совпадает с W, содержится не более двух точек из V, соответствующих числам последовательности $\{\alpha_s\}$. Но тогда на W имеется не более $n(n-1)$ таких точек. Следовательно, в любой окрестности начала мы имеем точки многообразия V, не принадлежащие W, а значит, V (как локальное аналитическое многообразие) не может содержаться в W, вопреки полученному ранее включению $V \subset W$. Полученное противоречие, как уже говорилось, и доказывает теорему 2.

Доказательство леммы 2. Так как по условию первая группа уравнений линейно независима, то мы можем (при надлежащей нумерации) выразить $\exp P_i$ $(i = 1, \ldots, n-2)$ через $\exp P_{n-1}$ и $\exp P_n$:

$$\exp P_i = a_i \exp P_{n-1} + b_i \exp P_n. \qquad (18)$$

Если $a_i = 0$, то из равенства $\exp P_i = b_i \exp P_n$, сравнивая свободные члены, находим, что $b_i = 1$ и, следовательно, $P_i = P_n$. Мы можем, таким образом, предполагать, что все a_i отличны от нуля. Положим

$$P_i - P_n = Q_i, \qquad i = 1, \ldots, n-1,$$

и предположим, что все Q_i отличны от нуля. Равенство (18) дает нам

$$\exp Q_i = a_i \exp Q_{n-1} + b_i, \tag{19}$$

откуда, дифференцируя по t (см. задачу 10), получаем

$$Q_i' \exp Q_i = a_i Q_{n-1}' \exp Q_{n-1}. \tag{20}$$

Равенства (19) и (20) приводят нас к соотношениям

$$Q_i' = Q_{n-1}' \exp Q_{n-1} \frac{1}{c_i + \exp Q_{n-1}}, \qquad i = 1, \ldots, n-2, \tag{21}$$

где $c_i = b_i a_i^{-1}$.

Воспользуемся теперь второй группой уравнений (16). По условию среди них имеется по крайней мере два линейно независимых. Но тогда, как легко видеть, мы можем найти нетривиальное соотношение между $Q_1, \ldots, Q_{n-1}$:

$$\sum_{i=1}^{n-1} d_i Q_i = 0.$$

Продифференцировав это тождество и заменив Q_i' выражениями (21), мы получим

$$Q_{n-1}' \exp Q_{n-1} \left(\sum_{i=1}^{n-2} \frac{d_i}{c_i + \exp Q_{n-1}} + \frac{d_{n-1}}{\exp Q_{n-1}} \right) = 0,$$

а так как $Q_{n-1}' \neq 0$ и $\exp Q_{n-1} \neq 0$, то

$$\sum_{i=1}^{n-1} \frac{d_i}{c_i + \exp Q_{n-1}} = 0 \tag{22}$$

(мы здесь считаем $c_{n-1} = 0$).

Равенство (22) может иметь место только в случае, когда рациональная функция

$$\sum_{i=1}^{n-1} \frac{d_i}{c_i + z} \tag{23}$$

тождественно равна нулю. В самом деле, если это не так, т. е. функция (23) равна $\varphi(z)/\psi(z)$, причем $\varphi(z) \neq 0$, то ввиду равенства $\varphi(\exp Q_{n-1}) = 0$ мы получаем, что отличный от константы формальный степенной ряд $\exp Q_{n-1}$ является корнем алгебраиче-

ского уравнения, вопреки утверждению задачи 4 § 1. Очевидно, что функция (23) может обратиться тождественно в нуль только при условии, что $c_k = c_j$ по крайней мере для двух различных индексов k и j. Но тогда из равенств (19) мы найдем, что

$$\exp P_k = \frac{a_k}{a_j} \exp P_j,$$

откуда легко следует равенство $P_k = P_j$. Лемма 2 доказана.

Замечание. Метод Сколема дает возможность доказать конечность числа целых решений уравнения (14). Однако он не дает алгоритма для нахождения самих решений. Причина этого следующая. После того как доказано, что система (7) имеет конечное число целых $\mathfrak{P}$-адических решений, можно легко указать алгоритм для последовательного вычисления коэффициентов в разложении любого из этих решений по степеням простого элемента. Однако не существует алгоритма, который на основании конечного числа коэффициентов давал бы возможность судить, имеем ли мы дело с целым рациональным решением.

Этим недостатком обладает и доказательство, данное самим Туэ.

Бейкеру удалось найти эффективный метод для определения всех решений уравнений (14) (см. [58]). Именно, основываясь на оценках линейных форм от логарифмов алгебраических чисел, Бейкер доказал существование такой эффективно вычислимой константы C, зависящей от коэффициентов формы f, ее степени n и числа c, что для всех целочисленных решений (x, y) уравнения (14) справедливы неравенства

$$|x| < C, \qquad |y| < C.$$

Например, можно положить $C = \exp\left(n^{r^2} A^{r n^3} + (\ln|c|)^{n+2}\right)$, где $r = 32n(n+2)^2$ и A — максимум абсолютной величины коэффициентов формы f.

Метод Бейкера позволяет также явно вычислить константу, которая ограничивает сверху дискриминанты всех одноклассных мнимых квадратичных полей. О решении проблемы десятого дискриминанта было сказано в конце п. 2 § 7.

Заметим в заключение, что Зигель доказал конечность числа целых решений для гораздо более широкого класса уравнений $F(x, y) = 0$, где F — многочлен с целыми коэффициентами, удовлетворяющий очень слабым ограничениям (уравнение $F = 0$ должно определять кривую, которая нерациональна, т. е. не допускает параметризации $x = \varphi(t)$, $y = \psi(t)$, где φ и ψ — рациональные функции от t). При этом теорема Зигеля справедлива и для решений в целых числах фиксированного поля алгебраических чисел (см. [30], гл. VII). К настоящему времени неизвестен,

однако, метод эффективного нахождения всех решений уравнений, которые рассматриваются в теореме Зигеля.

4. Замечания о формах с бо́льшим числом переменных. В связи с теоремой Туэ возникает вопрос: при каком условии уравнение вида (1) с неполной разложимой формой имеет лишь конечное число решений в целых числах? В некоторых случаях такие уравнения могут иметь бесконечное число решений. Примером может служить уравнение

$$x^4 + 4y^4 + 9z^4 - 4x^2y^2 - 6x^2z^2 - 12y^2z^2 = N(x + y\sqrt{2} + z\sqrt{3}) = 1$$

(норма берется в расширении $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$). Это уравнение имеет две бесконечные серии решений, задаваемые формулами:

$$x + y\sqrt{2} = \pm(1 + \sqrt{2})^n, \qquad z = 0;$$
$$x + z\sqrt{3} = \pm(2 + \sqrt{3})^n, \qquad y = 0.$$

Причина этого явления заключается в том, что, полагая $z = 0$ или $y = 0$, мы получаем из нашей формы квадрат полной формы: $(x^2 - 2y^2)^2$ и $(x^2 - 3z^2)^2$ соответственно. Это означает, что модуль $\{1, \sqrt{2}, \sqrt{3}\}$, соответствующий нашей форме, содержит полный подмодуль меньшего поля, а именно:

$$\{1, \sqrt{2}\} \subset \mathbb{Q}(\sqrt{2}) \quad \text{и} \quad \{1, \sqrt{3}\} \subset \mathbb{Q}(\sqrt{3}).$$

Опишем общий тип форм, обладающих аналогичным свойством. Запишем уравнение (1) в виде (3) и рассмотрим линейное подпространство L (над $\mathbb{Q}$), порожденное числами модуля M. Модуль M назовем *вырожденным*, если соответствующее ему пространство L содержит подпространство L', подобное некоторому подполю $k' \subset k$, причем k' не является ни полем рациональных чисел, ни мнимым квадратичным полем.

Покажем, что для вырожденного модуля уравнение (3) имеет бесконечно много решений (во всяком случае, для некоторых a). Действительно, если $L' = \gamma k'$ ($\gamma \in k$) и $M' = L' \cap M$, то $\gamma^{-1}M'$ — полный модуль поля k'. По определению вырожденного модуля для поля k' число основных единиц в любом порядке не равно нулю, поэтому уравнение

$$N_{k'/\mathbb{Q}}(\xi) = a, \quad \xi \in \gamma^{-1}M', \tag{24}$$

имеет бесконечное число решений (если только оно имеет хотя бы одно решение). Положим $a_1 = N_{k/\mathbb{Q}}(\gamma)\, a^r$, где $r = (k : k')$. Так как

$$N_{k/\mathbb{Q}}(\xi\gamma) = \left(N_{k'/\mathbb{Q}}(\xi)\right)^r N_{k/\mathbb{Q}}(\gamma) = a$$

и $\xi\gamma \in M' \subset M$ (для любого ξ, удовлетворяющего уравнению (24)), то уравнение $N_{k/\mathbb{Q}}(\eta) = a_1$, $\eta \in M$, имеет бесконечно много решений.

Основная гипотеза об уравнениях вида (1) заключается в том, что *каждое такое уравнение имеет лишь конечное число решений в целых числах, если только соответствующий ему модуль не является вырожденным.*

В. Шмидт доказал эту гипотезу в общем виде [119]. Его метод, так же как и первоначальный метод Туэ, основан на теории приближений алгебраических чисел рациональными.

Задачи

1. Пусть ряд $f(t) = a_0 + a_1 t + a_2 t^2 + \ldots$ с целыми p-адическими коэффициентами сходится для всех целых p-адических значений t. Доказать, что если

$$\nu_p(a_1) < \nu_p(a_k), \qquad k = 2, 3, \ldots,$$

то уравнение $f(t) = 0$ имеет ровно одно целое p-адическое решение при $\nu_p(a_0) \geqslant \nu_p(a_1)$ и не имеет целых p-адических решений при $\nu_p(a_0) < \nu_p(a_1)$.

2. Пусть $d > 1$ — натуральное число, свободное от кубов, и пусть (a, b) и (a_1, b_1) — два нетривиальных (отличных от (1, 0)) решения уравнения

$$x^3 + dy^3 = 1$$

(в целых рациональных числах). В кубическом поле $K = \mathbb{Q}\left(\sqrt[3]{d}\right)$ положим $\varepsilon = a + b\sqrt[3]{d}$, $\varepsilon_1 = a_1 + b_1\sqrt[3]{d}$. Доказать, что тогда $\varepsilon^u = \varepsilon_1^v$ при некоторых целых рациональных u и v, из которых хотя бы одно не делится на 3.

3. Сохраняя обозначения предшествующей задачи, предположим, что $d \not\equiv \pm 1 \pmod 9$. Тогда в поле K имеет место разложение $3 = \mathfrak{p}^3$ (задача 24 § 7 гл. III), а значит, степень $\mathfrak{p}$-адического пополнения $K_\mathfrak{p}$ поля K над полем 3-адических чисел $\mathbb{Q}_3$ равна 3. Считая, что $v \not\equiv 0 \pmod 3$, положим $t = u/v$. Доказать, что число t (рассматриваемое как целое 3-адическое число) является корнем уравнения

$$\sum_{n=2}^{\infty} a_n t^n = 0. \qquad (*)$$

где $a_n = \frac{1}{n!}\operatorname{Sp}\left((\ln \eta)^n\right)$, $\eta = \varepsilon^3$. (Здесь Sp означает след относительно расширения $K_\mathfrak{p}/\mathbb{Q}_3$.) Доказать, что ряд, стоящий в левой части уравнения $(*)$, сходится при всех целых 3-адических значениях t.

Указание. Доказать, что $\operatorname{Sp}(\ln \eta) = 0$ и $\operatorname{Sp} \eta_1 = 3$, $\eta_1 = \varepsilon_1^3$.

4. Для коэффициентов a_n ряда $(*)$ доказать, что

$$\nu_3(a_2) = \nu_3(a_3) = \mu + 3, \quad \nu_3(a_n) > \mu + 3 \text{ при } n > 3,$$

где $\mu = \nu_3(a^3 b^3 d)$ (ν_3 — 3-адический показатель).

Указание. Воспользоваться тем, что если $\eta = 1 + 3x$, $x = ab\sqrt[3]{d}\,\varepsilon$, то

$$\log \eta \equiv 3x - \frac{9}{2}x^2 + 9x^3 \pmod{3^{4+\mu}},$$

а также тем, что след любого элемента из кольца $\mathbb{Z}_3\left[\sqrt[3]{d}\right]$ делится на 3 ($\mathbb{Z}_3$ — кольцо целых 3-адических чисел).

5. Основываясь на задачах 1—4, доказать, что уравнение $x^3 + dy^3 = 1$ при $d \not\equiv \pm 1 \pmod 9$ имеет не более одного нетривиального решения в целых рациональных числах.

6. Доказать утверждение предшествующей задачи для случая, когда $d \equiv \pm 1 \pmod 9$.

Указание. Принять во внимание, что число 3 в поле $K = \mathbb{Q}\left(\sqrt[3]{d}\right)$ раскладывается в произведение $3 = \mathfrak{p}^2\mathfrak{q}$ (задача 24 § 7 гл. III), и перенести утверждения задач 3 и 4 на прямую сумму $K_3 = K_\mathfrak{p} \oplus K_\mathfrak{q}$ (см. § 2). Логарифмическая функция на K_3 определяется точно так же, как и на поле: ряд будет сходящимся для всех тех $\xi = (\alpha, \beta) \in K_3$, для которых α и β являются главными единицами полей $K_\mathfrak{p}$ и $K_\mathfrak{q}$ соответственно. След $\mathrm{Sp}(\xi)$ определяется как след матрицы линейного преобразования $\xi' \to \xi\xi'$ ($\xi' \in K_3$). и поэтому для элементов из $\widehat{K}$ он совпадает со следом соответствующих чисел из K. (Относительно задач 2—6 см. работу Б. Н. Делоне [44].)

7. Пусть ряд $f(t) = a_0 + a_1 t + a_2 t^2 + \ldots$ с целыми p-адическими коэффициентами сходится при всех целых p-адических значениях t. Доказать, что если a_n является p-адической единицей и $a_s \equiv 0 \pmod p$ при всех $s > n$, то уравнение $f(t) = 0$ имеет не более n целых p-адических решений.

8. Пусть целочисленная последовательность

$$u_0, u_1, \ldots, u_n, \ldots \qquad (**)$$

удовлетворяет рекуррентному соотношению $u_n = a_1 u_{n-1} + \ldots + a_m u_{n-m}$ ($a_m \neq 0$) с целыми рациональными коэффициентами $a_1, \ldots, a_m$. Предположим, что многочлен $\varphi(x) = x^m - a_1 x^{m-1} - \ldots - a_m$ не имеет кратных корней. Доказать, что тогда существует такое натуральное число M, что для всех индексов n из одного и того же фиксированного класса вычетов по модулю M либо все значения u_n совпадают, либо никакое число не встречается среди этих значений бесконечно много раз.

Указание. Воспользоваться формулой $u_n = A_1\alpha_1^n + \ldots + A_m\alpha_m^n$ (α_i — корни $\varphi(x)$) и тем, что при надлежащем простом p и натуральном M функции $\alpha_i^{Mx} = \exp\left(x \ln \alpha_i^M\right)$ будут аналитическими функциями для всех целых p-адических x.

9. В обозначениях предшествующей задачи предположим, что все корни α_i ($1 \leqslant i \leqslant m$) многочлена $\varphi(x)$ и все отношения α_i/α_j ($i \neq j$) не являются корнями из 1. Доказать, что тогда никакое целое число не встречается в рекуррентной последовательности $(**)$ бесконечно много раз (если только она не состоит сплошь из нулей).

10. Пусть $f(y)$ — произвольный степенной ряд, а $g(x)$ — степенной ряд без свободного члена с коэффициентами из некоторого поля. Положим $F(x) = f(g(x))$. Доказать, что

$$F'(x) = f'(g(x))\,g'(x).$$

11. Пусть $P(t) \neq 0$ — формальный степенной ряд без свободного члена над произвольным полем характеристики 0. Доказать, что если $\sum_{i=1}^{n} a_i \exp \gamma_i P(t) = 0$, где не все a_i равны нулю, то $\gamma_k = \gamma_j$ по крайней мере для двух значений индексов $k \neq j$.

12. Доказать утверждение леммы 2 в предположениях $n_1 = n - 1$, $n_2 = 1$ и $n_1 = 1$, $n_2 = n - 1$.

§ 7. Локальные аналитические многообразия

Пусть k — поле характеристики нуль, полное относительно показателя ν, и φ — метрика, соответствующая показателю ν. В этом параграфе под n-мерным пространством k^n мы будем понимать совокупность последовательностей $(\alpha_1, \ldots, \alpha_n)$, называе-

мых точками, компоненты которых принадлежат k или конечным расширениям поля k. Под ε-окрестностью нулевой точки в $\tilde{k}^n$ будет подразумеваться совокупность точек $(\alpha_1, \ldots, \alpha_n)$, удовлетворяющих условиям $\varphi(\alpha_i) < \varepsilon$ $(i = 1, \ldots, n)$ (ε — вещественное положительное число).

Рассмотрим совокупность степенных рядов $f(x_1, \ldots, x_n)$ от n переменных с коэффициентами из k, сходящихся в некоторой ε-окрестности нулевой точки (для каждого ряда своя окрестность). Легко видеть, что все такие ряды образуют кольцо. Обозначим это кольцо через $\mathfrak{O}$. Мы иногда будем писать $f(X)$ вместо $f(x_1, \ldots, x_n)$.

Определение. *Совокупность V точек $(\alpha_1, \ldots, \alpha_n) \in \tilde{k}^n$, принадлежащих некоторой ε-окрестности нуля и удовлетворяющих системе уравнений*

$$f_1(X) = 0, \ \ldots, \ f_m(X) = 0, \tag{1}$$

где $f_1(X), \ldots, f_m(X)$ — степенные ряды из кольца $\mathfrak{O}$ без свободного члена, называется локальным аналитическим многообразием или, короче, *локальным многообразием.*

Два локальных многообразия мы будем считать равными, если они совпадают в некоторой ε-окрестности нуля.

Локальные многообразия можно, конечно, рассматривать в окрестности произвольной точки пространства $\tilde{k}^n$. Нулевая точка нами выбрана для удобства обозначений.

Пусть V — некоторое локальное многообразие. Совокупность всех степенных рядов $f(X) \in \mathfrak{O}$, обращающихся в нуль во всех точках многообразия V, принадлежащих некоторой ε-окрестности нуля, образует, очевидно, идеал кольца $\mathfrak{O}$. Этот идеал в $\mathfrak{O}$ мы будем обозначать через $\mathfrak{A}_V$. Очевидно, что элементы факторкольца $\mathfrak{O}/\mathfrak{A}_V = \overline{\mathfrak{O}}$ можно рассматривать как функции на точках многообразия V, принадлежащих некоторой ε-окрестности нуля (для каждой функции своя окрестность). Ввиду этого факторкольцо $\overline{\mathfrak{O}}$ называется *кольцом аналитических функций на V.*

Определение. *Локальное многообразие V называется неприводимым, если кольцо функций $\mathfrak{O}/\mathfrak{A}_V$ на V не имеет делителей нуля. В противном случае V называется приводимым.*

Исследование локальных многообразий основывается на трех простых фактах, из которых один относится к алгебре, а два другие — к свойствам степенных рядов. Мы приведем их без доказательств, ограничившись ссылками.

Лемма 1. *Для m многочленов $g_1(t), \ldots, g_m(t)$ из кольца $k[t]$, старшие коэффициенты которых равны 1, существует система $h_1, \ldots, h_r$ целочисленных многочленов от их коэффициентов, обладающая тем свойством, что при частных значениях коэффициентов из k условия $h_1 = 0, \ldots, h_r = 0$ необходимы и достаточны*

для того, чтобы многочлены $g_1(t)$, ..., $g_m(t)$ имели общий корень в некотором конечном расширении поля k.

Если $m=2$, то $r=1$ и h_1 является результантом многочленов g_1 и g_2. Общий случай легко сводится к случаю $m=2$. Доказательство содержится в книге [5].

Лемма 2. *Пусть в степенном ряде $f(x_1, \ldots, x_n) \in \mathfrak{O}$ наименьшая степень входящего в него члена равна $k \geqslant 1$ и коэффициент при x_n^k отличен от нуля. Тогда в кольце $\mathfrak{O}$ можно найти степенной ряд $e(x_1, \ldots, x_n)$ с отличным от нуля свободным членом, такой, что*

$$f(X)\,e(X) = x_n^k + \varphi_1(x_1, \ldots, x_{n-1})\,x_n^{k-1} + \ldots + \varphi_k(x_1, \ldots, x_{n-1}),$$

где φ_1, ..., φ_k — степенные ряды от переменных x_1, ..., x_{n-1} с нулевыми свободными членами.

Доказательство этой леммы содержится в книге [11].

Заметим, что условие необращения в нуль коэффициента при x_n^k, выполнение которого предполагается в лемме 2, всегда может быть достигнуто при помощи неособенного линейного преобразования переменных. При этом, как легко видеть, если мы имеем несколько степенных рядов f_1, ..., f_m, то линейное преобразование можно выбрать так, чтобы это условие выполнялось для всех них одновременно.

Лемма 3. *Всякий идеал $\mathfrak{A}$ кольца $\mathfrak{O}$ имеет конечную систему образующих, т. е. в нем существуют такие ряды h_1, ..., h_s, что всякий ряд $h \in \mathfrak{A}$ представляется в виде*

$$h = g_1 h_1 + \ldots + g_s h_s,$$

где g_1, ..., g_s — некоторые ряды из $\mathfrak{O}$.

По поводу доказательства леммы 3 см. книгу [3]. Заметим, что в этой книге и в книге Зигеля речь идет о рядах над полем комплексных чисел, однако приведенные в них доказательства дословно переносятся и на наш случай полного поля с показателем.

Лемма 3 нам нужна для доказательства следующего результата.

Теорема 1. *Каждое локальное многообразие является объединением конечного числа неприводимых локальных многообразий.*

Доказательство. Пусть многообразие V определяется уравнениями (1). Если V приводимо, то в $\mathfrak{O}$ существуют степенные ряды f и g, не обращающиеся в нуль в точках V, сколь угодно близких к нулевой точке, такие, что произведение fg равно нулю во всех точках V из некоторой ε-окрестности нулевой точки. Обозначим через V_1 и V_1' многообразия, определяющие уравнения которых получаются из системы (1) приписыванием уравнений $f(X)=0$ и $g(X)=0$ соответственно. Очевидно, что V_1 и V_1'

являются собственными подмногообразиями V, причем

$$V = V_1 \cup V_1'.$$

Если многообразия V_1 и V_1' неприводимы, то теорема доказана. Если же одно из них приводимо, то мы можем аналогичным образом и его представить в виде объединения двух собственных подмногообразий. Повторяя этот процесс, мы либо придем к представлению многообразия V в виде объединения конечного числа неприводимых многообразий (что нам и нужно), либо получим бесконечную последовательность многообразий

$$V = V_0 \supsetneq V_1 \supsetneq V_2 \supsetneq \dots \tag{2}$$

Докажем, что второй случай невозможен. Рассмотрим для этого идеалы $\mathfrak{A}_{V_i}$ многообразий V_i. Из (2) следует, что

$$\mathfrak{A}_{V_0} \subsetneq \mathfrak{A}_{V_1} \subsetneq \mathfrak{A}_{V_2} \subsetneq \dots \tag{3}$$

Обозначим через $\mathfrak{A}$ объединение идеалов $\mathfrak{A}_{V_i}$. Согласно лемме 3 идеал $\mathfrak{A}$ порождается конечной системой рядов $h_1, \dots, h_s$. Так как каждый ряд из $\mathfrak{A}$ содержится в некотором идеале $\mathfrak{A}_{V_i}$, то существует такое k, что все ряды $h_1, \dots, h_s$ содержатся в $\mathfrak{A}_{V_k}$. Но тогда $\mathfrak{A} \subset \mathfrak{A}_{V_k}$ и, следовательно, $\mathfrak{A}_{V_k} = \mathfrak{A}_{V_{k+1}} = \dots$, а это противоречит включениям (3). Теорема 1, таким образом, доказана.

Мы изложим сейчас общий прием исследования локальных многообразий, основанный на редукции к многообразиям в пространстве меньшего числа измерений.

Пусть многообразие V в пространстве $\tilde{k}^n$ определяется уравнениями (1). Предполагая V отличным от $\tilde{k}^n$, мы можем считать, что ряды $f_1, \dots, f_m$ $(m \geqslant 1)$ не равны тождественно нулю. Допустим, что нами уже сделано такое линейное преобразование переменных, что все многочлены f_i удовлетворяют условиям леммы 2. Тогда по этой лемме в кольце $\mathfrak{O}$ существуют такие степенные ряды $e_1(X), \dots, e_m(X)$ с отличными от нуля свободными членами, что

$$f_i e_i = g_i = x_n^{k_i} + \varphi_{i1} x_n^{k_i - 1} + \dots + \varphi_{ik_i}, \tag{4}$$

где $\varphi_{ij} = \varphi_{ij}(x_1, \dots, x_{n-1})$ — степенные ряды от $n-1$ переменных с нулевыми свободными членами. Так как $e_i(X) \neq 0$ в некоторой ε-окрестности нуля, то многообразие V задается также системой уравнений

$$g_1(X) = 0, \dots, g_m(X) = 0, \tag{5}$$

левые части которых являются многочленами от x_n со старшими коэффициентами, равными 1. К этим многочленам мы можем применить лемму 1. Соответствующие многочлены $h_1, \dots, h_r$ от коэффициентов многочленов $g_1, \dots, g_m$ будут степенными рядами от

$x_1, \ldots, x_{n-1}$ без свободных членов, и так как все Φ_{ij} сходятся в некоторой ε-окрестности нуля, то сходящимися в той же окрестности будут и ряды $h_1, \ldots, h_r$.

Рассмотрим в пространстве $\tilde{k}^{n-1}$ локальное многообразие W, определяемое уравнениями

$$h_1(x_1, \ldots, x_{n-1}) = 0, \ldots, h_r(x_1, \ldots, x_{n-1}) = 0.$$

Очевидно, что точка $(\alpha_1, \ldots, \alpha_{n-1}) \in \tilde{k}^{n-1}$ принадлежит W тогда и только тогда, когда все многочлены $g_i(\alpha_1, \ldots, \alpha_{n-1}, x_n)$ имеют общий корень, т. е. существует такое α_n, что $(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) \in V$. Таким образом, W является проекцией многообразия V на гиперплоскость $x_n = 0$. При этом каждая точка $(\alpha_1, \ldots, \alpha_{n-1}) \in W$ является проекцией конечного числа точек $(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) \in V$, так как α_n определяется как общий корень многочленов $g_i(\alpha_1, \ldots, \alpha_{n-1}, x_n)$. Переход от многообразия V к его проекции W послужит нам основным методом исследования локальных многообразий.

Определение. *Кривой в пространстве $\tilde{k}^n$ называется система n целых формальных степенных рядов $\omega_1(t), \ldots, \omega_n(t)$ без свободных членов с коэффициентами из поля k или некоторого его конечного расширения, причем не все $\omega_i(t)$ тождественно равны нулю.*

Для наших целей нам не будет нужды предполагать ряды $\omega_i(t) = \alpha_{i1}t + \alpha_{i2}t^2 + \ldots$ сходящимися и даже проще будет этого не делать. Таким образом, кривая задается не множеством своих точек, а набором рядов $\omega_i(t)$. В связи с этим принадлежность кривой к локальному многообразию будет пониматься несколько иначе, чем обычно.

Определение. *Мы будем говорить, что кривая $\omega_1(t), \ldots, \omega_n(t)$ принадлежит многообразию V, если для любого ряда $f(x_1, \ldots, x_n)$ из идеала $\mathfrak{A}_V$ степенной ряд $f(\omega_1(t), \ldots, \omega_n(t))$ тождественно равен нулю.*

Основное нужное нам свойство локальных аналитических многообразий состоит в следующем.

Теорема 2. *Всякое локальное многообразие или совпадает с нулевой точкой, или содержит некоторую кривую.*

Доказательство ведется индукцией по размерности n.

По лемме 3 идеал $\mathfrak{A}_V$ имеет конечное число образующих. Можно поэтому считать, что в качестве системы (1), определяющей многообразие V, взята система образующих идеала $\mathfrak{A}_V$. При $n = 1$ многообразие V состоит только из нулевой точки, если хоть один из рядов f_i не равен тождественно нулю, и совпадает с $\tilde{k}^1$, если все f_i тождественно равны нулю. Во втором случае любой ряд $\omega(t)$ удовлетворяет системе (1).

Пусть теперь $n > 1$. Утверждение теоремы очевидно, если все f_i тождественно равны нулю (или если $m = 0$). Можно поэтому считать, что все ряды $f_1, \ldots, f_m$ $(m > 0)$ не равны нулю. Пред-

положим также, что эти ряды удовлетворяют условиям леммы 2, так что вместо уравнений (1) мы можем для задания V взять уравнения (5), где g_i определены равенствами (4). Рассмотрим в пространстве $\tilde{k}^{n-1}$ проекцию W многообразия V. Для W по индуктивному предположению теорема 2 справедлива. Если W совпадает с нулевой точкой, то многообразие V будет определяться системой уравнений

$$g_i(0, \ldots, 0, x_n) = 0, \qquad 1 \leqslant i \leqslant m,$$

т. е. тоже будет совпадать с нулевой точкой. Если же W отлично от нуля, то в W содержится кривая $\omega_1(t), \ldots, \omega_{n-1}(t)$. Обозначим через k_1 конечное расширение поля k, в котором содержатся коэффициенты степенных рядов $\omega_1, \ldots, \omega_{m-1}$. Из определения многообразия W следует, что при подстановке рядов $\omega_1(t), \ldots, \omega_{n-1}(t)$ в ряды $g_1, \ldots, g_m$ вместо $x_1, \ldots, x_{n-1}$ мы получим m многочленов от x_n:

$$g_i(\omega_1(t), \ldots, \omega_{n-1}(t), x_n), \qquad 1 \leqslant i \leqslant m, \tag{6}$$

коэффициенты которых принадлежат полю $k_1\{t\}$ формальных степенных рядов от t над k_1 и которые будут иметь общий корень $x_n = \xi$ в некотором конечном расширении Ω поля $k_1\{t\}$. По теореме 6 § 1 поле Ω содержится в поле формальных степенных рядов $k'\{u\}$, где $u^e = t$ при некотором натуральном e, а k' — конечное расширение над k_1. Элемент ξ можно поэтому представить в виде степенного ряда $\xi = \omega(u)$ с коэффициентами из k'. Так как ξ является корнем многочленов (6), старшие коэффициенты которых равны 1, а все остальные коэффициенты являются целыми элементами поля $k_1\{t\}$, то ряд $\omega(u)$ является целым элементом поля $k'\{u\}$, т. е. он не содержит членов с отрицательными степенями u. Далее, в представлении (4) все ряды φ_{ij} не имеют свободных членов. Подставив в (4) вместо $x_1, \ldots, x_{n-1}$ ряды $\omega_1(u^e), \ldots, \omega_{n-1}(u^e)$, а вместо x_n — ряд $\omega(u)$ и обратив внимание на свободный член полученного ряда, мы получим, во-первых, что свободный член ряда $\omega(u)$ равен нулю и, во-вторых, что

$$g_i(\omega_1(u^e), \ldots, \omega_{n-1}(u^e), \omega(u)) = 0, \qquad 1 \leqslant i \leqslant m.$$

Так как ряды $\omega_1, \ldots, \omega_{n-1}$ не все равны нулю, то набор степенных рядов $\omega_1(u^e), \ldots, \omega_{n-1}(u^e), \omega(u)$ является кривой в $\tilde{k}^n$. По предположению ряды $f_1, \ldots, f_m$, а значит, и ряды $g_1, \ldots, g_m$ порождают идеал $\mathfrak{A}_V$. Следовательно, для любого ряда $f(x_1, \ldots, x_n)$ из $\mathfrak{A}_V$ справедливо равенство

$$f(\omega_1(u^e), \ldots, \omega_{n-1}(u^e), \omega(u)) = 0,$$

а значит, кривая $\omega_1(u^e), \ldots, \omega_{n-1}(u^e), \omega(u)$ принадлежит многообразию V. Теорема 2 доказана.

Теорема 3. *Если V и V' — два локальных многообразия в $\tilde{k}^n$, причем V не содержится в V', то в $\tilde{k}^n$ существует кривая, принадлежащая V и не принадлежащая V'.*

Доказательство. Мы можем предполагать, что многообразие V неприводимо, так как в противном случае V можно заменить одной из его неприводимых компонент.

Пусть многообразие V' определяется уравнениями

$$F_1(X) = 0, \ldots, F_l(X) = 0,$$

где F_j — ряды из кольца $\mathfrak{O}$. Так как $V \not\subset V'$, то хотя бы один из рядов F_j не обращается тождественно в нуль на точках из V (в любой сколь угодно малой окрестности нулевой точки). Обозначим этот ряд через $F(X)$ и докажем, что многообразию V принадлежит такая кривая $\omega_1(t), \ldots, \omega_n(t)$, что

$$F(\omega_1(t), \ldots, \omega_n(t)) \not\equiv 0.$$

Доказательство этого факта мы проведем индукцией по n.

Мы можем, очевидно, считать, что ряд $F(X)$ удовлетворяет условию леммы 2, так что существует ряд $e(X) = e(x_1, \ldots, x_n) \in \mathfrak{O}$ с отличным от нуля свободным членом, для которого

$$e(X)F(X) = G(x_1, \ldots, x_n) = x_n^k + \psi_1 x_n^{k-1} + \ldots + \psi_k, \qquad (7)$$

где $\psi_1, \ldots, \psi_k$ — ряды от $x_1, \ldots, x_{n-1}$.

В случае $V = \tilde{k}^n$ (в частности, при $n = 1$) утверждение теоремы 3 справедливо очевидным образом: достаточно, например, взять $\omega_1(t) = \ldots = \omega_{n-1}(t) = 0$, $\omega_n(t) = t$. Если же $V \neq \tilde{k}^n$, то мы рассмотрим проекцию $W \subset \tilde{k}^{n-1}$ многообразия V (здесь мы предполагаем, что условию леммы 2 наряду с $F(X)$ удовлетворяют и все ряды $f_1, \ldots, f_m$, определяющие многообразие V; это достигается, как мы знаем, линейным преобразованием переменных). Вместе с V многообразие W также неприводимо, так как кольцо функций на нем, т. е. фактор-кольцо $\mathfrak{O}_{n-1}/\mathfrak{A}_W = \overline{\mathfrak{O}}_{n-1}$, является подкольцом кольца функций $\mathfrak{O}/\mathfrak{A}_V = \overline{\mathfrak{O}}$ на V (наряду с $\mathfrak{O}_{n-1} \subset \mathfrak{O}$ мы имеем также включение $\mathfrak{A}_W \subset \mathfrak{A}_V$). Для каждого ряда $f \in \mathfrak{O}$ через $\overline{f}$ условимся обозначать соответствующую функцию из $\overline{\mathfrak{O}}$. Из равенств (4) следует, что

$$\overline{x}_n^{k_i} + \overline{\varphi}_{i1}\overline{x}_n^{k_i-1} + \ldots + \overline{\varphi}_{ik_i} = 0,$$

а значит, функция $\overline{x}_n$ является целым элементом кольца $\overline{\mathfrak{O}}$ относительно подкольца $\overline{\mathfrak{O}}_{n-1}$. Отсюда следует, что функция

$$\overline{G} = \overline{x}_n^k + \overline{\psi}_1 \overline{x}_n^{k-1} + \ldots + \overline{\psi}_k, \quad \overline{\psi}_i \in \overline{\mathfrak{O}}_{n-1},$$

также является целым элементом относительно $\overline{\mathfrak{O}}_{n-1}$.

Выберем равенство

$$\bar{G}^s + \bar{L}_1\bar{G}^{s-1} + \ldots + \bar{L}_s = 0, \qquad L_j \in \mathfrak{O}_{n-1}, \tag{8}$$

с наименьшим возможным s. Ясно, что здесь $\bar{L}_s \not\equiv 0$, так как иначе мы могли бы сократить на $\bar{G}$ и получить равенство с меньшим значением s. Ряд $L_s \in \mathfrak{O}_{n-1}$ не обращается, таким образом, в нуль в точках многообразия W (в любой окрестности). По индуктивному предположению в пространстве $\tilde{k}^{n-1}$ существует кривая $\omega_1(t)$, ..., $\omega_{n-1}(t)$, которая принадлежит многообразию W и для которой $L_s(\omega_1(t), \ldots, \omega_{n-1}(t)) \not\equiv 0$. В доказательстве теоремы 2 мы видели, что тогда в $\tilde{k}^n$ существует кривая вида $\omega_1(u^e)$, ..., $\omega_{n-1}(u^e)$, $\omega(u)$, принадлежащая многообразию V. Проверим, что для этой кривой

$$G(\omega_1(u^e), \ldots, \omega_{n-1}(u^e), \omega(u)) \not\equiv 0$$

и, следовательно, эта кривая не принадлежит многообразию V'. Действительно, если бы ряд, стоящий слева, был тождественно равен нулю, то ввиду (8) мы имели бы равенство

$$L_s(\omega_1(u^e), \ldots. \omega_{n-1}(u^e)) = 0$$

или, после замены u^e на t,

$$L_s(\omega_1(t), \ldots, \omega_{n-1}(t)) = 0,$$

а это не так по выбору кривой $\omega_1(t)$, ..., $\omega_{n-1}(t)$. Теорема 3, таким образом, доказана.

Глава V

АНАЛИТИЧЕСКИЙ МЕТОД

В главе III мы видели, насколько важной характеристикой арифметических свойств поля алгебраических чисел является число h его классов дивизоров. В силу этого для числа h хотелось бы найти явное выражение через какие-то простейшие величины, связанные с данным полем K. Для произвольного поля алгебраических чисел эта задача до сих пор не решена, но для ряда полей, наиболее интересных с точки зрения теории чисел (например, для квадратичных полей и полей деления круга), такие формулы найдены.

Число классов дивизоров является некоторой характеристикой совокупности всех дивизоров поля K. Поскольку все дивизоры выражаются через простые, а число простых дивизоров бесконечно, то в конечном счете число h определяется некоторой бесконечной конструкцией. В этом, по-видимому, и кроется причина того, что при определении h приходится рассматривать бесконечные произведения, ряды и другие аналитические понятия. Аппарат математического анализа применяется для решения многих задач теории чисел. В настоящей главе мы рассмотрим этот метод на примере задачи о числе классов дивизоров.

§ 1. Аналитическая формула для числа классов дивизоров

1. Дзета-функция Дедекинда. Определение числа классов дивизоров h поля алгебраических чисел K основывается на рассмотрении так называемой *дзета-функции Дедекинда* $\zeta_K(s)$, определяемой рядом

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}, \tag{1}$$

где $\mathfrak{a}$ пробегает все целые дивизоры поля K, а $N(\mathfrak{a})$ обозначает норму дивизора $\mathfrak{a}$. Мы докажем, что ряд, стоящий в правой части равенства (1), сходится при $1 < s < \infty$ и представляет собой в этом промежутке непрерывную функцию от вещественного аргумента s. Далее мы получим формулу

$$\lim_{s \to 1+0} (s-1)\,\zeta_K(s) = h\varkappa, \tag{2}$$

где $\varkappa$ — некоторая константа, простым образом зависящая от поля K, которая будет вычислена в процессе доказательства.

Ценность формулы (2) обусловлена тем, что для функции $\zeta_K(s)$ имеется разложение в бесконечное произведение

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}}, \tag{3}$$

распространенное на все простые дивизоры $\mathfrak{p}$ поля K, которое носит название тождества Эйлера. Если для некоторого поля K мы достаточно хорошо знаем его простые дивизоры (точнее, знаем законы разложения простых рациональных чисел в произведение простых дивизоров поля K), то для этого поля формулы (2) и (3) дают возможность получить явное выражение для h. На этом пути законченные формулы для h нами будут получены в последующих параграфах для случая, когда K — квадратичное или круговое поле.

Разобьем ряд (1) на сумму h рядов

$$\zeta_K(s) = \sum_C \left(\sum_{\mathfrak{a} \in C} \frac{1}{N(\mathfrak{a})^s} \right),$$

где $\mathfrak{a}$ пробегает все целые дивизоры из данного класса дивизоров C, а внешнее суммирование ведется по всем h классам C. Для доказательства сходимости ряда (1) нам достаточно, очевидно, показать, что каждый из рядов

$$f_C(s) = \sum_{\mathfrak{a} \in C} \frac{1}{N(\mathfrak{a})^s} \tag{4}$$

сходится при $s > 1$. Далее, если мы докажем, что для каждого класса C существует предел $\lim\limits_{s \to 1+0} (s-1) f_C(s)$ и что этот предел один и тот же для всех классов C, то, обозначая его через $\varkappa$, мы и получим формулу (2).

Преобразуем ряд (4) в ряд, распространенный на некоторые целые числа поля K. Выберем в обратном классе дивизоров C^{-1} целый дивизор $\mathfrak{a}'$. Тогда для любого $\mathfrak{a} \in C$ произведение $\mathfrak{a}\mathfrak{a}'$ будет главным дивизором:

$$\mathfrak{a}\mathfrak{a}' = (\alpha), \qquad \alpha \in K.$$

Ясно, что отображение $\mathfrak{a} \to (\alpha)$, $\mathfrak{a} \in C$, устанавливает (при фиксированном $\mathfrak{a}'$) взаимно однозначное соответствие между целыми дивизорами $\mathfrak{a}$ из класса C и главными дивизорами (α), делящимися на $\mathfrak{a}'$. Принимая во внимание равенство $N(\mathfrak{a})N(\mathfrak{a}') = |N(\alpha)|$, мы получаем, что

$$f_C(s) = N(\mathfrak{a}')^s \sum_{\substack{(\alpha) \\ \alpha \equiv 0 (\mathrm{mod}\, \mathfrak{a}')}} \frac{1}{|N(\alpha)|^s}, \tag{5}$$

где суммирование ведется по всем главным дивизорам поля K,

делящимся на $\mathfrak{a}'$. Так как два главных дивизора (α_1) и (α_2) равны тогда и только тогда, когда числа α_1 и α_2 ассоциированы, то можно считать, что в ряде (5) суммирование ведется по полному набору попарно не ассоциированных целых чисел $\neq 0$ поля K, делящихся на $\mathfrak{a}'$.

Чтобы придать ряду (5) еще более удобную для исследования форму, воспользуемся геометрическим изображением чисел поля K точками в n-мерном вещественном пространстве $\mathbb{R}^n = \mathfrak{L}^{s,t}$ и в логарифмическом пространстве $\mathbb{R}^{s+t}$ (здесь $n = s + 2t$ — степень поля K, см. пп. 1 и 3 § 3 гл. II). Мы определим сейчас в $\mathbb{R}^n$ такой конус X, что среди ассоциированных между собой чисел поля K существует одно и только одно, геометрический образ которого принадлежит X (под конусом здесь понимается тело в $\mathbb{R}^n$, которое вместе с точкой $x \neq 0$ содержит и весь луч ξx, $0 < \xi < \infty$).

В § 3 гл. II (все обозначения которого мы здесь сохраняем) равенством (13) был определен гомоморфизм $x \to l(x)$ мультипликативной группы точек $x \in \mathbb{R}^n$ с ненулевой нормой $N(x)$ в аддитивную группу векторов логарифмического пространства $\mathbb{R}^{s+t}$. Если $\varepsilon_1, \ldots, \varepsilon_r$ — некоторая система основных единиц поля K, то векторы $l(\varepsilon_1), \ldots, l(\varepsilon_r)$, как мы знаем, образуют базис подпространства размерности $r = s + t - 1$, состоящего из тех точек $(\lambda_1, \ldots, \lambda_{s+t}) \in \mathbb{R}^{s+t}$, для которых $\lambda_1 + \ldots + \lambda_{s+t} = 0$. Поскольку вектор

$$l^* = (\underbrace{1, \ldots, 1}_{s}; \underbrace{2, \ldots, 2}_{t})$$

не принадлежит этому подпространству, то система векторов

$$l^*, \ l(\varepsilon_1), \ \ldots, \ l(\varepsilon_r) \tag{6}$$

является базисом $\mathbb{R}^{s+t}$. Всякий вектор $l(x) \in \mathbb{R}^{s+t}$ $(x \in \mathbb{R}^n, N(x) \neq 0)$ можно представить, следовательно, в виде

$$l(x) = \xi l^* + \xi_1 l(\varepsilon_1) + \ldots + \xi_r l(\varepsilon_r), \tag{7}$$

где $\xi, \xi_1, \ldots, \xi_r$ — вещественные числа.

Через m обозначим порядок группы корней из 1, содержащихся в поле K.

Определение. *Фундаментальной областью для поля K называется подмножество X пространства $\mathbb{R}^n$, состоящее из всех тех точек x, которые удовлетворяют следующим трем условиям:*

1° $N(x) \neq 0$;

2° *в разложении* (7) *коэффициенты* ξ_i $(i = 1, \ldots, r)$ *удовлетворяют неравенствам* $0 \leqslant \xi_i < 1$;

3° $0 \leqslant \arg x_1 < 2\pi/m$,

где x_1 — первая компонента точки x.

Заметим, что при $s \geqslant 1$ число m равно 2, поэтому условие 3° в этом случае означает попросту, что $x_1 > 0$.

В следующем пункте мы увидим, что фундаментальная область X является конусом в $\mathbb{R}^n$. Там же будет доказана

Теорема 1. *В каждом классе ассоциированных между собой целых чисел* ($\neq 0$) *поля* K *имеется одно и только одно число, геометрическое изображение которого в пространстве* $\mathbb{R}^n$ *содержится в фундаментальной области* X.

Вернемся к ряду (5). Если через $\mathfrak{M}$ мы обозначим n-мерную решетку в $\mathbb{R}^n$, состоящую из изображений $x(\alpha) \in \mathbb{R}^n$ целых чисел $\alpha \in K$, делящихся на $\mathfrak{a}'$, то ввиду равенства $|N(\alpha)| = |N(x(\alpha))|$ мы можем ряд (5) переписать в виде

$$f_C(s) = N(\mathfrak{a}')^s \sum_{x \in \mathfrak{M} \cap X} \frac{1}{|N(x)|^s}, \tag{8}$$

где суммирование ведется по всем тем точкам $x = x(\alpha)$ решетки $\mathfrak{M}$, которые содержатся в X.

В п. 4 нами будет доказан один общий результат о рядах, в которых суммирование ведется по всем точкам решетки, лежащим в некотором конусе (теорема 3). В применении к нашему случаю этот результат показывает, что ряд (8) сходится при $s > 1$ и

$$\lim_{s \to 1+0} (s-1) \sum_{x \in \mathfrak{M} \cap X} \frac{1}{|N(x)|^s} = \frac{v}{\Delta}, \tag{9}$$

где Δ — объем основного параллелепипеда решетки $\mathfrak{M}$, а v — объем тела T, состоящего из тех точек x фундаментальной области X, для которых $|N(x)| \leqslant 1$.

Ввиду теоремы 2 § 4 гл. II и равенства (3) § 6 гл. II для Δ имеем формулу

$$\Delta = \frac{1}{2^t} N(\mathfrak{a}') \sqrt{|D|}, \tag{10}$$

где D — дискриминант поля K. Что касается объема v тела T, то он будет вычислен нами в п. 3. Именно, мы найдем, что

$$v = 2^s \pi^t \mathrm{R}/m, \tag{11}$$

где R — регулятор поля K. Из (9), (10) и (11) легко получаем теперь, что

$$\lim_{s \to 1+0} (s-1) f_C(s) = \frac{2^{s+t} \pi^t \mathrm{R}}{m \sqrt{|D|}},$$

а так как

$$\zeta_K(s) = \sum_C f_C(s),$$

то этим установлен следующий основной результат этого параграфа.

Теорема 2. *Для поля алгебраических чисел K степени $n = s + 2t$ ряд*

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$$

сходится для всех $s > 1$ и имеет место формула

$$\lim_{s \to 1+0} (s-1)\,\zeta_K(s) = \frac{2^{s+t}\pi^t \mathrm{R}}{m\sqrt{|D|}}\, h.$$

где h — число классов дивизоров, D — дискриминант и R — регулятор поля K, а m — число содержащихся в K корней из 1.

Перейдем теперь к доказательству тех утверждений, которыми мы пользовались при выводе теоремы 2.

2. Фундаментальная область. Считая ξ вещественным положительным, вычислим $l(\xi x) \in \mathfrak{L}^{s,\,t}$, где $x \in \mathbb{R}^n$, $N(x) \neq 0$. В силу равенств (12) § 3 гл. II мы имеем:

$$l_k(\xi x) = \ln \xi + l_k(x) \qquad \text{при } 1 \leqslant k \leqslant s;$$
$$l_{s+j}(\xi x) = 2\ln \xi + l_{s+j}(x) \quad \text{при } 1 \leqslant j \leqslant t.$$

Отсюда следует, что $l(\xi x) = \ln \xi \cdot l^* + l(x)$, а значит, в разложении векторов $l(x)$ и $l(\xi x)$ через базис (6) коэффициенты при $l(\varepsilon_1)$, ..., $l(\varepsilon_r)$ для обоих векторов одинаковы. Так как к тому же $N(\xi x) = \xi^n N(x) \neq 0$ и $\arg(\xi x)_1 = \arg x_1$, то для всякой точки x из фундаментальной области X весь луч ξx также принадлежит X, т. е. область X является конусом в $\mathbb{R}^n$ (тело X не пусто, так как в нем содержится, например, точка $x(1)$, являющаяся изображением числа $1 \in K$).

Лемма 1. *Каждая точка $y \in \mathbb{R}^n$, для которой $N(y) \neq 0$, однозначно представляется в виде*

$$y = x\varkappa(\varepsilon), \tag{12}$$

где x — точка из фундаментальной области X, а ε — единица поля K.

Доказательство. Разложим вектор $l(y)$ по элементам базиса (6):

$$l(y) = \gamma l^* + \gamma_1 l(\varepsilon_1) + \ldots + \gamma_r l(\varepsilon_r),$$

и каждое вещественное γ_j $(j = 1, \ldots, r)$ представим в виде

$$\gamma_j = k_j + \xi_j,$$

где k_j целое рациональное и $0 \leqslant \xi_j < 1$. Полагая $\eta = \varepsilon_1^{k_1} \ldots \varepsilon_n^{k_r}$, рассмотрим точку $z = y\varkappa(\eta^{-1})$. Мы имеем

$$l(z) = l(y) + l(\eta^{-1}) = l(y) - k_1 l(\varepsilon_1) - \ldots - k_r l(\varepsilon_r) =$$
$$= \gamma l^* + \xi_1 l(\varepsilon_1) + \ldots + \xi_r l(\varepsilon_r).$$

Пусть теперь $\arg z_1 = \varphi$. При некотором целом k

$$0 \leqslant \varphi - \frac{2\pi k}{m} < \frac{2\pi}{m}.$$

При изоморфизме $\alpha \to \sigma_1(\alpha)$ $(\alpha \in K)$ корни m-й степени из 1 поля K отображаются на корни m-й степени из 1 поля всех комплексных чисел $\mathbb{C}$. Обозначим через ζ тот корень m-й степени из 1 (он будет первообразным), для которого

$$\sigma_1(\zeta) = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}.$$

Докажем, что точка $x = zx(\zeta^{-k})$ принадлежит фундаментальной области X. В самом деле,

$$l(x) = l(z) + l(\zeta^{-k}) = l(z) = \gamma l^* + \xi_1 l(\varepsilon_1) + \ldots + \xi_r l(\varepsilon_r),$$

причем $0 \leqslant \xi_j < 1$, так что условия 1° и 2° выполнены. Далее, $x_1 = z_1 x(\zeta^{-k})_1 = z_1\sigma_1(\zeta)^{-k}$, поэтому

$$\arg x_1 = \arg z_1 - k\,\frac{2\pi}{m} = \varphi - \frac{2\pi k}{m},$$

откуда $0 \leqslant \arg x_1 < 2\pi/m$. Таким образом, $x \in X$. Замечая теперь, что $x(\alpha)^{-1} = x(\alpha^{-1})$, мы получаем

$$y = zx(\eta) = xx(\zeta^k)x(\eta) = xx(\varepsilon),$$

где $\varepsilon = \zeta^k\eta$. Представление точки y в виде (12), таким образом, получено. Остается доказать единственность такого разложения. Пусть, помимо (12), $y = x'x(\varepsilon')$, где $x' \in X$ и ε' — единица в K. Так как $xx(\varepsilon) = x'x(\varepsilon')$, то

$$l(x) + l(\varepsilon) = l(x') + l(\varepsilon').$$

Векторы $l(\varepsilon)$ и $l(\varepsilon')$ являются целочисленными линейными комбинациями векторов $l(\varepsilon_1)$, ..., $l(\varepsilon_r)$, в то время как коэффициенты при этих векторах в разложениях $l(x)$ и $l(x')$ через базис (6) все неотрицательны и меньше единицы (условие 2° в определении фундаментальной области). В силу этого из последнего равенства следует, что $l(\varepsilon') = l(\varepsilon)$, а значит, $\varepsilon' = \varepsilon\zeta_0$, где ζ_0 — корень m-й степени из 1 (см. п. 4 § 3 гл. II). Равенство $x(\varepsilon') = x(\varepsilon)x(\zeta_0)$ дает нам теперь, что $x = x'x(\zeta_0)$, а значит,

$$x_1 = x_1'\sigma_1(\zeta_0).$$

По условию 3° для точек x и x' фундаментальной области справедливы неравенства

$$0 \leqslant \arg x_1 < 2\pi/m, \qquad 0 \leqslant \arg x_1' < 2\pi/m,$$

поэтому $0 \leqslant |\arg\sigma_1(\zeta_0)| < 2\pi/m$, а так как $\sigma_1(\zeta_0)$ есть корень степени m из 1, то последнее неравенство возможно лишь при условии $\arg\sigma_1(\zeta_0) = 0$. Но в таком случае $\sigma_1(\zeta_0) = 1$ и $\zeta_0 = 1$.

Этим показано, что $\varepsilon' = \varepsilon$ и, следовательно, $x' = x$. Лемма 1 доказана.

Доказательство теоремы 1. Пусть β — произвольное, отличное от нуля целое число из K. По лемме 1 существует разложение $x(\beta) = xx(\varepsilon)$, где $x \in X$, а ε — единица. Число $\alpha = \beta\varepsilon^{-1}$ ассоциировано с β, и его геометрическое изображение $x(\alpha)$ (совпадающее с точкой x) принадлежит области X. Далее, в силу единственности разложения (12) число α условиями $\beta = \alpha\varepsilon$ и $x(\alpha) \in X$ определено однозначно, а это и доказывает теорему 1.

В качестве примера найдем фундаментальную область для квадратичных полей.

Предположим сначала, что K — вещественное квадратичное поле, так что $n = s = 2$, $t = 0$, $r = s + t - 1 = 1$. Мы будем считать, что K является подполем поля всех комплексных чисел $\mathbb{C}$, а также, что в качестве первого изоморфизма σ_1: $K \to \mathbb{C}$ (см. п. 1 § 3 гл. II) взят тождественный изоморфизм. Если ε — основная единица поля K, то $-\varepsilon$, $1/\varepsilon$, $-1/\varepsilon$ будут также основными единицами, поэтому можно предположить, что $\varepsilon > 1$. Если $x = (x_1, x_2) \in \mathbb{R}^2$, $N(x) = x_1x_2 \neq 0$, то $l(x) = (\ln|x_1|, \ln|x_2|)$. Разложение (7) в данном случае имеет вид

$$l(x) = \xi(1, 1) + \xi_1(\ln\varepsilon, -\ln\varepsilon).$$

Фундаментальная область X определяется здесь, очевидно, условиями

$$x_1 > 0, \quad x_2 \neq 0, \quad 0 \leqslant \xi_1 < 1.$$

Легко видеть, что $\ln|x_1| = \ln|x_2| + 2\xi_1\ln\varepsilon$, а значит, $|x_1| = |x_2|\varepsilon^{2\xi_1}$. Условие $0 \leqslant \xi_1 < 1$ можно заменить поэтому следующим:

$$1 \geqslant |x_2|/|x_1| > \varepsilon^{-2}.$$

Фундаментальная область X состоит, таким образом, из точек, заштрихованных на рис. 7 (стороны углов, ближайшие к положительному лучу оси x_1, к X не причисляются).

Пусть теперь K — мнимое квадратичное поле. Так как здесь $s = 0$, $t = 1$, то $r = s + t - 1 = 0$. Фундаментальная область X состоит, следовательно, из тех точек $x = y + iz$, для которых

$$N(x) = y^2 + z^2 \neq 0, \qquad 0 \leqslant \arg x < 2\pi/m$$

(см. рис. 8, $K = \mathbb{Q}(\sqrt{-3})$, $m = 6$).

3. Вычисление объема. Займемся здесь вычислением n-мерного объема тела T, состоящего из тех точек x фундаментальной области X, для которых $|N(x)| \leqslant 1$. Тот факт, что этот объем существует и отличен от нуля, будет получен нами в процессе вычисления. (В случае квадратичного поля, тело T отмечено на рис. 7 и 8 двойной штриховкой.)

Докажем прежде всего, что тело T ограничено. На каждом луче, входящем в состав конуса X, существует одна и только одна точка x, для которой $|N(x)| = 1$. Обозначим через S множество всех этих точек. Ясно, что T состоит из всех отрезков ξx $(0 < \xi \leqslant 1)$, где x пробегает все точки из S.

В разложении (7) произвольной точки $x \in \mathbb{R}^n$ с ненулевой нормой сравним суммы компонент векторов, стоящих слева и

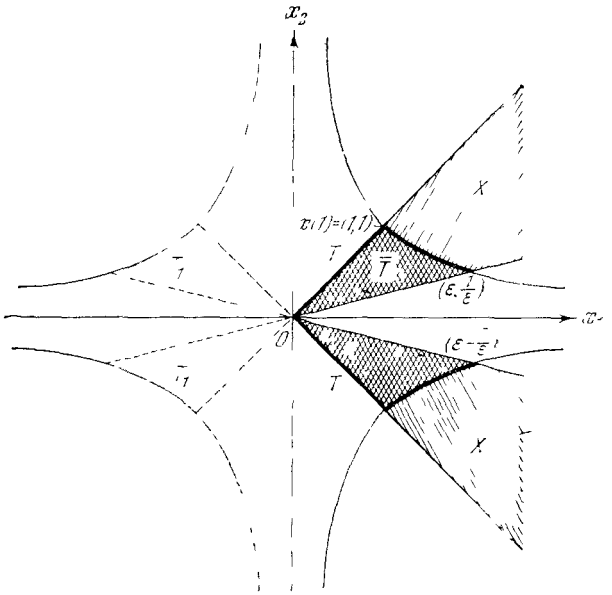

Рис. 7.

справа. В силу формулы (15) § 3 гл. II слева эта сумма равна $\ln|N(x)|$. Справа же ввиду соотношения (18) § 3 гл. II она равна $\xi(s+2t) = n\xi$. Это показывает, что $\xi = \frac{1}{n}\ln|N(x)|$, и разложение (7) мы можем, следовательно, переписать в виде

$$l(x) = \frac{1}{n}\ln|N(x)| \cdot l^* + \xi_1 l(\varepsilon_1) + \ldots + \xi_r l(\varepsilon_r). \qquad (13)$$

Если теперь $x \in S$, то $\ln|N(x)| = 0$, и поэтому точка $l(x) = (l_1(x), \ldots, l_{s+t}(x)) \in \mathbb{R}^{s+t}$ представляется в виде $l(x) = \xi_1 l(\varepsilon_1) + \ldots + \xi_r l(\varepsilon)$, где $0 \leqslant \xi_i < 1$. Отсюда следует, что существует такая константа ρ, что $l_j(x) < \rho$, а тогда $|x_k| < e^{\rho}$ при $1 \leqslant k \leqslant s$ и $|x_{s+j}| < e^{\rho/2}$ при $1 \leqslant j \leqslant t$ для всех $x \in S$ (см. обозначения (13) и (12) § 3 гл. II). Этим доказано, что множество S, а значит, и тело T ограничены.

Вместо тела T мы рассмотрим другое тело, простым образом связанное с T и обладающее тем преимуществом, что оно определяется более простыми условиями, а это облегчит нам наши исследования. Сформулируем предварительно следующую почти очевидную лемму.

Лемма 2. *Если* ε *есть единица поля* K, *то при линейном преобразовании* $x \to x\varepsilon$ *пространства* $\mathbb{R}^n$ *объемы тел не меняются.*

Действительно, при любом неособенном линейном преобразовании евклидова пространства объем тела умножается на абсолютную величину определителя матрицы этого линейного преобразования (см. формулу (2) § 4 гл. II). Согласно доказанному в п. 1 § 3 гл. II определитель преобразования $x \to x\varepsilon$ равен $N(x(\varepsilon))$, т. е. равен $N(\varepsilon) = \pm 1$.

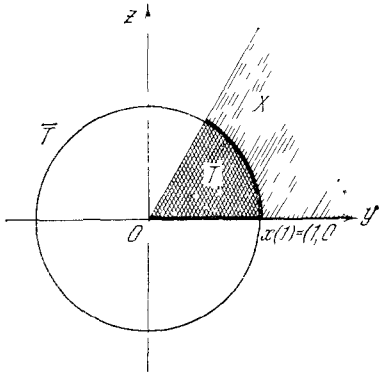

Рис. 8.

Обозначим теперь, как и ранее, через ζ тот корень степени m из 1, для которого $\sigma_1(\zeta) = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}$. Рассмотрим множества T_k ($k = 0, 1, \ldots, m-1$), получающиеся из T линейным преобразованием $x \to x\varepsilon(\zeta^k)$ ($T_0 = T$). По лемме 2 имеем $v(T_k) = v(T)$ (если только хоть один из этих объемов существует). Так как

$$|N(x\varepsilon(\zeta^k))| = |N(x)\,N(\zeta^k)| = |N(x)|,$$
$$l(x\varepsilon(\zeta^k)) = l(x) + l(\zeta^k) = l(x),$$
$$\arg(x\varepsilon(\zeta^k))_1 = \arg x_1 + \frac{2\pi}{m}k,$$

то (см. определение фундаментальной области X, п. 1) тело T_k состоит из тех точек $x \in \mathbb{R}^n$, для которых:

1) $0 < |N(x)| \leqslant 1$;

2) в разложении (13) коэффициенты ξ_i удовлетворяют неравенствам $0 \leqslant \xi_i < 1$;

3) $\frac{2\pi k}{m} \leqslant \arg x_1 < \frac{2\pi}{m}(k+1)$.

Отсюда следует, что $T_0, T_1, \ldots, T_{m-1}$ попарно не пересекаются и что их объединение $\bigcup_{k=0}^{m-1} T_k$ определяется условиями 1) и 2) (без условия 3)).

Обозначим через $\overline{T}$ множество тех точек $x \in \bigcup_{k=0}^{m-1} T_k$, для которых $x_1 > 0, \ldots, x_s > 0$ (см. (2) § 3 гл. II). Зафиксируем произвольно s знаков $\delta_1, \ldots, \delta_s$ ($\delta_i = \pm 1$). Умножение точек из $\mathbb{R}^n$ на точку $(\delta_1, \ldots, \delta_s; 1, \ldots, 1) \in \mathfrak{L}^{s,t} = \mathbb{R}^n$ является линейным преобразованием $\mathbb{R}^n$, не меняющим объема тел (так как норма этой точки равна ± 1). Подвергая множество $\overline{T}$ всем таким линейным преобразованиям, мы получим 2^s попарно не пересекающихся множеств, объединение которых совпадает с $\bigcup_{k=0}^{m-1} T_k$. Если мы докажем, что $\overline{T}$ имеет отличный от нуля объем $\overline{v}$, то отсюда, очевидно, будет следовать существование объема и для T, причем будет иметь место формула

$$v(T) = \frac{2^s}{m}\,\overline{v}. \tag{14}$$

(Для вещественного квадратичного поля $\overline{T}$ является частью T, расположенной в первой четверти, а для мнимого квадратичного поля $\overline{T}$ совпадает с единичным кругом без центра, см. рис. 7 и 8.)

Векторное равенство (13) равносильно следующей системе равенств:

$$l_j(x) = \frac{e_j}{n} \ln |N(x)| + \sum_{k=1}^{r} \xi_k l_j(\varepsilon_k), \qquad j = 1, \ldots, s+t,$$

где $e_j = 1$, если $1 \leqslant j \leqslant s$, и $e_j = 2$, если $s+1 \leqslant j \leqslant s+t$. Сделаем замену переменных по формулам

$$x_k = \rho_k, \qquad k = 1, \ldots, s,$$
$$y_j = \rho_{s+j} \cos \varphi_j, \qquad z_j = \rho_{s+j} \sin \varphi_j, \qquad j = 1, \ldots, t.$$

(В соответствии с обозначениями п. 1 § 3 гл. II вещественные y_j и z_j определяются равенствами $x_{s+j} = y_j + iz_j$, $1 \leqslant j \leqslant t$.) Якобиан этого преобразования, как легко подсчитать, равен $\rho_{s+1} \ldots \rho_{s+t}$. Так как $l_j(x) = \ln \rho_j^{e_j}$ и $N(x) = \prod_{j=1}^{s+t} \rho_j^{e_j}$ (мы считаем $x_1 > 0, \ldots, x_s > 0$), то в новых переменных $\rho_1, \ldots, \rho_{s+t}, \varphi_1, \ldots, \varphi_t$ тело $\overline{T}$ определяется условиями:

1) $$\rho_1 > 0, \quad \ldots, \quad \rho_{s+t} > 0, \qquad \prod_{j=1}^{s+t} \rho_j^{e_j} \leqslant 1;$$

2) в равенствах

$$\ln \rho_j^{e_j} = \frac{e_j}{n} \ln \left(\prod_{i=1}^{s+t} \rho_i^{e_i} \right) + \sum_{k=1}^{r} \xi_k l_j(\varepsilon_k)$$

$(j=1, \ldots, s+t)$ коэффициенты ξ_k удовлетворяют неравенствам $0 \leqslant \xi_k < 1$ $(k=1, \ldots, r)$.

Поскольку эти условия на переменные $\varphi_1, \ldots, \varphi_t$ не накладывают ограничений, то каждая из них (независимо от других) пробегает все значения из промежутка $[0, 2\pi)$. Вместо $\rho_1, \ldots, \rho_{s+t}$ введем теперь новые переменные $\xi, \xi_1, \ldots, \xi_r$ по формулам

$$\ln \rho_j^{e_j} = \frac{e_j}{n} \ln \xi + \sum_{k=1}^{r} \xi_k l_j(\varepsilon_k), \quad j = 1, \ldots, s+t. \tag{15}$$

Складывая все эти равенства и замечая, что

$$\sum_{j=1}^{s+t} e_j = n, \quad \sum_{j=1}^{s+t} l_j(\varepsilon_k) = 0, \tag{16}$$

получим

$$\xi = \prod_{j=1}^{s+t} \rho_j^{e_j}. \tag{17}$$

Тело $\overline{T}$ определяется теперь условиями

$$0 < \xi \leqslant 1, \qquad 0 \leqslant \xi_k < 1, \qquad k = 1, \ldots, r.$$

Существование объема $\bar{v} = v(\overline{T})$ стало теперь очевидным. Так как

$$\frac{\partial \rho_j}{\partial \xi} = \frac{\rho_j}{n\xi}, \quad \frac{\partial \rho_j}{\partial \xi_k} = \frac{\rho_j}{e_j} l_j(\varepsilon_k),$$

то якобиан преобразования (15) равен

$$J = \begin{vmatrix} \frac{\rho_1}{n\xi} & \frac{\rho_1}{e_1} l_1(\varepsilon_1) & \ldots & \frac{\rho_1}{e_1} l_1(\varepsilon_r) \\ \cdots & \cdots & \cdots & \cdots \\ \frac{\rho_{s+t}}{n\xi} & \frac{\rho_{s+t}}{e_{s+t}} l_{s+t}(\varepsilon_1) & \ldots & \frac{\rho_{s+t}}{e_{s+t}} l_{s+t}(\varepsilon_r) \end{vmatrix} =$$

$$= \frac{\rho_1 \cdots \rho_{s+t}}{n\xi 2^t} \begin{vmatrix} e_1 & l_1(\varepsilon_1) & \ldots & l_1(\varepsilon_r) \\ \cdots & \cdots & \cdots & \cdots \\ e_{s+t} & l_{s+t}(\varepsilon_1) & \ldots & l_{s+t}(\varepsilon_r) \end{vmatrix}.$$

Сложим в последнем определителе все строчки с первой. Учитывая (16) и (17) и вспоминая определение регулятора R поля K (см. гл. II, § 4, п. 4), получаем $|J| = \dfrac{R}{2^t \rho_{s+1} \cdots \rho_{s+t}}$. Теперь уже легко находим объем $\bar{v}$:

$$\bar{v} = \int\limits_{(\overline{T})} \ldots \int dx_1 \ldots dx_s dy_1 dz_1 \ldots dy_t dz_t =$$

$$= \int\limits_{(\overline{T})} \ldots \int \rho_{s+1} \ldots \rho_{s+t} d\rho_1 \ldots d\rho_{s+t} d\varphi_1 \ldots d\varphi_t =$$

$$= \int_0^{2\pi} d\varphi_1 \dots \int_0^{2\pi} d\varphi_t \int \dots \int \rho_{s+1} \dots \rho_{s+t} d\rho_1 \dots d\rho_{s+t} =$$

$$= 2^t \pi^t \int \dots \int |J| \rho_{s+1} \dots \rho_{s+t} d\xi d\xi_1 \dots d\xi_r =$$

$$= \pi^t \mathrm{R} \int_0^1 d\xi \int_0^1 d\xi_1 \dots \int_0^1 d\xi_r = \pi^t \mathrm{R}.$$

Подставляя найденное значение $\bar{v}$ в (14), получаем окончательно:

$$v(T) = 2^s \pi^t \mathrm{R}/m.$$

4. **Принцип Дирихле.** Рассмотрим сначала функцию $\zeta_K(s)$ для случая, когда K есть поле рациональных чисел $\mathbb{Q}$. Так как в поле $\mathbb{Q}$ целые дивизоры могут быть отождествлены с натуральными числами n и при этом $N(n) = n$, то

$$\zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{18}$$

Таким образом, для поля рациональных чисел ζ-функция Дедекинда совпадает с ζ-функцией Римана $\zeta(s)$. Докажем, что при $s > 1$ ряд (18) сходится. Так как функция $1/x^s$ при возрастании $x > 0$ убывает, то

$$\int_n^{n+1} \frac{dx}{x^s} < \frac{1}{n^s} < \int_{n-1}^{n} \frac{dx}{x^s},$$

при этом левое неравенство имеет место при $n \geqslant 1$, а правое — при $n \geqslant 2$. Для натурального $N > 1$ мы получаем, следовательно, что

$$\int_1^{N+1} \frac{dx}{x^s} < \sum_{n=1}^{N} \frac{1}{n^s} < 1 + \int_1^{N} \frac{dx}{x^s}.$$

Так как при $s > 1$ интеграл $\int_1^{\infty} \frac{dx}{x^s}$ сходится, то правое неравенство и доказывает сходимость ряда (18). Далее, для $s > 1$ мы имеем

$$\int_1^{\infty} \frac{dx}{x^s} < \zeta(s) < 1 + \int_1^{\infty} \frac{dx}{x^s},$$

или

$$\frac{1}{s-1} < \zeta(s) < 1 + \frac{1}{s-1}.$$

Умножая эти неравенства на $s-1$ и устремляя s к единице, приходим к важному соотношению:

$$\lim_{s\to 1+0}(s-1)\zeta(s)=1, \tag{19}$$

дающему представление о порядке роста функции $\zeta(s)$ при $s\to 1$.

Перейдем теперь к доказательству одной общей аналитико-геометрической теоремы о рядах, принадлежащей Дирихле.

Пусть в пространстве $\mathbb{R}^n$ задан конус X, на котором определена вещественная положительная функция $F(x)$, $x\in X$. (Мы считаем, что точка $(0, \ldots, 0)$ не принадлежит конусу X.) На функцию F и на конус X накладываются следующие условия:

1) для любой точки $x\in X$ и любого вещественного $\xi>0$ справедливо равенство $F(\xi x)=\xi^n F(x)$;

2) тело T, состоящее из тех точек $x\in X$, для которых $F(x)\leqslant 1$, ограничено и имеет отличный от нуля n-мерный объем $v=v(T)$.

Точки конуса, в которых $F(x)=1$, образуют поверхность, пересекающую каждый луч конуса только в одной точке и отсекающую от конуса ограниченное тело с отличным от нуля объемом. Ясно, что задание такой поверхности в X равносильно определению функции $F(x)$.

Предположим, что в $\mathbb{R}^n$ задана n-мерная решетка $\mathfrak{M}$ с объемом основного параллелепипеда Δ. Рассмотрим ряд

$$\widetilde{\zeta}(s)=\sum_{x\in\mathfrak{M}\cap X}\frac{1}{F(x)^s}, \qquad s>1, \tag{20}$$

распространенный на все точки x решетки $\mathfrak{M}$, содержащиеся в конусе X. Этот ряд зависит, таким образом, от конуса X, функции F и решетки $\mathfrak{M}$.

Теорема 3. *При соблюдении только что сделанных обозначений и предположений ряд* (20) *сходится при всех* $s>1$ *и*

$$\lim_{s\to 1+0}(s-1)\widetilde{\zeta}(s)=v/\Delta. \tag{21}$$

Доказательство. Для каждого вещественного $r>0$ через $\mathfrak{M}_r$ обозначим решетку, получающуюся из $\mathfrak{M}$ сжатием в r раз. Объем основного параллелепипеда решетки $\mathfrak{M}_r$ равен, очевидно, $\frac{\Delta}{r^n}$. Если $N(r)$ есть число точек решетки $\mathfrak{M}_r$, содержащихся в теле T, то по определению объема имеем

$$v=v(T)=\lim_{r\to\infty}N(r)\frac{\Delta}{r^n}=\Delta\lim_{r\to\infty}\frac{N(r)}{r^n}. \tag{22}$$

Рассмотрим тело rT, получающееся из T расширением в r раз. Ясно, что $N(r)$ равно также числу точек решетки $\mathfrak{M}$, содержащихся в rT, а это в свою очередь равно числу точек $x\in\mathfrak{M}\cap X$,

для которых $F(x) \leqslant r^n$. Все точки из $\mathfrak{M} \cap X$ расположим в виде последовательности $\{x_k\}$ так, чтобы

$$0 < F(x_1) \leqslant F(x_2) \leqslant \ldots \leqslant F(x_k) \leqslant \ldots$$

Положим $\sqrt[n]{F(x_k)} = r_k$. Точки $x_1, \ldots, x_k$ принадлежат телу $r_k T$, поэтому $N(r_k) \geqslant k$. В то же время при любом $\varepsilon > 0$ точка x_k не принадлежит телу $(r_k - \varepsilon)T$, следовательно, $N(r_k - \varepsilon) < k$. Таким образом,

$$N(r_k - \varepsilon) < k \leqslant N(r_k),$$

откуда $\dfrac{N(r_k-\varepsilon)}{(r_k-\varepsilon)^n}\left(\dfrac{r_k-\varepsilon}{r_k}\right)^n < \dfrac{k}{r_k^n} \leqslant \dfrac{N(r_k)}{r_k^n}$. Переходя здесь к пределу при $k \to \infty$, т. е. при $r_k \to \infty$, и принимая во внимание (22), получим

$$\lim_{k\to\infty} \frac{k}{F(x_k)} = \frac{v}{\Delta}. \tag{23}$$

Сравним ряд $\widetilde{\zeta}(s) = \sum\limits_{k=1}^{\infty} \dfrac{1}{F(x_k)^s}$ с рядом (18). Так как $\lim\limits_{k\to\infty} \dfrac{k^s}{F(x_k)^s} = (v/\Delta)^s \neq 0$, то вместе с рядом (18) ряд (20) также сходится (если, конечно, $s > 1$). Пусть ε — сколь угодно малое вещественное положительное число. В силу (23) имеем

$$\left(\frac{v}{\Delta} - \varepsilon\right)\frac{1}{k} < \frac{1}{F(x_k)} < \left(\frac{v}{\Delta} + \varepsilon\right)\frac{1}{k}$$

для всех достаточно больших $k \geqslant k_0$, откуда

$$\left(\frac{v}{\Delta} - \varepsilon\right)^s \sum_{k=k_0}^{\infty} \frac{1}{k^s} < \sum_{k=k_0}^{\infty} \frac{1}{F(x_k)^s} < \left(\frac{v}{\Delta} + \varepsilon\right)^s \sum_{k=k_0}^{\infty} \frac{1}{k^s}$$

при всех $s > 1$. Умножим это неравенство на $s - 1$ и устремим s к единице справа. Так как $\lim\limits_{s\to 1}(s-1)\sum\limits_{k=1}^{k_0-1}\dfrac{1}{k^s} = 0$, то в силу (19) $\lim\limits_{s\to 1+0}(s-1)\sum\limits_{k=k_0}^{\infty}\dfrac{1}{k^s} = 1$. Учитывая, с другой стороны, что $\lim\limits_{s\to 1}(s-1)\sum\limits_{k=1}^{k_0-1}\dfrac{1}{F(x_k)^s} = 0$, мы приходим к неравенствам

$$\frac{v}{\Delta} - \varepsilon \leqslant \varliminf_{s\to 1+0} (s-1)\widetilde{\zeta}(s) \leqslant \varlimsup_{s\to 1+0} (s-1)\widetilde{\zeta}(s) \leqslant \frac{v}{\Delta} + \varepsilon,$$

которые ввиду произвольности ε и доказывают теорему 3.

Замечание. В равенствах (21) и (22) легко подмечаются некоторые общие черты. Чтобы сходство между этими равенствами сделать более отчетливым, предположим, что объем Δ основного параллелепипеда решетки $\mathfrak{M}$ равен 1, и перепишем их в виде

$$\lim_{s\to 1+0}(s-1)\,\widetilde{\zeta}(s)=v, \tag{21'}$$

$$\lim_{r\to\infty}\frac{1}{r^n}N(r)=v. \tag{22'}$$

Оба предела дают нам одно и то же число — объем тела T. Определение объема равенством (22′) включает в себя следующие операции. Решетка $\mathfrak{M}$ сжимается в r раз, и подсчитывается число $N(r)$ точек сжатой решетки $\mathfrak{M}_r$, содержащихся в T. Затем число $N(r)$ умножается на объем $\frac{1}{r^n}$ основного параллелепипеда решетки $\mathfrak{M}_r$, и, наконец, находится предел произведения $\frac{1}{r^n}N(r)$ при $r\to\infty$. По такой же схеме мы приходим к объему и в равенстве (21′). Здесь сумма $\widetilde{\zeta}(s)$ играет роль числа $N(r)$, множитель $(s-1)$ соответствует множителю $\frac{1}{r^n}$ и предельный переход $s\to 1+0$ — предельному переходу $r\to\infty$.

Вернемся к фундаментальной области X поля алгебраических чисел K. Так как функция $F(x)=|N(x)|$ удовлетворяет условиям 1) и 2), то к ряду (8) можно применить теорему 3, а значит, этот ряд сходится при $s>1$ и для него справедливо соотношение (9).

Этим мы закончили доказательство всех тех утверждений, которыми пользовались в п. 1, и тем самым завершили доказательство теоремы 2.

5. Тождество Эйлера. Чтобы формулу (2) можно было использовать для вычисления числа классов дивизоров h, надо иметь возможность вычислить предел $\lim\limits_{s\to 1+0}(s-1)\,\zeta_K(s)$ другим способом. В некоторых случаях это удается сделать, если воспользоваться представлением $\zeta_K(s)$ в виде некоторого бесконечного произведения, известным под названием тождества Эйлера.

Теорема 4. *При $s>1$ функция $\zeta_K(s)$ может быть представлена в виде сходящегося бесконечного произведения*

$$\zeta_K(s)=\prod_{\mathfrak{p}}\frac{1}{1-\frac{1}{N(\mathfrak{p})^s}},$$

где $\mathfrak{p}$ пробегает все простые дивизоры поля K.

Доказательство. Для каждого простого дивизора $\mathfrak{p}$ имеем

$$\frac{1}{1-\frac{1}{N(\mathfrak{p})^s}} = 1 + \frac{1}{N(\mathfrak{p})^s} + \frac{1}{N(\mathfrak{p})^{2s}} + \dots \qquad (24)$$

Пусть N — произвольное натуральное число и $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ — все простые дивизоры, норма которых не превосходит N. Перемножая абсолютно сходящиеся ряды (24) для $\mathfrak{p} = \mathfrak{p}_1, \dots, \mathfrak{p}_r$, получим

$$\prod_{N(\mathfrak{p}) \leqslant N} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = \sum_{k_1, \dots, k_r = 0}^{\infty} \frac{1}{N\left(\mathfrak{p}_1^{k_1} \dots \mathfrak{p}_r^{k_r}\right)^s} = \sum_{\mathfrak{a}}{}' \frac{1}{N(\mathfrak{a})^s},$$

где $\mathfrak{a}$ в сумме $\sum'$ пробегает все те целые дивизоры поля K, разложение которых в произведение степеней простых дивизоров содержит лишь простые дивизоры с нормой, не превосходящей N. Сравним ряд $\sum'$ с рядом $\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$. Поскольку в ряде $\sum$ встретятся все те целые дивизоры, норма которых $\leqslant N$, то

$$\left| \prod_{N(\mathfrak{p}) \leqslant N} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} - \zeta_K(s) \right| < \sum_{N(\mathfrak{a}) > N} \frac{1}{N(\mathfrak{a})^s}.$$

Так как при $s > 1$ ряд (1) сходится, то

$$\sum_{N(\mathfrak{a}) > N} \frac{1}{N(\mathfrak{a})^s} \to 0$$

при $N \to \infty$, а это и доказывает теорему.

Значение теоремы 4 состоит в том, что она в соединении с теоремой 2 устанавливает связь между числом h и простыми дивизорами поля K. Как уже отмечалось в п. 1, если все простые дивизоры поля K нам известны, то, пользуясь теоремой 4, левую часть соотношения (2) можно будет вычислить другим способом, а это даст нам законченную формулу для h. С другой стороны, тот факт, что $\varkappa h \neq 0$, позволяет сделать важные выводы о простых дивизорах поля K. Например, взяв в качестве K круговое поле, мы придем в § 3 настоящей главы к теореме Дирихле о распределении простых рациональных чисел в арифметических прогрессиях.

Задачи

1. Используя сходимость ряда $\sum_{n=1}^{\infty} \frac{1}{n^s}$ $(s > 1)$, доказать, что при $s > 1$ ряд $\sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s}$, где $\mathfrak{p}$ пробегает все простые дивизоры поля K, также сходится.

2. Пользуясь результатом задачи 1, доказать сходимость произведения $\prod_{\mathfrak{p}} \frac{1}{1-\frac{1}{N(\mathfrak{p})^s}}$, $s>1$. Вывести отсюда сходимость ряда $\sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$.

3. Пусть a_k и b_k $(k \geqslant 1)$ — вещественные положительные числа, причем $\lim\limits_{k\to\infty} \frac{b_k}{a_k} = c$. Доказать, что если ряд $\sum\limits_{k=1}^{\infty} a_k^s$ сходится при $s>1$ и

$$\lim_{s\to 1+0} (s-1) \sum_{k=1}^{\infty} a_k^s = A,$$

то ряд $\sum\limits_{k=1}^{\infty} b_k^s$ также сходится (при $s>1$) и

$$\lim_{s\to 1+0} (s-1) \sum_{k=1}^{\infty} b_k^s = cA.$$

4. Пусть C — произвольный класс дивизоров поля алгебраических чисел K. Обозначим через $Z(\xi, C)$ число целых дивизоров $\mathfrak{a}$ из класса C, для которых $N(\mathfrak{a}) \leqslant \xi$. Доказать, что

$$\lim_{\xi\to\infty} \frac{Z(\xi, C)}{\xi} = \varkappa = \frac{2^{s+t}\pi^t R}{m\sqrt{|D|}}.$$

5. Пусть $\psi(a)$ обозначает число целых дивизоров поля алгебраических чисел K с нормой a. Доказать, что

$$\frac{\zeta_K(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{c_n}{n^s},$$

где $c_n = \sum\limits_{d|n} \mu(d)\psi\left(\frac{n}{d}\right)$ ($\mu(a)$ — функция Мёбиуса).

§ 2. Число классов дивизоров кругового поля

Пусть m — натуральное число и ζ — первообразный корень степени m из 1. Так как все корни m-й степени из 1 изображаются на комплексной плоскости точками, которые делят единичную окружность на m равных частей, то поле $\mathbb{Q}(\zeta)$ принято называть полем деления окружности на m частей или, короче, *m-круговым полем*. В этом параграфе, пользуясь теоремами 2 и 4 § 1, мы найдем формулу для числа h классов дивизоров произвольных круговых полей. Для этой цели мы должны будем предварительно выяснить, каким образом в этих полях простые рациональные числа раскладываются в произведение простых дивизоров. Мы начнем с определения степени поля $\mathbb{Q}(\zeta)$.

1. Неприводимость кругового многочлена. Степень поля $\mathbb{Q}(\zeta)$ равна, как известно, степени минимального многочлена числа ζ над полем рациональных чисел $\mathbb{Q}$. В этом пункте мы докажем,

что минимальным многочленом числа ζ является многочлен

$$\Phi_m = \Phi_m(t) = \prod_{(k,m)=1} (t - \zeta^k)$$

(произведение распространено на приведенную систему вычетов по модулю m), корнями которого являются все первообразные корни m-й степени из 1. Так как степень Φ_m равна значению функции Эйлера $\varphi(m)$, то отсюда будет следовать равенство $(\mathbb{Q}(\zeta) : \mathbb{Q}) = \varphi(m)$.

Многочлен $\Phi_m(t)$ называется многочленом деления окружности на m частей или *m-круговым многочленом*.

Докажем прежде всего, что Φ_m имеет целые рациональные коэффициенты. Для $m = 1$ это очевидно ($\Phi_1 = t - 1$). Доказательство в общем случае проведем индукцией по m. Так как каждый корень m-й степени из 1 является первообразным корнем некоторой степени $d \mid m$, то

$$t^m - 1 = \prod_d \Phi_d,$$

где d пробегает все делители числа m. По индуктивному предположению многочлен $F = \prod_{d \neq m} \Phi_d$ имеет целые рациональные коэффициенты, и к тому же его старший коэффициент равен 1. В силу этого $\Phi_m = (t^m - 1)/F$ также имеет целые рациональные коэффициенты.

Обозначим, как всегда, через $\mathbb{Z}$ кольцо целых рациональных чисел, через $\mathbb{F}_p$ — поле вычетов по простому модулю p и для каждого $a \in \mathbb{Z}$ через $\bar{a}$ — соответствующий класс вычетов из $\mathbb{F}_p$. Если в многочлене $f(t)$ с целыми рациональными коэффициентами мы заменим все коэффициенты их классами вычетов по модулю p, то получим многочлен $\bar{f}(t)$ с коэффициентами из поля $\mathbb{F}_p$. Очевидно, что отображение $f \to \bar{f}$ является гомоморфизмом кольца $\mathbb{Z}[t]$ на кольцо $\mathbb{F}_p[t]$. Так как $(\bar{f} + \bar{g})^p = \bar{f}^p + \bar{g}^p$ и по малой теореме Ферма $\bar{a}^p = \bar{a}$ ($a \in \mathbb{Z}$), то в кольце $\mathbb{F}_p[t]$ справедлива формула

$$(\bar{f}(t))^p = \bar{f}(t^p). \tag{1}$$

Положим $h = t^m - 1$. Если простое число p не входит в m, то многочлен $\bar{h}$ из $\mathbb{F}_p[t]$ взаимно прост со своей производной, и, следовательно, он не имеет кратных множителей. Замечая теперь, что $\bar{\Phi}_m$ является делителем $\bar{h}$, мы приходим к следующему утверждению.

Лемма 1. *Если простое рациональное число p взаимно просто с m, то многочлен $\bar{\Phi}_m$ из кольца $\mathbb{F}_p[t]$ не имеет кратных множителей.*

Если $f(t)$ есть минимальный многочлен числа ζ, то $\Phi_m = fG$, где G, так же как и f, принадлежит кольцу $\mathbb{Z}[t]$. Для любого простого числа p, взаимно простого с m, степень ζ^p также явля-

ется первообразным корнем m-й степени из 1, т. е. $\Phi_m(\zeta^p)=0$. Докажем, что ζ^p — корень f. Если это не так, то $G(\zeta^p)=0$. Рассмотрим тогда многочлен $H(t)=G(t^p)$. Поскольку $H(\zeta)=G(\zeta^p)=0$, то H делится на f, т. е. $H=fQ$, где $Q\in\mathbb{Z}[t]$. Перейдем в равенстве $H=fQ$ к полю вычетов $\mathbb{F}_p$. Мы получим $\bar{H}=\bar{f}\bar{Q}$. Но в силу свойства (1) $\bar{H}(t)=\bar{G}(t^p)=(\bar{G}(t))^p$, поэтому

$$\bar{G}^p=\bar{f}\bar{Q}.$$

Пусть $\bar{\psi}$ — какой-нибудь неприводимый множитель многочлена $\bar{f}$ (в кольце $\mathbb{F}_p[t]$). Из последнего равенства вытекает, что $\bar{G}$ делится на $\bar{\psi}$. Но тогда из равенства $\bar{\Phi}_m=\bar{f}\bar{G}$ будет следовать, что $\bar{\Phi}_m$ делится на $\bar{\psi}^2$, что, однако, противоречит лемме 1. Таким образом, ζ^p не может быть корнем $G(t)$, а значит, он является корнем $f(t)$.

Если теперь ζ' — произвольный корень Φ_m, то $\zeta'=\zeta^k$, где k взаимно просто с m. Пусть $k=p_1p_2\dots p_s$. По только что доказанному ζ^{p_1} есть корень $f(t)$. Аналогично, взяв вместо ζ корень ζ^{p_1}, заключаем, что $\zeta^{p_1p_2}$ — корень $f(t)$. Рассуждая так далее, мы получим в конце концов, что и ζ^k является корнем $f(t)$.

Таким образом, все корни Φ_m являются также корнями многочлена f, а поэтому $\Phi_m=f$. Полученный результат мы можем сформулировать в виде следующей теоремы.

Теорема 1. *При любом натуральном m круговой многочлен Φ_m неприводим над полем рациональных чисел.*

Следствие. *Степень m-кругового поля $\mathbb{Q}(\zeta)$, $\zeta^m=1$, равна $\varphi(m)$ (где $\varphi(m)$ — функция Эйлера).*

Замечание. Поле $\mathbb{Q}(\zeta)$ деления круга на m частей нормально над $\mathbb{Q}$, и его группа Галуа естественным образом изоморфна группе приведенных классов вычетов по модулю m. Именно, если $(a, m)=1$, то соответствие $\zeta\to\zeta^a$ определяет автоморфизм σ_a расширения $\mathbb{Q}(\zeta)/\mathbb{Q}$ и отображение $a\to\sigma_a$ индуцирует изоморфизм группы классов приведенных вычетов по модулю m (порядка $\varphi(m)$) на группу Галуа расширения $\mathbb{Q}(\zeta)/\mathbb{Q}$. Таким образом, круговые поля являются абелевыми расширениями поля рациональных чисел $\mathbb{Q}$. Согласно теории Галуа всякое промежуточное поле F, $\mathbb{Q}\subset F\subset\mathbb{Q}(\zeta)$, также абелево над $\mathbb{Q}$. Все промежуточные поля F для всех m-круговых полей — это, оказывается, вообще все абелевы расширения над $\mathbb{Q}$: согласно знаменитой теореме Кронекера — Вебера каждое поле F, нормальное над $\mathbb{Q}$ и с абелевой группой Галуа, является подполем некоторого кругового поля. (Доказательство теоремы Кронекера — Вебера, основанное на привлечении полей p-адических чисел, приведено в [53], см. также [38].)

Теорема Кронекера — Вебера позволяет дать обозримое описание всех абелевых расширений над $\mathbb{Q}$. Для этого надо привлечь группу $\mathfrak{X}$ всех примитивных числовых характеров, указан-

ную в задаче 15 § 5 Дополнения. Пусть X — конечная подгруппа группы $\mathfrak{X}$. Выберем натуральное m, делящееся на ведущие модули всех характеров из X, и рассмотрим m-круговое поле $K = \mathbb{Q}_m(\zeta)$, $\zeta^m = 1$, группу Галуа которого обозначим через G. Группу X можно отождествить с группой характеров группы G, полагая $\chi(\sigma_a) = \chi(a)$, $(a, m) = 1$. Обозначим через H подгруппу в G, состоящую из тех $\sigma \in G$, для которых $\chi(\sigma) = 1$ при всех $\chi \in X$, и через F — подполе H-инвариантных элементов из K. Легко видеть, что поле F определено группой X однозначно, т. е. что оно не зависит от выбора m. Можно показать, далее, что отображение $X \to F$ является взаимно однозначным соответствием между всеми конечными подгруппами группы $\mathfrak{X}$ и всеми конечными абелевыми расширениями поля $\mathbb{Q}$. Поле F при этом будет вещественным тогда и только тогда, когда все характеры из X четные.

2. Закон разложения в круговом поле. Так как степень m-кругового поля $\mathbb{Q}(\zeta)$ равна $\varphi(m)$, то числа

$$1, \zeta, \ldots, \zeta^{\varphi(m)-1} \tag{2}$$

образуют базис $\mathbb{Q}(\zeta)$ над $\mathbb{Q}$.

Можно показать, что числа (2) образуют фундаментальный базис поля $\mathbb{Q}(\zeta)$. Другими словами, кольцо целых чисел поля $\mathbb{Q}(\zeta)$ (максимальный порядок) совпадает с кольцом $\mathbb{Z}[\zeta]$. При простом $m = l$ этот факт будет доказан в п. 1 § 5 этой главы.

Лемма 2. *Если простое число p не входит в m, то оно не входит также и в дискриминант $D = D(1, \zeta, \ldots, \zeta^{\varphi(m)-1})$ базиса* (2).

Доказательство. Дискриминант D равен, как известно, дискриминанту $D(\Phi_m)$ кругового многочлена Φ_m. Класс вычетов $\overline{D(\Phi_m)} \in \mathbb{F}_p$ числа $D(\Phi_m)$ по модулю p совпадает, очевидно, с дискриминантом $D(\bar{\Phi}_m)$ многочлена $\bar{\Phi}_m \in \mathbb{F}_p[t]$. Но $\bar{\Phi}_m(t)$ не имеет кратных корней (лемма 1), поэтому $D(\bar{\Phi}_m) \neq 0$, а значит, $D = D(\Phi_m)$ не делится на p.

Лемма 3. *Если в поле алгебраических чисел K содержится первообразный корень степени m из 1, то для любого простого дивизора $\mathfrak{p}$ поля K, взаимно простого с m, $N(\mathfrak{p}) \equiv 1 \pmod m$.*

Доказательство. Пусть $\mathfrak{O}$ — кольцо целых чисел поля K, p — простое рациональное число, делящееся на $\mathfrak{p}$, и ζ — первообразный корень степени m из 1 ($\zeta \in \mathfrak{O}$). В п. 1 мы видели, что в поле вычетов $\mathfrak{O}/\mathfrak{p}$, являющемся расширением поля $\mathbb{F}_p$, многочлен $t^m - 1$ не имеет кратных корней (так как $p \nmid m$). Следовательно, классы вычетов $\bar{1}, \bar{\zeta}, \ldots, \bar{\zeta}^{m-1}$ из $\mathfrak{O}/\mathfrak{p}$ попарно различны. Ясно, что эти классы образуют группу по умножению порядка m — подгруппу в мультипликативной группе поля вычетов $\mathfrak{O}/\mathfrak{p}$. Порядок последней группы равен $N(\mathfrak{p}) - 1$. Но порядок конечной группы делится на порядок любой ее подгруппы, поэтому $N(\mathfrak{p}) - 1$ делится на m, а это и требовалось доказать.

Теорема 2. *Пусть для простого числа p, не входящего в m, через f обозначено наименьшее натуральное число, для которого $p^f \equiv 1 \pmod m$, и пусть $g = \varphi(m)/f$. Тогда в m-круговом поле $\mathbb{Q}(\zeta)$ для p имеет место разложение*

$$p = \mathfrak{p}_1 \dots \mathfrak{p}_g, \tag{3}$$

где простые дивизоры $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ попарно различны и $N(\mathfrak{p}_i) = p^f$.

Доказательство. Так как $(p, m) = 1$, то по лемме 2 p не входит в дискриминант базиса (2), и поэтому согласно теореме 8 § 5 гл. III для p будем иметь разложение вида (3). Нам остается только определить степень каждого простого дивизора $\mathfrak{p}_i$ и доказать, что число всех $\mathfrak{p}_i$ равно $\varphi(m)/f$.

Пусть $\mathfrak{p}$ — какой-нибудь из простых дивизоров $\mathfrak{p}_i$ и s — его степень, так что $N(\mathfrak{p}) = p^s$. По лемме 3 $p^s \equiv 1 \pmod m$, а значит, $s \geqslant f$. Для доказательства обратного неравенства рассмотрим поле вычетов $\mathfrak{O}/\mathfrak{p}$ в кольце $\mathfrak{O}$ целых чисел поля $\mathbb{Q}(\zeta)$ по модулю $\mathfrak{p}$. Согласно следствию леммы п. 4 § 7 гл. III в каждом классе вычетов из $\mathfrak{O}/\mathfrak{p}$ имеется представитель вида

$$\xi = \sum_{j=0}^{\varphi(m)-1} a_j \zeta^j, \tag{4}$$

где a_j — целые рациональные числа. Возведем (4) в степень p^f. Так как $p^f \equiv 1 \pmod m$, то $\zeta^{p^f} = \zeta$. Учитывая, далее, что $(\alpha + \beta)^{p^f} \equiv \alpha^{p^f} + \beta^{p^f} \pmod{\mathfrak{p}}$ при любых α и β из $\mathfrak{O}$, а также, что $a^{p^f} \equiv a \pmod{\mathfrak{p}}$ при любом целом рациональном a, мы из (4) получим сравнение

$$\xi^{p^f} \equiv \xi \pmod{\mathfrak{p}}.$$

Таким образом, произвольно взятый класс вычетов $\overline{\xi} \in \mathfrak{O}/\mathfrak{p}$ является корнем многочлена $t^{p^f} - t$. Но в любом поле число корней многочлена не превосходит его степени, поэтому $p^s \leqslant p^f$ и, значит, $s \leqslant f$. Сопоставляя это неравенство с полученным ранее, мы получаем, что $s = f$.

Нами доказано, таким образом, что все простые дивизоры $\mathfrak{p}_i$ из разложения (3) имеют одну и ту же степень f, равную показателю числа p по модулю m. Применяя теперь теорему 8 § 5 гл. III, мы устанавливаем, что число g простых дивизоров $\mathfrak{p}_i$ равно $\varphi(m)/f$. Теорема 2 доказана.

3. Выражение h через значения L-рядов. Обратимся к дзета-функции $\zeta_K(s)$ m-кругового поля $K = \mathbb{Q}(\zeta)$, $\zeta^m = 1$. Воспользовавшись тождеством Эйлера (теорема 4 § 1) и объединив в нем вместе все те множители, которые соответствуют простым дивизорам $\mathfrak{p}$, делящим одно и то же простое рациональное p, можно

записать

$$\zeta_K(s) = \prod_{p} \prod_{\mathfrak{p}|p} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} \tag{5}$$

(внешнее произведение распространяется на все простые рациональные числа p). Множители, соответствующие простым дивизорам $\mathfrak{p}$, делящим m, образуют конечное произведение. Обозначим его через

$$G(s) = \prod_{\mathfrak{p}|m} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}. \tag{6}$$

Если $(p, m) = 1$, то для всякого простого дивизора $\mathfrak{p}$, делящего p, имеем $N(\mathfrak{p}) = p^{f_p}$, где f_p — показатель числа p по модулю m. Поскольку число различных $\mathfrak{p}$, делящих p, равно $\varphi(m)/f_p$ (теорема 2), то

$$\zeta_K(s) = G(s) \prod_{(p,m)=1} \left(1 - \frac{1}{p^{f_p s}}\right)^{-\varphi(m)/f_p}. \tag{7}$$

Каждый сомножитель из этого произведения преобразуем к более удобному для исследования виду. Для этого воспользуемся разложением

$$1 - \left(\frac{1}{p^s}\right)^{f_p} = \prod_{k=0}^{f_p-1} \left(1 - \frac{\varepsilon^k}{p^s}\right), \tag{8}$$

где $\varepsilon = \varepsilon_p = \cos\frac{2\pi}{f_p} + i \sin\frac{2\pi}{f_p}$. Теперь произведение

$$\prod_{k=0}^{f_p-1} \left(1 - \frac{\varepsilon_p^k}{p^s}\right)^{-\varphi(m)/f_p}$$

содержит $\varphi(m)$ сомножителей, и это число сомножителей одно и то же для всех p. Оказывается, что сомножители для различных p можно так сопоставить друг другу, что бесконечное произведение, стоящее в правой части равенства (7), распадается в произведение $\varphi(m)$ множителей, имеющих довольно простой вид. Это разложение основывается на понятии характера по модулю m. Нужные здесь сведения о характерах изложены в § 5 Дополнения.

Обозначим через G_m группу классов вычетов в кольце целых рациональных чисел по модулю m, состоящих из чисел, взаимно простых с m. Класс $\bar{p} \in G_m$ с представителем p имеет порядок f_p. Следовательно, для любого характера χ группы G_m значение $\chi(\bar{p})$, являясь корнем степени f_p из 1, должно совпадать с некоторым ε^k. Обратно, если выбрать произвольно один из корней ε^k, то на циклической подгруппе $\{\bar{p}\}$ группы G_m, порожденной классом $\bar{p}$, существует один и только один характер χ_1, для которого $\chi_1(\bar{p}) = \varepsilon^k$. По теореме 3 § 5 Дополнения этот характер χ_1 можно про-

должить $\varphi(m)/f_p$ способами до характера группы G_m. Таким образом, если χ будет пробегать все характеры группы G_m, то $\chi(\bar{p})$ даст нам все корни ε^k ($k=0, 1, \ldots, f_p-1$), причем каждый корень ε^k встретится ровно $\varphi(m)/f_p$ раз. Подставляя выражение (8) в формулу (7), получаем, следовательно,

$$\zeta_K(s) = G(s) \prod_{(p,m)=1} \prod_{\chi} \left(1 - \frac{\chi(\bar{p})}{p^s}\right)^{-1} \tag{9}$$

(внутреннее произведение распространяется на все характеры χ группы G_m).

Вместо характеров на группе G_m мы будем теперь рассматривать числовые характеры по модулю m (см. п. 3 § 5 Дополнения). Так как $\chi(p)=0$ для всякого p, входящего в m, и для всякого числового характера χ по модулю m, то равенству (9) можно придать вид

$$\zeta_K(s) = G(s) \prod_{p} \prod_{\chi} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

(здесь p пробегает уже все простые числа, а χ — все числовые характеры по модулю m). Меняя порядок умножения, мы приходим к формуле

$$\zeta_K(s) = G(s) \prod_{\chi} L(s, \chi), \tag{10}$$

в которой использовано следующее обозначение:

$$L(s, \chi) = \prod_{p} \frac{1}{1-\chi(p)/p^s}. \tag{11}$$

Заметим, что во всех только что проведенных выкладках предполагалось, что $s>1$ (при этом условии все операции над бесконечными произведениями легко могут быть обоснованы).

Замечание. В формуле (10) множитель $G(s)$ может быть опущен, если под χ будем понимать примитивные характеры по всем модулям d, являющимся делителями m; см. по этому поводу задачи 13—16.

Множитель $L(s, \chi_0)$ из произведения (10), соответствующий единичному характеру χ_0, лишь простым множителем отличается от ζ-функции Римана $\zeta(s)$. В самом деле, так как $\chi_0(p)=1$ при $(p, m)=1$ и $\chi_0(p)=0$ при $(p, m)>1$, то

$$L(s, \chi_0) = \prod_{(p,m)=1} \frac{1}{1-1/p^s} \qquad (s>1).$$

С другой стороны, применив теорему 4 § 1 к полю рациональных чисел $\mathbb{Q}$, мы получаем $\zeta(s) = \prod_{p} \frac{1}{1-1/p^s}$. Таким образом, $L(s, \chi_0) = \left(\prod_{p \mid m} \frac{1}{1-1/p^s}\right)^{-1} \zeta(s)$. Подставляя это выражение в

(10), получаем следующую окончательную формулу для $\zeta_K(s)$:

$$\zeta_K(s) = F(s)\,\zeta(s) \prod_{\chi \neq \chi_0} L(s, \chi), \qquad s > 1, \tag{12}$$

где нами положено (см. (6))

$$F(s) = \prod_{\mathfrak{p}|m} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} \cdot \prod_{p|m} \left(1 - \frac{1}{p^s}\right).$$

Изучим подробнее функции $L(s, \chi)$. *Рассматривая абсолютно* сходящийся при $s > 1$ ряд $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ и заменив разложение (24) § 1 равенством

$$\frac{1}{1 - \frac{\chi(p)}{p^s}} = \sum_{k=0}^{\infty} \left(\frac{\chi(p)}{p^s}\right)^k,$$

мы, почти дословно повторяя доказательство теоремы 4 § 1 (использовав лишь мультипликативное свойство характера χ), легко получим, что

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \qquad s > 1. \tag{13}$$

Ряд, стоящий в правой части равенства (13), называется *L-рядом* или *рядом Дирихле* для числового характера χ. Нашей ближайшей целью является доказательство того, что для неединичного характера χ L-ряд сходится не только при $s > 1$, но также и при $s > 0$ (конечно, в промежутке $0 < s \leqslant 1$ сходимость будет неабсолютной). Установим для этого следующую лемму.

Лемма 4. *Пусть последовательность комплексных чисел* $\{a_n\}$ $(n = 1, 2, \ldots)$ *такова, что суммы* $A_n = \sum_{k=1}^{n} a_k$ *ограничены, т. е.* $|A_n| \leqslant C$ *при всех* $n \geqslant 1$. *Тогда ряд*

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

сходится при всех вещественных $s > 0$. *Для любого* $\sigma > 0$ *в промежутке* $[\sigma, \infty)$ *сходимость будет равномерной, так что сумма* $f(s)$ *является непрерывной функцией от* s (*в области сходимости* $(0, \infty)$).

Доказательство. Зафиксируем произвольно $\sigma > 0$. Для любого $\varepsilon > 0$ найдется такое n_0, что $\frac{1}{n^\sigma} < \varepsilon$ при всех $n > n_0$. При тех же $n > n_0$ также $\frac{1}{n^s} < \varepsilon$, если только $s \geqslant \sigma$. Пусть $M > N > n_0$.

Тогда

$$\sum_{k=N}^{M}\frac{a_k}{k^s}=\sum_{k=N}^{M}\frac{A_k-A_{k-1}}{k^s}=\sum_{k=N}^{M}\frac{A_k}{k^s}-\sum_{k=N-1}^{M-1}\frac{A_k}{(k+1)^s}=$$

$$=-\frac{A_{N-1}}{N^s}+\sum_{k=N}^{M-1}A_k\left(\frac{1}{k^s}-\frac{1}{(k+1)^s}\right)+\frac{A_M}{M^s},$$

откуда

$$\left|\sum_{k=N}^{M}\frac{a_k}{k^s}\right|\leqslant\frac{C}{N^s}+C\sum_{k=N}^{M-1}\left(\frac{1}{k^s}-\frac{1}{(k+1)^s}\right)+\frac{C}{M^s}=\frac{2C}{N^s}<2C\varepsilon$$

для всех s из промежутка $[\sigma, \infty)$. Лемма 4 доказана.

Следствие. *Для неединичного характера* χ *ряд Дирихле* $L(s, \chi)$ *сходится при* $s>0$ *и представляет в промежутке* $(0, \infty)$ *непрерывную функцию.*

Действительно, если $\chi\neq\chi_0$, то $\sum\overline{\chi(k)}=0$, если k пробегает полную систему вычетов по модулю m. Представим произвольное натуральное n в виде $n=mq+r$, $0\leqslant r<m$. Тогда $A_n=\sum_{k=1}^{n}\chi(k)=\sum_{k=1}^{r}\chi(k)$, откуда $|A_n|\leqslant r<m$.

Возвращаясь к функции $\zeta_K(s)$, умножим равенство (12) на $s-1$ и перейдем к пределу при $s\to 1+0$. В силу соотношения (19) § 1 мы получим, что

$$\lim_{s\to 1+0}(s-1)\zeta_K(s)=F(1)\prod_{\chi\neq\chi_0}L(1,\chi), \tag{14}$$

где

$$L(1,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n}. \tag{15}$$

Заметим, что поскольку ряд (15) сходится не абсолютно, то надо иметь в виду, что его члены расположены в порядке возрастания n. Сопоставляя (14) с теоремой 2 § 1, получаем для числа h следующую формулу:

$$h=\frac{w\sqrt{|D|}}{2^{s+t}\pi^t R}F(1)\prod_{\chi\neq\chi_0}L(1,\chi) \tag{16}$$

(здесь w обозначает число корней из 1, содержащихся в K). Полученное выражение (16) для числа классов дивизоров кругового поля еще нельзя считать окончательным, так как оно содержит бесконечные ряды $L(1, \chi)$. Суммирование этих рядов мы проведем в следующем пункте.

Замечание. В соответствии с замечанием к формуле (10) множитель $F(1)$ в формуле (14) также будет отсутствовать, если χ будет пробегать все примитивные характеры для всех ведущих модулей $d\neq 1$, являющихся делителями числа m (задача 16).

Можно показать, что для любого абелева расширения $F/\mathbb{Q}$, соответствующего конечной подгруппе X группы числовых примитивных характеров χ (см. замечание в конце п. 1) справедлива формула

$$\lim_{s\to 1+0}(s-1)\zeta_F(s)=\prod_{\chi\in X,\chi\neq 1}L(1,\chi),$$

где χ пробегает все характеры из X, кроме единичного. Сопоставление этой формулы с теоремой 2 § 1 дает возможность получить формулу для числа классов дивизоров $h(F)$ поля F. Если F — вещественное абелево расширение поля рациональных чисел степени n (в этом случае все характеры $\chi\in X$ четные), то $s=n$, $t=0$, $w=2$, и мы получаем формулу

$$\frac{2^{n-1}h(F)\,\mathrm{R}(F)}{\sqrt{D(F)}}=\prod_{\chi\in X,\chi\neq 1}L(1,\chi),$$

в которой $\mathrm{R}(F)$ — регулятор и $D(F)$ — дискриминант поля F.

4. Суммирование рядов $L(1,\chi)$. Считая, что χ — неединичный характер по модулю m, обратимся к ряду (13). Опуская в нем слагаемые, равные нулю, и замечая, что $\chi(n_1)=\chi(n_2)$ при $n_1\equiv n_2 \pmod m$, мы можем его переписать следующим образом (здесь существенно, что $s>1$):

$$L(s,\chi)=\sum_{(x,m)=1}\chi(x)\sum_{n\equiv x(\mathrm{mod}\,m)}\frac{1}{n^s}$$

(внешнее суммирование ведется по приведенной системе вычетов по модулю m). Внутренний ряд представим в виде $\sum_{n=1}^{\infty}\frac{c_n}{n^s}$, где

$$c_n=\begin{cases}1 & \text{при } n\equiv x \pmod m,\\ 0 & \text{при } n\not\equiv x \pmod m.\end{cases}$$

Чтобы найти удобную запись для коэффициентов c_n, обратим внимание на следующую очевидную формулу:

$$\sum_{k=0}^{m-1}\zeta^{rk}=\begin{cases}m & \text{при } r\equiv 0 \pmod m,\\ 0 & \text{при } r\not\equiv 0 \pmod m,\end{cases}$$

где $\zeta=\cos\frac{2\pi}{m}+i\sin\frac{2\pi}{m}$ — первообразный корень степени m из 1. Подчеркнем здесь, что, в то время как при алгебраических исследованиях кругового поля нам было безразлично, какой именно первообразный корень m-й степени из 1 мы обозначаем через ζ, сейчас, при аналитических выкладках, нам надо четко фиксировать один из этих корней. Мы имеем, следовательно,

$$c_n=\frac{1}{m}\sum_{k=0}^{m-1}\zeta^{(x-n)k}.$$

Таким образом,

$$L(s,\chi)=\sum_{(x,m)=1}\chi(x)\sum_{n=1}^{\infty}\frac{1}{m}\sum_{k=0}^{m-1}\zeta^{(x-n)k}\frac{1}{n^s}=$$

$$=\frac{1}{m}\sum_{k=0}^{m-1}\left(\sum_{(x,m)=1}\chi(x)\zeta^{xk}\right)\sum_{n=1}^{\infty}\frac{\zeta^{-nk}}{n^s}.$$

Выражение, стоящее в скобках, в случае простого $m=p$ нам уже встречалось в § 2 гл. I и называлось там гауссовой суммой. Дадим определение гауссовых сумм для произвольных m.

Определение. *Пусть ζ — фиксированный первообразный корень степени m из 1 и χ — числовой характер по модулю m. Выражение*

$$\tau_a(\chi)=\sum_{x \bmod m}\chi(x)\zeta^{ax},$$

где x пробегает полную (или приведенную) систему вычетов по модулю m, называется гауссовой суммой, соответствующей характеру χ и целому рациональному числу a.

Гауссова сумма $\tau_a(\chi)$ зависит, таким образом, не только от χ и вычета a по модулю m, но и от выбора первообразного корня ζ. Мы в дальнейшем будем предполагать, что в качестве ζ взят корень $\cos\frac{2\pi}{m}+i\sin\frac{2\pi}{m}$. Гауссова сумма с таким значением ζ называется *нормированной*.

Сумму $\tau_1(\chi)$ мы будем обозначать также через $\tau(\chi)$.

Если характер χ неединичный, то

$$\tau_0(\chi)=\sum_{(x,m)=1}\chi(x)=0.$$

Полученное нами выражение для ряда $L(s,\chi)$ мы можем поэтому переписать в виде

$$L(s,\chi)=\frac{1}{m}\sum_{k=1}^{m-1}\tau_k(\chi)\sum_{n=1}^{\infty}\frac{\zeta^{-nk}}{n^s}.$$

К ряду $\sum_{n=1}^{\infty}\frac{\zeta^{-nk}}{n^s}$ можем применить лемму 4 ($\zeta^{-k}\neq 1$ при $k\not\equiv 0 \pmod m$, поэтому $\sum_{n=1}^{mr}\zeta^{-nk}=0$). Согласно этой лемме наш ряд сходится при $0<s<\infty$ и представляет в этом промежутке непрерывную функцию от s. В силу этого в последнем равенстве мы можем положить $s=1$ и в результате получим

$$L(1,\chi)=\frac{1}{m}\sum_{k=1}^{m-1}\tau_k(\chi)\sum_{n=1}^{\infty}\frac{\zeta^{-nk}}{n}.$$

Чтобы найти сумму внутреннего ряда, обратимся к степенному ряду $\sum_{n=1}^{\infty} \frac{z^n}{n}$. Известно, что он сходится в круге $|z|<1$ и представляет там ветвь функции $-\ln(1-z)$, мнимая часть которой (т. е. коэффициент при i) содержится в промежутке $(-\pi/2, \pi/2)$. Поскольку наш степенной ряд в точке $z=\zeta^{-k}$ (на единичной окружности) также сходится, то по теореме Абеля

$$\sum_{n=1}^{\infty} \frac{\zeta^{-nk}}{n} = -\ln(1-\zeta^{-k}),$$

а значит,

$$L(1,\chi) = -\frac{1}{m}\sum_{k=1}^{m-1} \tau_k(\chi)\ln(1-\zeta^{-k}). \tag{17}$$

Для ряда $L(1, \chi)$ получено, таким образом, конечное выражение. Подставляя его в (16), находим формулу для числа классов дивизоров кругового поля, уже не содержащую бесконечных рядов.

Формула (17) может быть исследована дальше и значительно упрощена. В следующем пункте мы проведем это исследование, но не для общего случая, а лишь для примитивных характеров χ. В § 5 мы применим полученные результаты к исследованию формулы для h в случае поля деления круга на простое число частей. Именно в этом случае формула для числа классов дивизоров имеет особенно важные приложения.

5. **Ряды $L(1, \chi)$ для примитивных характеров.** Докажем, что если χ — примитивный характер по модулю m и $(a, m)=r>1$, то

$$\tau_a(\chi)=0.$$

Положим $m=rd$. Ясно, что ζ^a является первообразным корнем степени d из 1, а потому $\zeta^{az}=\zeta^a$, если только $z\equiv 1 \pmod d$. Возьмем в качестве z число, для которого $(z, m)=1$, $z\equiv 1 \pmod d$ и $\chi(z)\neq 1$ (существование такого z обеспечено теоремой 4 § 5 Дополнения). Так как вместе с x произведение zx также пробегает полную систему вычетов по модулю m, то

$$\tau_a(\chi) = \sum_{x \bmod m} \chi(zx)\zeta^{azx} = \chi(z)\sum_{x \bmod m}\chi(x)\zeta^{ax} = \chi(z)\tau_a(\chi).$$

Так как $\chi(z)\neq 1$, то отсюда следует, что $\tau_a(\chi)=0$.

Далее, если $(a, m)=1$, то $\tau_a(\chi)=\chi(a)^{-1}\tau(\chi)$.

В самом деле, так как вместе с x произведение ax также пробегает полную систему вычетов по модулю m, то

$$\chi(a)\tau_a(\chi) = \sum_{x \bmod m}\chi(ax)\zeta^{ax} = \tau_1(\chi) = \tau(\chi).$$

Формулу (17) в случае примитивного характера χ мы можем, следовательно, переписать в виде

$$L(1, \chi) = -\frac{\tau(\chi)}{m} \sum_{(k,m)=1} \overline{\chi}(k) \ln(1 - \zeta^{-k}). \tag{18}$$

Обратимся к изучению суммы

$$S_\chi = \sum_{(k,m)=1} \overline{\chi}(k) \ln(1 - \zeta^{-k}) \tag{19}$$

(k пробегает приведенную систему вычетов по модулю m). Исследование суммы S_χ приводит нас к двум существенно различным по виду результатам. Для разграничения этих двух случаев нам надо ввести следующее определение.

Определение. *Числовой характер* χ *называется четным, если* $\chi(-1) = 1$ (и, следовательно, $\chi(-x) = \chi(x)$ при всех целых x), *и называется нечетным, если* $\chi(-1) = -1$ (в этом случае $\chi(-x) = -\chi(x)$).

Так как

$$(\chi(-1))^2 = \chi((-1)^2) = \chi(1) = 1,$$

то $\chi(-1) = \pm 1$, поэтому всякий характер χ будет либо четным, либо нечетным.

Тригонометрическая форма числа $1 - \zeta^{-k}$ при $0 < k < m$ имеет вид

$$1 - \zeta^{-k} = 2 \sin \frac{\pi k}{m} \left(\cos\left(\frac{\pi}{2} - \frac{\pi k}{m}\right) + i \sin\left(\frac{\pi}{2} - \frac{\pi k}{m}\right)\right),$$

причем $-\frac{\pi}{2} < \frac{\pi}{2} - \frac{\pi k}{m} < \frac{\pi}{2}$; поэтому

$$\ln(1 - \zeta^{-k}) = \ln|1 - \zeta^{-k}| + i\pi\left(\frac{1}{2} - \frac{k}{m}\right).$$

Далее, так как $1 - \zeta^{-k}$ и $1 - \zeta^k$ сопряжены между собой, то

$$\ln(1 - \zeta^k) = \ln|1 - \zeta^k| - i\pi\left(\frac{1}{2} - \frac{k}{m}\right).$$

(Подчеркнем еще раз, что обе последние формулы справедливы лишь при условии, что k находится среди наименьших положительных вычетов по модулю m.)

Предположим теперь, что характер χ (а значит, и $\overline{\chi}$) четный. Заменив в сумме (19) k на $-k$, получим

$$S_\chi = \sum_{(k,m)=1} \overline{\chi}(k) \ln(1 - \zeta^k),$$

что при сложении с (19) дает нам

$$2S_\chi = \sum_{(k,m)=1} \overline{\chi}(k)\left[\ln\left(1-\zeta^{-k}\right)+\ln\left(1-\zeta^{k}\right)\right] =$$

$$= 2\sum_{(k,m)=1} \overline{\chi}(k)\ln\left|1-\zeta^{k}\right| = 2\sum_{\substack{(k,m)=1\\0<k<m}} \overline{\chi}(k)\ln 2\sin\frac{\pi k}{m}.$$

Если же характер χ нечетный, то, опять заменив в (19) k на $-k$, мы получим

$$S_\chi = -\sum_{(k,m)=1} \overline{\chi}(k)\ln\left(1-\zeta^{k}\right),$$

откуда

$$2S_\chi = \sum_{(k,m)=1} \overline{\chi}(k)\left[\ln\left(1-\zeta^{-k}\right)-\ln\left(1-\zeta^{k}\right)\right] =$$

$$= 2\sum_{\substack{(k,m)=1\\0<k<m}} \overline{\chi}(k)\,\pi i\left(\frac{1}{2}-\frac{k}{m}\right).$$

Учитывая, что $\sum_{(k,m)=1} \overline{\chi}(k) = 0$ (ведь характер $\overline{\chi}$ неединичный), и принимая во внимание (18), мы приходим к следующему результату.

Теорема 3. *Пусть χ — примитивный характер по модулю $m>1$. Если χ четный, то*

$$L(1,\chi) = -\frac{\tau(\chi)}{m}\sum_{(k,m)=1} \overline{\chi}(k)\ln\left|1-\zeta^{k}\right| =$$

$$= -\frac{\tau(\chi)}{m}\sum_{\substack{(k,m)=1\\0<k<m}} \overline{\chi}(k)\ln\sin\frac{\pi k}{m}. \qquad (20)$$

Если же χ нечетный, то

$$L(1,\chi) = \frac{\pi i\tau(\chi)}{m^2}\sum_{\substack{(k,m)=1\\0<k<m}} \overline{\chi}(k)\,k. \qquad (21)$$

Задачи

1. Доказать, что если χ — примитивный характер по модулю m, то $|\tau(\chi)| = \sqrt{m}$.

Указание. Следовать доказательству теоремы 4 § 2 гл. I.

2. Пусть p — нечетное простое число, $p^* = (-1)^{(p-1)/2}p$. Доказать, что квадратичное поле $\mathbb{Q}(\sqrt{p^*})$ содержится в поле деления круга на p частей (использовать задачу 5 § 2 гл. I при $a=b=1$).

3. Доказать, что всякое квадратичное поле содержится в некотором круговом поле.

4. В обозначениях задачи 6 § 5 Дополнения доказать равенство

$$\tau_a(\chi) = \tau_a(\chi_1)\ldots\tau_a(\chi_k)\chi_1(m/m_1)\ldots\chi_k(m/m_k)$$

(при определении гауссовых сумм $\tau_a(\chi_i)$ предполагается, что в качестве первообразного корня степени m_i из 1 взят корень ζ^{m/m_i}, где ζ — первообразный корень степени m из 1, участвующий в определении суммы $\tau_a(\chi)$).

5. Пусть простое число p не входит в m, и пусть f есть наименьшее натуральное число, для которого $p^f \equiv 1 \pmod m$. Доказать, что многочлен $\overline{\Phi}_m(t)$ с коэффициентами из $\mathbb{F}_p$ (см. п. 1) в кольце $\mathbb{F}_p[t]$ раскладывается в произведение $\varphi(m)/f$ неприводимых множителей, каждый из которых имеет степень f. (Ввиду теоремы 8 § 5 гл. III это дает нам второе доказательство теоремы 2.)

6. Пусть p — простое нечетное число. Рассматривая поле $\mathbb{Q}(\sqrt{-1})$ и сопоставляя для этого поля теорему 1 § 8 гл. III с теоремой 2 настоящего параграфа, получить равенство $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ (первое дополнение к квадратичному закону взаимности).

7. Пусть p и $q \neq 2$ — различные простые числа, K — поле деления круга на q частей и g — число различных простых дивизоров поля K, входящих в разложение числа p. Пользуясь критерием Эйлера $\left(\frac{a}{q}\right) \equiv a^{(q-1)/2} \pmod q$, доказать, что $\left(\frac{p}{q}\right) = (-1)^g$.

8. Сохраняя те же обозначения, рассмотрим квадратичное подполе $k = \mathbb{Q}(\sqrt{q^*})$ поля K, $q^* = (-1)^{(q-1)/2}q$. Положим $f = (q-1)/g$. Доказать, что если p разлагается в поле k в произведение двух простых дивизоров, то g четно, а если p остается простым в k, то f четно. Основываясь на теореме 1 § 8 гл. III, показать далее, что при $p \neq 2$

$$\left(\frac{q^*}{p}\right) = (-1)^g.$$

Таким образом, p разлагается в k тогда и только тогда, когда g четно.

Указание. В случае $q \equiv 1 \pmod 4$ воспользоваться задачей 7 и показать, что из $\left(\frac{p}{q}\right) = \left(\frac{p^*}{q}\right) = 1$ следует $\left(\frac{q}{p}\right) = \left(\frac{q^*}{p}\right) = 1$.

9. Из предшествующих двух задач вывести квадратичный закон взаимности $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

10. Доказать, что если простое $q \neq 2$ в поле $\mathbb{Q}(\sqrt{2})$ разлагается в произведение двух простых дивизоров и $q \equiv 1 \pmod 4$, то $q \equiv 1 \pmod 8$. (Рассмотреть разложение q в поле $\mathbb{Q}(\sqrt{2}, \sqrt{-1})$ деления круга на 8 частей.)

11. В обозначениях задач 7 и 8 показать, что число $p = 2$ разлагается в поле k в произведение двух простых дивизоров тогда и только тогда, когда g четно.

12. Сопоставляя результат предшествующей задачи с теоремой 1 § 8 гл. III, доказать, что равенство $\left(\frac{2}{q}\right) = +1$ эквивалентно сравнению $q^* \equiv 1 \pmod 8$, т. е. что $\left(\frac{2}{q}\right) = (-1)^{(q^2-1)/8}$ (второе дополнение к квадратичному закону взаимности).

13. Доказать, что в поле деления круга на p^k частей для простого числа p имеет место разложение

$$p = \mathfrak{p}^g, \quad g = \varphi(p^k) = p^{k-1}(p-1), \quad N(\mathfrak{p}) = p.$$

14. Пусть $m = p^k m'$, $(p, m') = 1$, и пусть f есть наименьшее натуральное число, для которого $p^f \equiv 1 \pmod{m'}$. Доказать, что в поле деления круга

на m частей разложение простого числа p имеет вид

$$p = (\mathfrak{p}_1 \dots \mathfrak{p}_g)^e, \quad N(\mathfrak{p}_i) = p^f,$$

где $e = \varphi(p^k)$, $fg = \varphi(m')$ (φ — функция Эйлера).

15. Доказать, что для функции $G(s)$, определенной равенством (6), справедлива формула

$$G(s) = \prod_{\mathfrak{p} \mid m} \prod_{\chi \bmod m'} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1},$$

где p пробегает все простые делители числа m, а χ (при данном p) пробегает все числовые характеры по модулю m', $m = p^h m'$, $p \nmid m$.

16. Используя задачу 9 § 5 Дополнения, равенство (10) и формулу предшествующей задачи, доказать, что для дзета-функции $\zeta_K(s)$ поля деления круга на m частей имеет место разложение

$$\zeta_K(s) = \prod_{d \mid m} \prod_{\substack{\chi \bmod d \\ \chi \text{ примит}}} L(s, \chi),$$

где d пробегает все делители числа m (включая 1 и m), а χ (при данном d) пробегает все примитивные характеры по модулю d. Вывести отсюда, что

$$\lim_{s \to 1+0} (s-1)\zeta_K(s) = \prod_{\substack{d \mid m \\ d \neq 1}} \prod_{\substack{\chi \bmod d \\ \chi \text{ примит}}} L(1, \chi).$$

§ 3. Простые дивизоры первой степени

В § 2 мы использовали теоремы 2 и 4 § 1 для вычисления числа h классов дивизоров в круговых полях. В этом параграфе мы покажем, что, наоборот, из наличия формулы (2) § 1 с отличной от нуля правой частью можно сделать важные выводы о простых дивизорах первой степени и о простых числах в арифметических прогрессиях.

1. Существование простых дивизоров первой степени.

Теорема 1. *В произвольном поле алгебраических чисел K существует бесконечно много простых дивизоров первой степени.*

Доказательство. Согласно теореме 4 § 1 для функции $\zeta_K(s)$ имеет место разложение

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}. \tag{1}$$

Так как сходящееся бесконечное произведение отлично от нуля, то $\zeta_K(s) \neq 0$ при всех $s > 1$. Прологарифмировав равенство (1), мы получим

$$\ln \zeta_K(s) = \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \frac{1}{m N(\mathfrak{p})^{ms}}. \tag{2}$$

Выделим в этом равенстве сумму

$$P(s) = \sum_{\mathfrak{p}_1} \frac{1}{N(\mathfrak{p}_1)^s}, \tag{3}$$

в которой суммирование распространено по всем простым дивизорам $\mathfrak{p}_1$ поля K первой степени. Если через $G(s)$ мы обозначим сумму всех остальных слагаемых, то равенство (2) можно будет переписать в виде

$$\ln \zeta_K(s) = P(s) + G(s). \tag{4}$$

Пусть f обозначает степень простого дивизора $\mathfrak{p}$, так что $N(\mathfrak{p}) = p^f$. Если $f \geqslant 2$, то

$$\sum_{m=1}^{\infty} \frac{1}{mN(\mathfrak{p})^{ms}} < \sum_{m=1}^{\infty} \frac{1}{p^{2sm}} = \frac{1}{p^{2s}-1} < \frac{2}{p^{2s}}.$$

Если же $f = 1$, то

$$\sum_{m=2}^{\infty} \frac{1}{mN(\mathfrak{p})^{ms}} < \sum_{m=2}^{\infty} \frac{1}{p^{sm}} = \frac{1}{p^s(p^s-1)} < \frac{2}{p^{2s}}.$$

Так как для каждого простого рационального числа p имеется не более $n = (K : \mathbb{Q})$ простых дивизоров поля K, делящих p, то для $G(s)$ мы получаем, таким образом, оценку

$$G(s) < \sum_{p} \frac{2n}{p^{2s}} < 2n \sum_{m=1}^{\infty} \frac{1}{m^{2s}},$$

откуда следует, что функция $G(s)$ ограничена при $s \to 1+0$. С другой стороны, из соотношения (2) § 1, в котором $\varkappa h \neq 0$, следует, что $\ln \zeta_K(s)$ вместе с $\zeta_K(s)$ стремится к бесконечности при $s \to 1+0$. Следовательно, ввиду (4) это же справедливо и для $P(s)$, а значит, сумма (3) не может состоять лишь из конечного числа слагаемых. Таким образом, число простых дивизоров $\mathfrak{p}_1$ первой степени бесконечно, и теорема 1 доказана.

Заметим, что приведенное доказательство бесконечности простых дивизоров первой степени использует ту же идею, на которой основано одно из доказательств бесконечности простых чисел (см. задачу 1).

2. Характеризация нормальных расширений законами разложения простых дивизоров первой степени. Пусть k — поле алгебраических чисел и K — его конечное расширение. Всякий простой дивизор $\mathfrak{p}$ поля k в поле K представляется в виде произведения степеней простых дивизоров $\mathfrak{P}$ поля K, делящих $\mathfrak{p}$ (см. равенство (2) § 5 гл. III). Такое разложение характеризуется набором индексов ветвления $e_{\mathfrak{P}}$ и степеней инерции $f_{\mathfrak{P}}$ дивизоров $\mathfrak{P}$ относительно k. В связи с этим под законом разложения в расширении K/k понимают соответствие, сопоставляющее каждому $\mathfrak{p}$ набор чисел $e_{\mathfrak{P}}$ и $f_{\mathfrak{P}}$ для всех $\mathfrak{P}$, делящих $\mathfrak{p}$.

Естественно возникает вопрос, характеризуется ли расширение своим законом разложения? Мы покажем, что для случая

нормальных расширений ответ утвердительный. Более того, нормальное расширение K/k однозначно определено уже указанием тех простых дивизоров $\mathfrak{p}$ поля k, абсолютная степень инерции которых равна 1 и для которых $e_{\mathfrak{P}} = f_{\mathfrak{P}} = 1$ при всех $\mathfrak{P}|\mathfrak{p}$.

Определение. *Простой дивизор $\mathfrak{p}$ поля k называется вполне распадающимся в конечном расширении K/k, если $e_{\mathfrak{P}} = f_{\mathfrak{P}} = 1$ для всех простых дивизоров $\mathfrak{P}$ поля K, делящих $\mathfrak{p}$.*

Согласно теореме 7 § 5 гл. III простые дивизоры $\mathfrak{p}$ поля k, вполне распадающиеся в расширении K/k степени n, характеризуются разложением $\mathfrak{p} = \mathfrak{P}_1 \dots \mathfrak{P}_n$.

Для конечного расширения K/k через $\Omega(K/k)$ обозначим множество всех простых дивизоров поля k, имеющих абсолютную степень инерции 1 и вполне распадающихся в K.

Теорема 2. *Пусть K_1/k и K_2/k — конечные нормальные расширения поля алгебраических чисел k (содержащиеся в некотором объемлющем их поле). Если $\Omega(K_1/k) = \Omega(K_2/k)$, то $K_1 = K_2$.*

Мы докажем несколько более общую теорему 2′, из которой теорема 2 будет вытекать в качестве очевидного следствия.

Все рассматриваемые здесь поля мы будем предполагать содержащимися в некотором объемлющем их поле. В этом случае для двух полей K и L однозначно определен их композит KL как наименьшее поле, содержащее K и L.

Теорема 2′. *Пусть K/k и L/k — конечные расширения поля алгебраических чисел k, причем расширение K/k нормально. Поле L содержится в K тогда и только тогда, когда $\Omega(L/k) \supset \Omega(K/k)$.*

Докажем предварительно следующий вспомогательный факт.

Лемма. *Пусть K/k и L/k — конечные расширения поля алгебраических чисел k. Тогда*

$$\Omega(KL/k) = \Omega(K/k) \cap \Omega(L/k).$$

Доказательство. Пусть $\mathfrak{p}$ — простой дивизор поля k первой степени. Если $\mathfrak{p}$ вполне распадается в KL, то, как это легко следует из задачи 21 § 5 гл. III, он будет вполне распадающимся и в промежуточных полях K и L. Обратно, пусть $\mathfrak{p}$ вполне распадается в K и в L. Воспользуемся теоремой 3 § 2 гл. IV. Согласно этой теореме минимальный многочлен всякого элемента из K или из L (над полем k) в $\mathfrak{p}$-адическом пополнении $k_{\mathfrak{p}}$ целиком раскладывается на линейные множители. Это значит (теорема 11 § 2 Дополнения), что все изоморфизмы расширений K/k и L/k в надлежащее расширение поля $k_{\mathfrak{p}}$, при котором каждый элемент из k отображается на себя, отображают K и L внутрь поля $k_{\mathfrak{p}}$. Но в таком случае всякий изоморфизм расширения KL/k в расширение поля $k_{\mathfrak{p}}$, тождественный на k, также отобразит KL внутрь поля $k_{\mathfrak{p}}$, а значит, минимальный многочлен всякого элемента из KL над k в поле $k_{\mathfrak{p}}$ раскладывается на линейные мно-

жители. Применяя опять теорему 3 § 2 гл. IV, заключаем, что $\mathfrak{p}$ вполне распадается в поле KL. Лемма доказана.

Доказательство теоремы 2′. Если $L \subset K$, то $\Omega(K/k)$ содержится в $\Omega(L/k)$ (как уже отмечалось, это очевидным образом следует из задачи 21 § 5 гл. III).

Обратно, предположим, что $\Omega(K/k) \subset \Omega(L/k)$. Рассмотрим композит $M = KL$. Согласно лемме имеет место равенство

$$\Omega(M/k) = \Omega(K/k). \tag{4°}$$

Пользуясь этим равенством, мы докажем, что $M = K$, откуда и будет следовать включение $L \subset K$. На самом деле мы докажем даже более сильное утверждение. Именно, из доказательства будет видно, что равенство $M = K$ следует уже из ослабленного включения $\Omega(K/k) - A \subset \Omega(M/k)$, где A — произвольное конечное подмножество в $\Omega(K/k)$.

Согласно п. 1 мы имеем

$$\ln \zeta_K(s) = \sum_{\mathfrak{P}} \frac{1}{N(\mathfrak{P})^s} + G_0(s), \tag{4′}$$

$$\ln \zeta_M(s) = \sum_{\mathfrak{Q}} \frac{1}{N(\mathfrak{Q})^s} + G_1(s), \tag{4″}$$

где $\mathfrak{P}$ и $\mathfrak{Q}$ пробегают все простые дивизоры первой степени полей K и M соответственно, а $G_0(s)$ и $G_1(s)$ — ограниченные функции при $s \to 1 + 0$.

Обозначим через A множество тех простых дивизоров из $\Omega(K/k)$, которые разветвлены в M (согласно следствию теоремы 8 § 5 гл. III подмножество A конечно). Пусть, далее, $\mathfrak{M}_0$ и $\mathfrak{M}$ — множества тех простых дивизоров первой степени полей K и M соответственно, которые не делят простых дивизоров поля k, содержащихся в A. Мы можем считать, что в равенствах (4′) и (4″) $\mathfrak{P}$ и $\mathfrak{Q}$ пробегают все простые дивизоры из $\mathfrak{M}_0$ и $\mathfrak{M}$ соответственно. В самом деле, те слагаемые, которые соответствуют делителям дивизоров из A, мы можем отнести к функциям $G_0(s)$ и $G_1(s)$, не нарушая их ограниченности при $s \to 1 + 0$.

Пусть $\mathfrak{P} \in \mathfrak{M}_0$ и $\mathfrak{p}$ — простой дивизор поля k, делящийся на $\mathfrak{P}$. Ясно, что индекс ветвления $e_{\mathfrak{P}}$ и степень инерции $f_{\mathfrak{P}}$ дивизора $\mathfrak{P}$ относительно k равны 1. Но тогда в силу нормальности расширения K/k (см. конец п. 3 § 5 гл. III) то же будет иметь место и для всех простых дивизоров поля K, делящих $\mathfrak{p}$, и, следовательно, $\mathfrak{p} \in \Omega(K/k)$, т. е. $\mathfrak{p}$ вполне распадается в K. Но тогда, в силу условия теоремы (равенство (4°)), $\mathfrak{p}$ будет вполне распадаться и в M, откуда очевидным образом следует, что

$$\mathfrak{P} = \mathfrak{Q}_1 \dots \mathfrak{Q}_m,$$

где все $\mathfrak{Q}_i$ принадлежат $\mathfrak{M}$, $m = (M : K)$ — степень расширения M/K и $N(\mathfrak{P}) = N(\mathfrak{Q}_i)$, $1 \leqslant i \leqslant m$ (последнее следует из того, что

$\mathfrak{P}$ и $\mathfrak{Q}_i$ являются делителями одного и того же простого рационального числа p).

Обратно, если $\mathfrak{Q} \in \mathfrak{M}$ и $\mathfrak{Q}$ является делителем простого дивизора $\mathfrak{P}$ поля K, то, очевидно, $\mathfrak{P} \in \mathfrak{M}_0$.

Из доказанного следует теперь, что

$$\sum_{\mathfrak{Q} \in \mathfrak{M}} \frac{1}{N(\mathfrak{Q})^s} = m \sum_{\mathfrak{P} \in \mathfrak{M}_0} \frac{1}{N(\mathfrak{P})^s},$$

а значит, разность $m \ln \zeta_K(s) - \ln \zeta_M(s)$ является ограниченной функцией при $s \to 1 + 0$.

С другой стороны, из соотношения (2) § 1 следует, что для любого поля алгебраических чисел K функция $\ln \zeta_K(s) - \ln \frac{1}{s-1}$ ограничена при $s \to 1 + 0$. Следовательно, ограниченной должна быть и функция $(m-1) \ln \frac{1}{s-1}$, что возможно лишь при $m = (M : K) = 1$. Таким образом, $M = K$, а значит, $L \subset K$.

Теорема 2′ и вместе с ней теорема 2 доказаны.

3. Теорема Дирихле о простых числах в арифметической прогрессии.

Теорема 3 (теорема Дирихле). *В каждом классе вычетов по модулю m, состоящем из чисел, взаимно простых с m, содержится бесконечно много простых чисел.*

Доказательство. В то время как в п. 1 нами был использован факт необращения в нуль предела (2) § 1, доказательство теоремы Дирихле основывается на том, что $L(1, \chi) \neq 0$ для любого неединичного характера χ по модулю m, что очевидным образом следует из формулы (16) § 2.

Рассмотрим разложение L-ряда $L(s, \chi)$ в бесконечное произведение:

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}. \tag{5}$$

Из сходимости этого бесконечного произведения следует, что для всякого числового характера χ по модулю m (в том числе и для единичного характера χ_0) $L(s, \chi)$ отлично от нуля при всех $s > 1$. Можно поэтому в промежутке $(1, \infty)$ рассмотреть комплекснозначную функцию $\ln L(s, \chi)$. При этом, поскольку логарифмическая функция неоднозначная, надо иметь в виду какую-нибудь определенную ее ветвь. Выбор этой ветви осуществим следующим образом. Возьмем логарифм от каждого сомножителя в бесконечном произведении (5), причем значение для него выберем так, чтобы имело место разложение

$$-\ln\left(1 - \frac{\chi(p)}{p^s}\right) = \sum_{n=1}^{\infty} \frac{\chi(p)^n}{np^{sn}}. \tag{6}$$

Просуммировав ряды (6) для всех p, мы получим

$$\sum_p -\ln\left(1-\frac{\chi(p)}{p^s}\right)=\sum_p\frac{\chi(p)}{p^s}+R(s,\chi),$$

где $R(s,\chi)=\sum_p\left(\frac{1}{2}\frac{\chi(p)^2}{p^{2s}}+\frac{1}{3}\frac{\chi(p)^3}{p^{3s}}+\dots\right)$ (абсолютная сходимость всех встречающихся здесь рядов при $s>1$ очевидна). Значение для $\ln L(s,\chi)$ выбираем теперь таким образом, чтобы для всех $s>1$ было справедливо равенство

$$\ln L(s,\chi)=\sum_p\frac{\chi(p)}{p^s}+R(s,\chi). \tag{7}$$

Заметим, что для единичного характера χ_0 значение $\ln L(s,\chi_0)$ будет вещественным.

Оценим функцию $R(s,\chi)$:

$$|R(s,\chi)|<\sum_p\sum_{n=2}^{\infty}\frac{1}{p^{sn}}<\sum_p\frac{1}{p(p-1)}<\sum_{n=1}^{\infty}\frac{1}{n(n+1)}=1.$$

Таким образом, $|R(s,\chi)|<1$ для всех $s>1$.

Наряду с числовыми характерами χ будем рассматривать характеры (обозначая их той же буквой χ) на группе G_m классов вычетов по модулю m, взаимно простых с m. Пусть C пробегает все классы из группы G_m. Так как $\chi(p)=\chi(C)$ при $p\in C$, то

$$\sum_p\frac{\chi(p)}{p^s}=\sum_C\chi(C)\sum_{p\in C}\frac{1}{p^s}$$

(напомним, что $\chi(p)=0$, если p делит m). Полагая

$$f(s,C)=\sum_{p\in C}\frac{1}{p^s},$$

равенству (7) можно придать вид

$$\ln L(s,\chi)=\sum_C\chi(C)f(s,C)+R(s,\chi). \tag{8}$$

Так как число всех характеров по модулю m равно $\varphi(m)$, то равенства (8) для всех χ можно рассматривать как систему $\varphi(m)$ линейных уравнений с $\varphi(m)$ неизвестными $f(s,C)$ (свободные члены которой равны разностям $\ln L(s,\chi)-R(s,\chi)$). Чтобы из этой системы найти $f(s,A)$ $(A\in G_m)$, умножим (8) на $\chi(A^{-1})$, а затем просуммируем по всем характерам χ. Мы получим

$$\sum_\chi\chi(A^{-1})\ln L(s,\chi)=\sum_C\sum_\chi\chi(CA^{-1})f(s,C)+R_A(s), \tag{9}$$

где для $R_A(s)=\sum_\chi\chi(A^{-1})R(s,\chi)$ имеет место оценка $|R_A(s)|<\varphi(m)$ при всех $s>1$. Согласно формуле (6) § 5 Дополнения

сумма $\sum_{\chi} \chi(CA^{-1})$ равна $\varphi(m)$ при $C = A$ и равна нулю при $C \neq A$, поэтому равенство (9) может быть переписано в виде

$$\ln L(s, \chi_0) + \sum_{\chi \neq \chi_0} \chi(A^{-1}) \ln L(s, \chi) = \varphi(m) f(s, A) + R_A(s). \quad (10)$$

Этим из системы (8) мы нашли значение $f(s, A)$.

Устремим теперь s к единице справа. Если $\chi \neq \chi_0$, то $L(s, \chi) \to L(1, \chi)$, при этом $L(1, \chi) \neq 0$, как было отмечено в начале доказательства. Следовательно, сумма, стоящая в левой части равенства (10) (распространенная на все неединичные характеры), будет иметь конечный предел. Перенося эту сумму в правую часть и объединяя ее с $R_A(s)$, получим равенство

$$\ln L(s, \chi_0) = \varphi(m) f(s, A) + T_A(s), \quad (11)$$

где T_A остается ограниченным при $s \to 1 + 0$.

Если мы предположим теперь, что число простых чисел в классе A конечно, то функция $f(s, A) = \sum_{p \in A} \frac{1}{p^s}$ будет иметь конечный предел при $s \to 1$, а тогда вся правая часть равенства (11) будет ограниченной при $s \to 1 + 0$. Это, однако, невозможно, так как

$$\lim_{s \to 1+0} L(s, \chi_0) = \infty,$$

что следует из равенства $L(s, \chi_0) = \zeta(s) \prod_{p \mid m} \left(1 - \frac{1}{p^s}\right)$. Полученное противоречие и доказывает теорему 3.

Теореме Дирихле можно дать следующее уточнение. Положим

$$f(s) = \sum_{A} f(s, A) = \sum_{(p, m) = 1} \frac{1}{p^s}.$$

Разделим равенство (11) на $\varphi(m)$ и просуммируем по всем классам $A \in G_m$. Мы получим

$$\ln L(s, \chi_0) = f(s) + T(s), \quad (12)$$

где $T(s)$ ограничено при $s \to 1 + 0$. Приравняем правые части (11) и (12), разделим полученное равенство на $\varphi(m) f(s)$ и перейдем к пределу при $s \to 1 + 0$. Мы придем тогда к равенству

$$\lim_{s \to 1+0} \frac{\sum_{p \in A} \frac{1}{p^s}}{\sum_{(p, m) = 1} \frac{1}{p^s}} = \frac{1}{\varphi(m)}.$$

Полученная формула говорит о том, что в определенном смысле простые числа, взаимно простые с m, распределяются равномерно по классам вычетов $\bmod m$ (с одинаковой плотностью).

Замечание 1. Поле деления круга на m частей, т. е. поле $\mathbb{Q}(\zeta)$, $\zeta^m = 1$, является нормальным расширением поля рациональных чисел $\mathbb{Q}$, и его группа Галуа G порядка $\varphi(m)$ естественным образом изоморфна группе приведенных классов вычетов по модулю m. Именно, каждому классу вычетов с представителем k, $(k, m) = 1$, взаимно однозначно соответствует автоморфизм σ из G, для которого $\zeta^\sigma = \zeta^k$. Каждому простому числу p, не входящему в m, мы можем, следовательно, однозначно сопоставить автоморфизм σ из G (для которого $\zeta^\sigma = \zeta^p$). Скажем в этом случае, что p принадлежит автоморфизму σ. Теорема Дирихле будет означать теперь, что каждому автоморфизму σ принадлежит бесконечно много простых чисел (с одной и той же плотностью распределения по всем автоморфизмам). В такой формулировке теорема Дирихле допускает обобщение на случай произвольного расширения Галуа поля рациональных чисел. Это обобщение, известное как закон плотности Н. Г. Чеботарева, состоит в следующем.

Пусть $K/\mathbb{Q}$ — расширение Галуа поля рациональных чисел $\mathbb{Q}$ с группой Галуа G. Пусть, далее, p — простое число, взаимно простое с дискриминантом поля K. Для каждого простого дивизора $\mathfrak{P}$ поля K, делящего p, однозначно определен автоморфизм $\sigma \in G$ такой, что для любого целого α из K справедливо сравнение $\alpha^\sigma \equiv \alpha^p \pmod{\mathfrak{P}}$. При замене $\mathfrak{P}$ на другой простой делитель числа p автоморфизм σ заменится на сопряженный с ним элемент группы G, и этим способом мы получим все сопряженные с σ элементы. Говорят, что простое число p принадлежит так построенному классу сопряженных элементов группы G. В 1923 г. Н. Г. Чеботарев показал [52], что плотность множества простых чисел, принадлежащих данному классу сопряженных автоморфизмов, равна отношению числа элементов в классе к порядку группы G. В частности, каждому классу принадлежит бесконечно много простых чисел.

Замечание 2. Теорема 3 дает нам информацию о простых числах p, удовлетворяющих сравнению $p \equiv a \pmod m$, или, в других терминах, конечному набору неравенств

$$\varphi_{p_i}(p - a) < \varepsilon_i, \quad i = 1, \ldots, r; \quad \varepsilon_i > 0,$$

где φ_{p_i} — метрики, соответствующие всем простым делителям $p_1, \ldots, p_r$ числа m. При такой интерпретации теорему Дирихле можно сопоставить с асимптотическим законом распределения простых чисел, дающим информацию о «плотности» простых чисел, удовлетворяющих условию $|x| < N$ (т. е. величина которых в смысле архимедовой метрики не превосходит заданной величины N).

Доказательство теоремы Дирихле, как мы видели, основывается на том, что $L(1, \chi) \neq 0$. Доказательство асимптотического

закона распределения простых чисел основывается на неравенстве $\zeta(1+i\tau)\neq 0$ для вещественных τ. Уже это обстоятельство наводит на мысль о существовании аналогий между функциями $L(\sigma, \chi)$ и $\zeta(\sigma+i\tau)$ от вещественного аргумента σ. Семейство L-функций параметризуется числовыми характерами χ, второе семейство — вещественными числами τ.

Покажем, что подмеченная аналогия простирается дальше и проявляется в родстве параметризаций. Каждый характер χ с ведущим модулем m *однозначно распространяется* до гомоморфизма группы $(\mathbb{Q}^*)_m$ тех не равных 0 рациональных чисел, числители и знаменатели которых взаимно просты с m, в группу комплексных чисел, по модулю равных 1, и этот гомоморфизм непрерывен относительно топологии, определенной конечным набором неархимедовых метрик $\varphi_{p_1}, \ldots, \varphi_{p_r}$. Можно считать поэтому, что все функции $L(\sigma, \chi)$ параметризуются непрерывными (в указанном смысле) гомоморфизмами групп типа $(\mathbb{Q}^*)_m$ в единичную окружность. С другой стороны, функция $\zeta(\sigma+i\tau)$ от вещественного аргумента σ может быть записана в виде

$$\zeta(\sigma+i\tau)=\sum_{n=1}^{\infty}\frac{\psi_\tau(n)}{n^\sigma}, \tag{13}$$

где $\psi_\tau(n)=n^{-i\tau}$. Так как $\psi_\tau(nm)=\psi_\tau(n)\psi_\tau(m)$ и $|\psi_\tau(n)|=1$, то функцию ψ_τ мы можем однозначно продолжить до непрерывного гомоморфизма всей мультипликативной группы $\mathbb{Q}^*$ в единичную окружность (непрерывность здесь понимается в смысле обычной архимедовой метрики). Таким образом, и здесь функции $\zeta(\sigma+i\tau)$ могут быть параметризованы непрерывными гомоморфизмами (характерами) группы $\mathbb{Q}^*$ в единичную окружность.

Мысль о наличии аналогий между функциями $L(\sigma, \chi)$ и $\zeta(\sigma+i\tau)$ подкрепляется также сравнением приведенной выше формулы (13) с формулой (13) § 2.

В свете изложенных соображений аналогом гипотезы Римана о нулях функции $\zeta(s)$ в полосе $0<\sigma<1$ будет предположение: $L(\sigma, \chi)\neq 0$ при вещественных $\sigma>1/2$. Хотя это утверждение, как и классическая гипотеза Римана, тоже не доказано, оно представляется более «арифметическим» ее аналогом и поэтому может оказаться доступнее. В следующем параграфе мы отметим один частный случай, когда аналог гипотезы Римана для L-рядов принимает особенно простой вид.

Задачи

1. Показать, что разность между функциями $\ln\zeta(s)$ и $g(s)=\sum_p \frac{1}{p^s}$ (p пробегает все простые рациональные числа) ограничена при $s\to 1+0$.

2. Пусть $P(s)$ — функция, определенная равенством (3). Доказать, что разность $P(s)-\ln\frac{1}{s-1}$ ограничена при $s\to 1+0$.

3. Целое рациональное число a называется *вычетом n-й степени* по простому модулю p, если разрешимо сравнение $x^n \equiv a \pmod p$. Доказать, что для любого a и любого n существует бесконечно много простых чисел p, по модулю которых a является вычетом n-й степени.

4. Пусть целые числа $a_1, \ldots, a_n$ таковы, что $a_1^{x_1} \ldots a_n^{x_n}$ является квадратом тогда и только тогда, когда все x_i четные. Доказать, что для любого набора знаков $\varepsilon_1, \ldots, \varepsilon_n$ ($\varepsilon_i = \pm 1$) существует бесконечно много простых чисел $p \neq 2$ (не делящих $a_1, \ldots, a_n$), для которых

$$\left(\frac{a_1}{p}\right) = \varepsilon_1, \ldots, \left(\frac{a_n}{p}\right) = \varepsilon_n.$$

Указание. Рассмотреть сумму

$$\sum_{\mathfrak{p}} \left(\prod_i \left(1 + \varepsilon_i \left(\frac{a_i}{p}\right)\right)\right) \frac{1}{p^s}.$$

§ 4. Число классов дивизоров квадратичного поля

1. Формула для числа классов дивизоров. Пусть $K = \mathbb{Q}(\sqrt{d})$ — квадратичное поле (d — свободное от квадратов целое рациональное число). Согласно теореме 2 § 8 гл. III в поле K для разложения простого рационального числа p в произведение простых дивизоров могут представиться следующие возможности:

1) $p = \mathfrak{p}\mathfrak{p}'$, $\mathfrak{p} \neq \mathfrak{p}'$, $N(\mathfrak{p}) = N(\mathfrak{p}') = p$, если $\chi(p) = 1$;

2) $p = \mathfrak{p}$, $N(\mathfrak{p}) = p^2$, если $\chi(p) = -1$;

3) $p = \mathfrak{p}^2$, $N(\mathfrak{p}) = p$, если $\chi(p) = 0$;

где χ — характер квадратичного поля K (см. определение п. 2 § 8 гл. III). Следовательно, в произведении

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}$$

множители, соответствующие числу p, будут соответственно равны:

1) $\left(1 - \frac{1}{p^s}\right)^{-1}\left(1 - \frac{1}{p^s}\right)^{-1}$;

2) $\left(1 - \frac{1}{p^{2s}}\right)^{-1} = \left(1 - \frac{1}{p^s}\right)^{-1}\left(1 + \frac{1}{p^s}\right)^{-1}$;

3) $1 - \frac{1}{p^s}$.

Во всех трех случаях вносимый числом p множитель может быть записан в виде

$$\left(1 - \frac{1}{p^s}\right)^{-1}\left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Так как $\prod_{\mathfrak{p}} \left(1 - \frac{1}{p^s}\right)^{-1} = \zeta(s)$ (теорема 4 § 1, примененная к полю

рациональных чисел), то для $\zeta_K(s)$ получаем представление

$$\zeta_K(s) = \zeta(s) \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}. \tag{1}$$

Бесконечное произведение, стоящее в правой части, является L-рядом $L(s, \chi)$ для характера χ (по модулю $|D|$, где D — дискриминант поля K), и так как этот характер неединичный, то $L(s, \chi)$ есть непрерывная функция в промежутке $0 < s < \infty$ (следствие к лемме 4 § 2). Умножим (1) на $s-1$ и перейдем к пределу при $s \to 1+0$. Учитывая равенство (19) § 1, получаем

$$\lim_{s \to 1+0} (s-1)\zeta_K(s) = L(1, \chi).$$

Воспользуемся теперь теоремой 2 § 1. Так как для вещественного квадратичного поля $s=2$, $t=0$, $m=2$, $R = \ln \varepsilon$ ($\varepsilon > 1$ — основная единица поля), а для мнимого $s=0$, $t=1$, $R=1$, то для числа классов дивизоров поля K имеем формулы

$$h = \begin{cases} \dfrac{\sqrt{D}}{2 \ln \varepsilon} L(1, \chi) & \text{при } d > 0, \\ \dfrac{m\sqrt{|D|}}{2\pi} L(1, \chi) & \text{при } d < 0. \end{cases}$$

(Заметим, что число m, т. е. число содержащихся в K корней из 1, равно 4 для $K = \mathbb{Q}(\sqrt{-1})$, равно 6 для $K = \mathbb{Q}(\sqrt{-3})$ и равно 2, для всех остальных мнимых квадратичных полей; см. п. 3 § 7 гл. II.)

В следующем пункте мы докажем, что характер квадратичного поля с дискриминантом D является примитивным характером по модулю $|D|$ (см. определение п. 3 § 5 Дополнения), а также, что он четный для вещественных полей и нечетный — для мнимых. Мы можем поэтому воспользоваться формулами (20) и (21) § 2 для значения $L(1, \chi)$. Чтобы получить законченные формулы для h, нам надо еще знать точное значение для нормированных гауссовых сумм $\tau(\chi) = \tau_1(\chi)$. В п. 3 настоящего параграфа мы увидим, что сумма $\tau(\chi)$ равна $\sqrt{D}$ для вещественных полей и равна $i\sqrt{|D|}$ — для мнимых. Учитывая это и замечая, что в случае вещественного поля $\chi(D-x) = \chi(x)$, мы можем сформулировать следующую теорему (в целях упрощения формулы для h в случае мнимого поля мы отбросили поля $\mathbb{Q}(\sqrt{-1})$ и $\mathbb{Q}(\sqrt{-3})$ с дискриминантами -4 и -3, для которых m равно соответственно 4 и 6; для этих полей $h=1$).

Теорема 1. *Число классов дивизоров h вещественного квадратичного поля с дискриминантом D выражается формулой*

$$h = -\frac{1}{\ln \varepsilon} \sum_{\substack{(x, D)=1 \\ 0 < x < D/2}} \chi(x) \ln \sin \frac{\pi x}{D}, \tag{2}$$

где $\varepsilon > 1$ — основная единица поля, а мнимого квадратичного поля с дискриминантом $D < -4$ — формулой

$$h = -\frac{1}{|D|} \sum_{\substack{(x, D)=1 \\ 0<x<|D|}} \chi(x)\, x. \tag{3}$$

В обоих случаях χ обозначает характер рассматриваемого поля, определенный в п. 2 § 8 гл. III (формулы (5)).

Отметим несколько теоретико-числовых следствий, вытекающих из теоремы 1. Начнем с формулы (2). Если мы введем в рассмотрение число

$$\eta = \frac{\prod\limits_b \sin \frac{\pi b}{D}}{\prod\limits_a \sin \frac{\pi a}{D}}, \tag{4}$$

где a и b пробегают натуральные числа из промежутка $(0, D/2)$, взаимно простые с D, удовлетворяющие соответственно условиям $\chi(a) = +1$ и $\chi(b) = -1$, то эту формулу можно будет переписать в виде $\varepsilon^h = \eta$. Отсюда следует, что η — единица нашего квадратичного поля, причем $\eta > 1$ (так как $\varepsilon > 1$). Таким образом, имеет место следующая неожиданная теорема.

Теорема 2. *Для вещественного квадратичного поля K с дискриминантом D и с характером χ число η вида (4) принадлежит этому полю K, является в нем единицей и связано с основной единицей $\varepsilon > 1$ соотношением $\varepsilon^h = \eta$, где h — число классов дивизоров поля K.*

Несмотря на всю простоту формулировки, теорема 2 до сих пор не доказана элементарными средствами. Более того, чисто арифметическим путем не удается доказать даже, что $\eta > 1$. А между тем из неравенства $\eta > 1$ можно извлечь некоторые выводы о распределении квадратичных вычетов по простому модулю $p \equiv 1 \pmod 4$. Действительно, для квадратичного поля $\mathbb{Q}(\sqrt{p})$ дискриминант равен p, а характер $\chi(x)$ совпадает с символом Лежандра $\left(\frac{x}{p}\right)$. Мы имеем поэтому неравенство

$$\prod_b \sin \frac{\pi b}{p} > \prod_a \sin \frac{\pi a}{p},$$

в котором a и b пробегают соответственно все квадратичные вычеты и невычеты по модулю p из промежутка $(0, p/2)$. В силу монотонности функции $\sin x$ на промежутке $(0, \pi/2)$ из этого неравенства следует, что все значения $\pi b/p$ «в среднем» больше значений $\pi a/p$, т. е. что квадратичные вычеты по модулю p «тяготеют» к началу промежутка $(0, p/2)$, а невычеты — к концу (общее число вычетов и невычетов на промежутке $(0, p/2)$ при $p \equiv 1 \pmod 4$, очевидно, одинаково).

Более определенные сведения о распределении квадратичных вычетов можно получить для простых чисел $p \equiv 3 \pmod 4$, если рассмотреть формулу (3) для поля $\mathbb{Q}(\sqrt{-p})$.

Займемся сначала преобразованием формулы (3) к несколько более простому виду в общем случае. В ближайших выкладках мы положим $|D| = m$.

Предположим сначала, что m четно. Простая проверка показывает (задача 9), что в этом случае $\chi\left(x+\frac{m}{2}\right) = -\chi(x)$, и формула (3) дает нам

$$hm = -\sum_{0<x<\frac{m}{2}} \chi(x)\, x - \sum_{0<x<\frac{m}{2}} \chi\left(x+\frac{m}{2}\right)\left(x+\frac{m}{2}\right) =$$

$$= -\sum_{0<x<\frac{m}{2}} \chi(x)\, x + \sum_{0<x<\frac{m}{2}} \chi(x)\left(x+\frac{m}{2}\right) = \frac{m}{2} \sum_{0<x<\frac{m}{2}} \chi(x),$$

откуда $h = \frac{1}{2} \sum_{0<x<m/2} \chi(x)$. Заметим, что условие четности m равносильно равенству $\chi(2) = 0$.

Пусть теперь m нечетно. Так как характер χ мнимого квадратичного поля нечетный, т. е. $\chi(-1) = -1$ (как уже отмечалось, это будет доказано в следующем пункте, теорема 6), то из (3) получаем

$$hm = -\sum_{0<x<m/2} \chi(x)\, x - \sum_{0<x<m/2} \chi(m-x)(m-x) =$$

$$= -2 \sum_{0<x<m/2} \chi(x)\, x + m \sum_{0<x<m/2} \chi(x). \quad (5)$$

С другой стороны,

$$hm = -\sum_{\substack{0<x<m \\ x \text{ четное}}} \chi(x)\, x - \sum_{\substack{0<x<m \\ x \text{ четное}}} \chi(m-x)(m-x) =$$

$$= -4 \sum_{0<x<m/2} \chi(2x)\, x + m \sum_{0<x<m/2} \chi(2x).$$

откуда

$$hm\chi(2) = -4 \sum_{0<x<m/2} \chi(x)\, x + m \sum_{0<x<m/2} \chi(x). \quad (6)$$

Исключая сумму $\sum \chi(x)\, x$ из (5) и (6), приходим к равенству

$$h(2-\chi(2)) = \sum_{0<x<m/2} \chi(x).$$

Так как это равенство справедливо, как показано выше, и для четных m (поскольку $\chi(2) = 0$ при $2 \mid m$), то нами получена следующая теорема.

Теорема 3. *Для числа классов дивизоров мнимого квадратичного поля с дискриминантом $D<-4$ и с характером χ справедлива формула*

$$h=\frac{1}{2-\chi(2)}\sum_{\substack{0<x<|D|/2\\(x,D)=1}}\chi(x). \tag{7}$$

Применим теорему 3 к случаю поля $\mathbb{Q}(\sqrt{-p})$, где p — простое число вида $4n+3$. Так как $-p\equiv 1 \pmod 4$, то, следовательно, в этом случае $D=-p$ и значение характера $\chi(x)$ совпадает с символом Лежандра $\left(\frac{x}{p}\right)$. Замечая, что число слагаемых в сумме $\sum_{0<x<p/2}\left(\frac{x}{p}\right)$ нечетно $\left(\frac{p-1}{2}=2n+1\right)$, а потому и сама сумма нечетна, а также, что $\chi(2)=1$, если $p\equiv 7 \pmod 8$, и $\chi(2)=-1$, если $p\equiv 3 \pmod 8$, мы получаем из теоремы 3 следующий результат.

Теорема 4. *Для простого числа p вида $4n+3$ число классов дивизоров поля $\mathbb{Q}(\sqrt{-p})$ нечетно и равно*

$$h=V-N \qquad \text{при } p\equiv 7 \pmod 8,$$

$$h=\frac{1}{3}(V-N) \quad \text{при } p\equiv 3 \pmod 8, \quad p\neq 3,$$

где V — число квадратичных вычетов по модулю p, содержащихся в промежутке $(0, p/2)$, а N — число невычетов из того же промежутка.

Из теоремы 4 очевидным образом вытекает, что $V>N$. Таким образом, для простого модуля p вида $4n+3$ на промежутке $(0, p/2)$ число квадратичных вычетов больше числа невычетов (на число, делящееся на 3, если только $p\equiv 3 \pmod 8$, $p\neq 3$).

Полученное утверждение, несмотря на свою простоту, принадлежит к числу глубоких фактов теории чисел. Оно нами получено как простое следствие того, что число h по своему смыслу положительно и, значит, выражение, стоящее в правой части формулы (7), также положительно. Однако знак этого выражения определяется в конечном итоге знаком гауссовой суммы $\tau_1(\chi)$, а в п. 3 мы увидим, что определение знака $\tau_1(\chi)$ представляет собой весьма трудную задачу.

Формула для числа h мнимых квадратичных полей в случае $D\not\equiv 1 \pmod 8$ может быть доказана чисто арифметическим путем. Это доказательство найдено Б. А. Венковым. Оно основано на теории представлений бинарных форм суммой трех квадратов линейных форм и на тонких свойствах непрерывных дробей (см. [42]). В случае же мнимых полей с $D\equiv 1 \pmod 8$ (как и в случае вещественных полей) чисто арифметический вывод формулы для h до сих пор не получен. Не существует также элементарного доказательства того факта, что для простого модуля p вида $8n+7$

в промежутке $(0, p/2)$ содержится больше квадратичных вычетов, чем невычетов.

Замечание 1. Элементарными средствами можно доказать (задача 7), что для простого $p = 8n+7$ в промежутке $(0, p/2)$ содержится одинаковое число нечетных квадратичных вычетов и нечетных невычетов. В силу этого для числа h поля $\mathbb{Q}(\sqrt{-p})$, $p \equiv 7 \pmod 8$, имеем также формулу $h = V^* - N^*$, где V^* и N^* — соответственно число четных квадратичных вычетов и невычетов $\bmod p$, содержащихся в $(0, p/2)$.

Замечание 2. В конце § 3 был сформулирован аналог гипотезы Римана для L-рядов: $L(s, \chi) \neq 0$ при вещественных $s > 1/2$. Если χ — квадратичный характер, то его значения $\chi(n)$ вещественны, и поэтому $L(s, \chi)$ — вещественная непрерывная функция от вещественного аргумента $s > 0$ (следствие леммы 4 § 2). Полученная нами в п. 1 формула, выражающая число h квадратичного поля через $L(1, \chi)$, показывает, что $L(1, \chi) > 0$. Гипотеза для L-рядов приобретает, следовательно, вид: $L(s, \chi) > 0$ при $s > 1/2$. Это утверждение (если только оно справедливо) выражает свойство квадратичных вычетов скапливаться больше к началу промежутка $(0, |D|)$ (аналогично свойству, вытекающему из теоремы 4).

2. Характер квадратичного поля. Докажем здесь все те утверждения о характере квадратичного поля, которыми мы пользовались в п. 1.

Теорема 5. *Характер χ (по модулю $|D|$) квадратичного поля с дискриминантом D примитивен.*

Доказательство. В силу теоремы 4 § 5 Дополнения нам достаточно показать, что для любого простого числа p, входящего в D, существует такое x, что $(x, D) = 1$, $x \equiv 1 \left(\bmod \frac{|D|}{p}\right)$ и $\chi(x) = -1$. Рассмотрим сначала случай $p \neq 2$. Выберем какой-нибудь квадратичный невычет s по модулю p и найдем целое x из системы сравнений

$$x \equiv s \pmod p, \qquad x \equiv 1 \left(\bmod \frac{2|D|}{p}\right).$$

Пользуясь формулами (5) § 8 гл. III, легко устанавливаем, что во всех случаях $\chi(x) = \left(\frac{x}{p}\right) = \left(\frac{s}{p}\right) = -1$.

Пусть теперь $p = 2$. Если $d \equiv 3 \pmod 4$, $D = 4d$, то, удовлетворив сравнениям

$$x \equiv 3 \pmod 4, \qquad x \equiv 1 \pmod{2|d|},$$

будем иметь $\chi(x) = (-1)^{(x-1)/2} = -1$. Если же $d = 2d'$, $D = 4d = 8d'$, то для числа x, удовлетворяющего сравнениям

$$x \equiv 5 \pmod 8, \qquad x \equiv 1 \pmod{4|d'|},$$

имеем $\chi(x) = (-1)^{(x^2-1)/8} = -1$.

Примитивность характера χ доказана.

Теорема 6. *Характеры вещественных квадратичных полей все четные, а мнимых квадратичных полей — все нечетные.*

Доказательство. Пусть χ — характер квадратичного поля $\mathbb{Q}(\sqrt{d})$. Вычислим $\chi(-1)$, пользуясь формулами (5) § 8 гл. III. Если $d \equiv 1 \pmod 4$, то

$$\chi(-1) = \left(\frac{-1}{|d|}\right) = (-1)^{\frac{|d|-1}{2}} = (-1)^{\frac{d-1}{2}+\frac{|d|-1}{2}}.$$

Если $d \equiv 3 \pmod 4$, то

$$\chi(-1) = -\left(\frac{-1}{|d|}\right) = -(-1)^{\frac{|d|-1}{2}} = (-1)^{\frac{d-1}{2}+\frac{|d|-1}{2}}.$$

Если, наконец, $d = 2d'$, то

$$\chi(-1) = (-1)^{\frac{d'-1}{2}}\left(\frac{-1}{|d'|}\right) = (-1)^{\frac{d'-1}{2}+\frac{|d'|-1}{2}}.$$

Но для нечетного a имеем

$$\frac{a-1}{2} + \frac{|a|-1}{2} = \begin{cases} a-1 \equiv 0 \pmod 2 & \text{при } a > 0, \\ -1 & \text{при } a < 0. \end{cases}$$

Следовательно, во всех случаях

$$\chi(-1) = \begin{cases} 1 & \text{при } d > 0, \\ -1 & \text{при } d < 0. \end{cases}$$

Теорема 6 доказана.

3. Гауссовы суммы для квадратичных характеров. При выводе формулы для числа классов дивизоров квадратичного поля нами была использована формула для значения нормированной гауссовой суммы $\tau(\chi)$. Напомним, что гауссова сумма $\tau_a(\chi)$ характера χ по модулю m называется нормированной, если в ее определении (см. § 2 п. 4 этой главы) в качестве первообразного корня m-й степени из 1 взят корень $\zeta = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}$. Займемся здесь вычислением значения $\tau(\chi)$.

Согласно теореме 5 характер χ квадратичного поля $\mathbb{Q}(\sqrt{d})$ с дискриминантом D является примитивным числовым характером по модулю $|D|$. Кроме того, он удовлетворяет условию $\chi^2 = \chi_0$, где χ_0 — единичный характер. Последнее, очевидно, равносильно тому, что значениями характера χ являются числа ± 1 (и, конечно, нуль).

Определение. *Неединичный числовой характер χ называется квадратичным, если $\chi^2 = \chi_0$.*

Характерами квадратичных полей исчерпываются, оказывается, вообще все примитивные квадратичные числовые характеры

(по всевозможным модулям). Действительно, согласно задаче 8 примитивные квадратичные характеры существуют лишь для модулей вида r и $4r$ (по одному характеру) и для модулей вида $8r$ (по два характера), где r — нечетное натуральное число, свободное от квадратов (в случае нечетного модуля $r>1$). Совокупность этих модулей совпадает, очевидно, с совокупностью модулей вида $|D|$, где D пробегает дискриминанты всех квадратичных полей. Замечая, что для $|D|=8r$ имеется два квадратичных поля: $\mathbb{Q}(\sqrt{2r})$ и $\mathbb{Q}(\sqrt{-2r})$, а также, что по модулю $8r$ один примитивный квадратичный характер четный, а другой нечетный, мы и получаем, что все квадратичные поля находятся в естественном взаимно однозначном соответствии со всеми примитивными квадратичными числовыми характерами.

Значения гауссовых сумм для примитивных квадратичных характеров определяются следующей теоремой.

Теорема 7. *Пусть χ — примитивный квадратичный характер по модулю m. Тогда для нормированной гауссовой суммы $\tau_1(\chi)=\tau(\chi)$ имеем:*

$$\tau(\chi)=\begin{cases}\sqrt{m}, & \text{если } \chi(-1)=1;\\ i\sqrt{m}, & \text{если } \chi(-1)=-1.\end{cases}$$

Доказательство. Мы ограничимся здесь полным доказательством теоремы 7 лишь для простого нечетного модуля p, так как именно этот случай содержит главные принципиальные трудности. Переход от простого нечетного к произвольному модулю осуществляется уже сравнительно легко. В конце доказательства мы укажем на основные моменты этого перехода.

Итак, пусть p — простое нечетное и $\zeta=\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}$. Так как неединичный квадратичный характер χ по модулю p совпадает с символом Лежандра $\left(\frac{x}{p}\right)$ (задача 4 § 2 гл. I), то, следовательно, для нормированной гауссовой суммы $\tau(\chi)$ мы имеем представление

$$\tau(\chi)=\sum_x{}'\left(\frac{x}{p}\right)\zeta^x$$

(штрих у суммы означает, что x пробегает приведенную систему вычетов по модулю p). Найдем комплексно сопряженное число $\overline{\tau(\chi)}$. Так как $\overline{\zeta}=\zeta^{-1}$, то

$$\overline{\tau(\chi)}=\sum_x{}'\left(\frac{x}{p}\right)\zeta^{-x}=\sum_x{}'\left(\frac{-x}{p}\right)\zeta^x=\left(\frac{-1}{p}\right)\tau(\chi). \tag{8}$$

С другой стороны, согласно теореме 4 § 2 гл. I

$$\overline{\tau(\chi)}\tau(\chi)=p. \tag{9}$$

Из равенств (8) и (9) следует теперь, что

$$\tau(\chi)^2 = \left(\frac{-1}{p}\right) p = (-1)^{(p-1)/2} p,$$

а значит,

$$\tau(\chi) = \begin{cases} \pm\sqrt{p}, & \text{если } p \equiv 1 \pmod 4, \\ \pm i\sqrt{p}, & \text{если } p \equiv 3 \pmod 4. \end{cases} \tag{10}$$

Для завершения доказательства теоремы 7 (при $m = p$), казалось бы, остается совсем немного: надо только определить знак при $\sqrt{p}$ и $i\sqrt{p}$. Однако именно в определении этого знака и лежит вся трудность доказательства.

Преобразуем сумму $\tau(\chi)$ к несколько другому виду. Пусть a пробегает все квадратичные вычеты по модулю p, а b — все невычеты. Тогда, очевидно,

$$\tau(\chi) = \sum_a \zeta^a - \sum_b \zeta^b.$$

Но $1 + \sum_a \zeta^a + \sum_b \zeta^b = 0$, поэтому

$$\tau(\chi) = 1 + 2\sum_a \zeta^a.$$

Если x пробегает значения $0, 1, \ldots, p-1$, то x^2 будет пробегать по модулю p значение 0 и все квадратичные вычеты, каждый ровно по два раза. В силу этого гауссову сумму $\tau(\chi)$ мы можем записать также в виде

$$\tau(\chi) = \sum_{x=0}^{p-1} \zeta^{x^2}. \tag{11}$$

Введем в рассмотрение матрицу

$$A = (\zeta^{xy})_{0 \leqslant x,y \leqslant p-1} = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \zeta & \zeta^2 & \ldots & \zeta^{p-1} \\ 1 & \zeta^2 & \zeta^4 & \ldots & \zeta^{2(p-1)} \\ \cdot & \cdot & \cdot & \ldots & \cdot \\ 1 & \zeta^{p-1} & \zeta^{2(p-1)} & \ldots & \zeta^{(p-1)^2} \end{pmatrix}.$$

Ввиду формулы (11) гауссова сумма $\tau(\chi)$ совпадает со следом этой матрицы A. Если поэтому через $\lambda_1, \ldots, \lambda_p$ мы обозначим ее характеристические числа (с учетом кратностей), то будем иметь

$$\tau(\chi) = \lambda_1 + \ldots + \lambda_p. \tag{12}$$

Вычисление $\tau(\chi)$ свелось, таким образом, к нахождению характеристических чисел матрицы A.

Возведем A в квадрат. Так как

$$\sum_{t=0}^{p-1}\zeta^{xt}\zeta^{ty}=\sum_{t=0}^{p-1}\zeta^{t(x+y)}=\begin{cases}p & \text{при } x+y\equiv 0 \pmod p,\\ 0 & \text{при } x+y\not\equiv 0 \pmod p,\end{cases}$$

то

$$A^2=\begin{pmatrix}p & 0\dots 0\\ 0 & 0\dots p\\ \cdot & \cdot\ \cdot\ \cdot\\ 0 & p\dots 0\end{pmatrix}.$$

Характеристические числа матрицы A^2 совпадают, как известно, с квадратами

$$\lambda_1^2,\ \dots,\ \lambda_p^2 \tag{13}$$

характеристических чисел для A. Но, с другой стороны, характеристический многочлен для A^2 легко может быть вычислен. Он равен $(t-p)^{(p+1)/2}(t+p)^{(p-1)/2}$. Следовательно, в ряде чисел (13) имеется $(p+1)/2$ чисел, равных p, и $(p-1)/2$ чисел, равных $-p$. Отсюда легко получаем, что каждое из λ_k совпадает с одним из чисел $\pm\sqrt{p}$, $\pm i\sqrt{p}$, при этом, если a, b, c и d обозначают кратности характеристических чисел $\sqrt{p}$, $-\sqrt{p}$, $i\sqrt{p}$ и $-i\sqrt{p}$ соответственно, то

$$a+b=(p+1)/2,\qquad c+d=(p-1)/2. \tag{14}$$

Сумму (12) мы можем теперь переписать в виде

$$\tau(\chi)=(a-b+(c-d)i)\sqrt{p}. \tag{15}$$

Сопоставляя это с (10), находим, что

$$\left.\begin{aligned} &a-b=\pm 1,\quad c=d && \text{при } p\equiv 1 \pmod 4,\\ &a=b,\quad c-d=\pm 1 && \text{при } p\equiv 3 \pmod 4.\end{aligned}\right\} \tag{16}$$

Для определения кратностей a, b, c и d нам не хватает еще одного соотношения между ними. Чтобы найти недостающую зависимость, вычислим определитель матрицы A. Так как $\det(A^2)=p^p(-1)^{p(p-1)/2}$, то

$$\det A=\pm i^{p(p-1)/2}p^{p/2}. \tag{17}$$

Определитель $\det A$ является определителем Вандермонда, поэтому, вводя дополнительное обозначение $\eta=\cos\frac{\pi}{p}+i\sin\frac{\pi}{p}$, мы имеем

$$\det A=\prod_{p-1\geqslant r>s\geqslant 0}(\zeta^r-\zeta^s)=\prod_{r>s}\eta^{r+s}(\eta^{r-s}-\eta^{(r-s)})=$$

$$=\prod_{r>s}\eta^{r+s}\prod_{r>s}\left(2i\sin\frac{(r-s)\pi}{p}\right)=i^{p(p-1)/2}2^{p(p-1)/2}\prod_{r>s}\sin\frac{(r-s)\pi}{p},$$

так как

$$\sum_{r>s}(r+s)=\sum_{r=1}^{p-1}\sum_{s=0}^{r-1}(r+s)=\sum_{r=1}^{p-1}\left(r^2+\frac{r(r-1)}{2}\right)=2p\left(\frac{p-1}{2}\right)^2$$

делится на $2p$. Сравним полученное выражение для $\det A$ с (17). Так как $\sin\frac{(r-s)\pi}{p}>0$ при $0\leqslant s<r\leqslant p-1$, то в (17) должен стоять знак плюс. Таким образом, $\det A=i^{p(p-1)/2}p^{p/2}$. С другой стороны, мы имеем

$$\det A=\prod_{k=1}^{p}\lambda_k=(-1)^b\,i^c\,(-i)^d\,p^{p/2}=i^{2b+c-d}p^{p/2}.$$

Оба результата вместе приводят нас к сравнению

$$2b+c-d\equiv p\,\frac{p-1}{2}\pmod 4,$$

из которого, приняв во внимание (14) и (16), выводим

$$a-b=\frac{p+1}{2}-2b\equiv\frac{p+1}{2}-\frac{p-1}{2}=1\pmod 4\text{ при }p\equiv 1\pmod 4,$$

$$c-d\equiv-\frac{p-1}{2}+2b=$$

$$=-\frac{p-1}{2}+\frac{p+1}{2}=1\pmod 4\text{ при }p\equiv 3\pmod 4.$$

Полученные сравнения показывают, что в равенствах (16) разности $a-b$ и $c-d$ равны $+1$, а это ввиду (10) дает нам окончательно:

$$\tau(\chi)=\begin{cases}\sqrt{p} & \text{при } p\equiv 1\pmod 4,\\ i\sqrt{p} & \text{при } p\equiv 3\pmod 4.\end{cases}$$

Доказательство теоремы 7 для случая простого нечетного модуля $m=p$ закончено.

Для доказательства теоремы в общем случае следует воспользоваться утверждением задачи 4 § 2. Эта задача показывает, что нормированная гауссова сумма $\tau(\chi)$ для примитивного квадратичного характера χ по модулю m простым образом выражается через нормированные гауссовы суммы для неединичного характера по модулю 4, двух примитивных характеров по модулю 8 и квадратичных характеров по модулям простых нечетных p. Так как все эти гауссовы суммы нам известны (относительно модулей 4 и 8 см. задачи 10 и 11 настоящего параграфа), то формула упомянутой задачи 4 § 2 позволяет найти явное выражение и для $\tau(\chi)$. Пусть, например, мы имеем характер

$$\chi(x)=(-1)^{\frac{x^2-1}{8}+\frac{x-1}{2}}\left(\frac{x}{r}\right),\qquad (x,2r)=1$$

по модулю $m = 8r$, где r — нечетное натуральное число, свободное от квадратов. Если $r = p_1 \dots p_s$, то для χ имеем разложение

$$\chi(x) = (-1)^{\frac{x^2-1}{8}+\frac{x-1}{2}} \left(\frac{x}{p_1}\right) \dots \left(\frac{x}{p_s}\right).$$

Обозначим через α число тех простых чисел среди $p_1, \dots, p_s$, которые $\equiv 3 \pmod 4$. Тогда

$$\tau(\chi) = 2i\sqrt{2}\, i^{\alpha} \sqrt{r}\, (-1)^{\frac{r^2-1}{8}+\frac{r-1}{2}} \left(\frac{2}{r}\right) \prod_{k \neq j} \left(\frac{p_k}{p_j}\right) =$$

$$= i^{\alpha+1} \sqrt{m}\, (-1)^{\frac{r-1}{2}+C_\alpha^2} = \sqrt{m}\, i^{\alpha+1+2\alpha+\alpha(\alpha-1)} =$$

$$= i^{(\alpha+1)^2} \sqrt{m} = \begin{cases} \sqrt{m}, & \text{если } \chi(-1) = (-1)^{\alpha+1} = 1, \\ i\sqrt{m}, & \text{если } \chi(-1) = (-1)^{\alpha+1} = -1. \end{cases}$$

Аналогичным образом вычисляются суммы $\tau(\chi)$ и для других, примитивных квадратичных характеров.

Приведенное нами доказательство теоремы 7 (для простого модуля) предложено Шуром. Другое доказательство, принадлежащее Кронекеру, содержится в задачах 13—16.

Задачи

1. Зная, что основная единица поля $\mathbb{Q}(\sqrt{5})$ равна $\frac{1+\sqrt{5}}{2} = 2\cos\frac{\pi}{5}$, вычислить число h для этого поля с помощью формулы (2).

2. Вычислить число h для полей $\mathbb{Q}(\sqrt{-5})$ и $\mathbb{Q}(\sqrt{-23})$.

3. Доказать, что произвольное квадратичное поле с дискриминантом D является подполем поля деления круга на $m = |D|$ частей.

4. Пусть p — простое нечетное и ζ — первообразный корень степени p из 1. Доказать, что круговое поле $\mathbb{Q}(\zeta)$ содержит одно и только одно квадратичное подполе. Этим подполем является $\mathbb{Q}(\sqrt{p})$, если $p \equiv 1 \pmod 4$, и $\mathbb{Q}(\sqrt{-p})$, если $p \equiv 3 \pmod 4$. (При решении этой и следующей задач использовать основную теорему теории Галуа.)

5. Независимо от теоремы 2 доказать, что для простого $p \equiv 1 \pmod 4$ число

$$\prod_b \sin\frac{\pi b}{p} \Big/ \prod_a \sin\frac{\pi a}{p},$$

где a и b пробегают соответственно все квадратичные вычеты и невычеты по модулю p из промежутка $(0, p/2)$, является единицей квадратичного поля $\mathbb{Q}(\sqrt{p})$. Доказать, далее, что норма этой единицы равна -1.

6. Используя второе утверждение задачи 5, показать, что число классов дивизоров поля $\mathbb{Q}(\sqrt{p})$, p — простое $\equiv 1 \pmod 4$, нечетно, а также что норма основной единицы этого поля равна -1.

7. Доказать, что для простого модуля p вида $8n+7$ среди нечетных чисел из промежутка $(0, p/2)$ имеется одинаковое число квадратичных вычетов и невычетов.

8. Доказать, что примитивные квадратичные характеры существуют только для модулей m вида r, $4r$ и $8r$, где r нечетное натуральное, свободное от квадратов (в случае нечетного модуля $r > 1$). Показать, далее, что все примитивные квадратичные характеры исчерпываются характерами:

$$\chi(x) = \left(\frac{x}{r}\right), \quad (x, r) = 1, \quad \text{для модуля } r;$$

$$\chi(x) = (-1)^{(x-1)/2}\left(\frac{x}{r}\right), \quad (x, 2r) = 1, \quad \text{для модуля } 4r;$$

$$\left.\begin{aligned} \chi(x) &= (-1)^{(x^2-1)/8}\left(\frac{x}{r}\right), \\ \chi(x) &= (-1)^{\frac{x^2-1}{8}+\frac{x-1}{2}}\left(\frac{x}{r}\right), \end{aligned}\right\} \quad (x, 2r) = 1, \quad \text{для модуля } 8r.$$

9. Доказать, что для любого примитивного квадратичного характера χ по четному модулю m ($= 4r$ или $= 8r$ с нечетным r) справедлива формула $\chi\left(x + \frac{m}{2}\right) = -\chi(x)$.

10. Проверить, что нормированная гауссова сумма для характера $\chi(x) = (-1)^{(x-1)/2}$, $(x, 2) = 1$, по модулю 4 равна $\tau_1(\chi) = 2i$.

11. Проверить, что для примитивных характеров

$$\chi'(x) = (-1)^{(x^2-1)/8}$$

и

$$\chi''(x) = (-1)^{\frac{x^2-1}{8}+\frac{x-1}{2}} \quad (2 \nmid x) \text{ по модулю } 8$$

нормированные гауссовы суммы равны $\tau_1(\chi') = 2\sqrt{2}$ и $\tau_1(\chi'') = 2i\sqrt{2}$.

12. Провести доказательство теоремы 7 для произвольного модуля.

13. Пусть p — простое нечетное число и $\zeta = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$. Положим $\delta = \prod_{x=1}^{(p-1)/2}(\zeta^x - \zeta^{-x})$. Доказать, что $\delta^2 = (-1)^{(p-1)/2}p$.

Таким образом, δ^2 совпадает с квадратом τ^2 гауссовой суммы $\tau = \sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\zeta^x$.

14. В тех же обозначениях показать, что

$$\left(\frac{-2}{p}\right)\delta = \begin{cases} \sqrt{p} & \text{при } p \equiv 1 \pmod 4, \\ i\sqrt{p} & \text{при } p \equiv 3 \pmod 4. \end{cases}$$

Далее, полагая $\lambda = 1 - \zeta$, доказать, что в порядке $\mathbb{Z}[\zeta]$ справедливо сравнение

$$\left(\frac{-2}{p}\right)\delta \equiv \left(\frac{p-1}{2}\right)!\,\lambda^{(p-1)/2} \pmod{\lambda^{(p+1)/2}}.$$

15. Доказать, что в кольце $\mathbb{Z}[\zeta]$ имеет место сравнение

$$\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\zeta^x = \tau \equiv \left(\frac{p-1}{2}\right)!\,\lambda^{(p-1)/2} \pmod{\lambda^{(p+1)/2}}.$$

Указание. Разложить сумму $\sum_{x=1}^{p-1} x^{(p-1)/2}(1-\lambda)^x$ по степеням λ и воспользоваться тем, что

$$\sum_{x=1}^{p-1} x^m \equiv \begin{cases} 0 \pmod p & \text{при } 0 < m < p-1, \\ -1 \pmod p & \text{при } m = p-1. \end{cases}$$

16. Основываясь на двух предшествующих задачах, показать, что

$$\tau = \begin{cases} \sqrt{p} & \text{при } p \equiv 1 \pmod 4, \\ i\sqrt{p} & \text{при } p \equiv 3 \pmod 4. \end{cases}$$

17. В линейном пространстве размерности p над полем комплексных чисел рассмотрим линейный оператор T, матрица которого в базисе $e_0, e_1, \ldots, e_{p-1}$ равна $A = (\zeta^{xy})_{0 \leqslant x,\, y \leqslant p-1}$. Обозначим через χ_0 единичный и через χ_* квадратичный характеры по модулю p. Все остальные (невещественные) характеры по модулю p разбиваются на пары сопряженных друг с другом характеров $\chi_i, \bar{\chi}_i$ $(i = 1, \ldots, r = (p-3)/2)$. Для каждого числового характера χ по модулю p положим $a(\chi) = \sum_{x=1}^{p-1} \chi(x) e_x$. Показать, что $T(a(\chi)) = \tau(\chi) a(\bar{\chi})$, если $\chi \neq \chi_0$ и $T(a(\chi_0)) = (p-1)e_0 - a(\chi_0)$. Найти матрицу оператора T в базисе

$$e_0,\ a(\chi_0),\ a(\chi_*),\ a(\chi_1),\ a(\bar{\chi}_1),\ \ldots,\ a(\chi_r),\ a(\bar{\chi}_r).$$

Показать, далее, что

$$\det A = (-1)^{(p-1)/2} \tau(\chi_*)\, p^{(p-1)/2} \prod_{i=1}^{r} \chi_i(-1)$$

(учесть формулу $\tau(\bar{\chi}) = \chi(-1)\overline{\tau(\chi)}$).

18. Получить теорему 7 (для простого $m = p$), сравнивая значение $\det A$ в задаче 17 с формулой (18).

§ 5. Число классов дивизоров поля деления круга на простое число частей

1. Разложение числа h на два множителя. Полученные нами в § 2 этой главы равенства (16) и (17) дают для числа классов дивизоров m-кругового поля формулу, которая уже не содержит бесконечных рядов и произведений. Все же эта формула оставляет некоторую неудовлетворенность, так как в ней число классов h, являющееся по своему смыслу натуральным числом, выражается через иррациональные и комплексные числа. В настоящем параграфе мы займемся преобразованием формулы для h к более законченному виду, ограничившись, однако, лишь случаем поля деления круга на простое число частей.

Итак, пусть $l = 2m+1$ — простое число и $K = \mathbb{Q}(\zeta)$ — поле деления круга на l частей. Для удобства изложения мы будем здесь считать, что K является подполем поля всех комплексных

чисел, и под ζ понимать корень $\zeta = \cos\frac{2\pi}{l} + i\sin\frac{2\pi}{l}$ (точно фиксированное значение корня ζ необходимо при проведении аналитических выкладок). Вычислим для поля K величины, стоящие перед произведением в формуле (16) § 2. Так как степень $(K:\mathbb{Q})$ равна $l-1$ (следствие теоремы 1 § 2) и все изоморфизмы K в поле комплексных чисел комплексные (здесь они являются на самом деле автоморфизмами поля K), то $s=0$, $t=(l-1)/2=m$. Число w корней из 1, содержащихся в K, по лемме 3 § 1 гл. III равно $2l$. Норма главного дивизора $\mathfrak{l}=(1-\zeta)$ равна $N(\mathfrak{l})=N(1-\zeta)=l$ (см. равенство (5) § 1, гл. III), поэтому дивизор $\mathfrak{l}$ простой, и для числа l согласно лемме 1 § 1 гл. III мы имеем разложение $l=\mathfrak{l}^{l-1}$. Множитель $F(s)$ в формуле (12) § 2, следовательно, равен

$$F(s)=\left(1-\frac{1}{N(\mathfrak{l})^s}\right)^{-1}\left(1-\frac{1}{l^s}\right)=1.$$

Займемся вычислением дискриминанта поля K.

Теорема 1. *Числа* $1, \zeta, \ldots, \zeta^{l-2}$ *образуют фундаментальный базис* l*-кругового поля* $K=\mathbb{Q}(\zeta)$.

Доказательство. Так как при $s\not\equiv 0 \pmod l$ характеристический многочлен числа ζ^s равен $X^{l-1}+X^{l-2}+\ldots+X+1$, то

$$\operatorname{Sp}\zeta^s=\begin{cases}-1, & \text{если } s\not\equiv 0 \pmod l,\\ l-1, & \text{если } s\equiv 0 \pmod l.\end{cases} \tag{1}$$

Пусть

$$\alpha=a_0+a_1\zeta+\ldots+a_{l-2}\zeta^{l-2}, \qquad a_i\in\mathbb{Q},$$

— произвольное целое число из K. Нам надо доказать, что для него все коэффициенты a_i — целые рациональные числа. Так как $\alpha\zeta^{-k}-\alpha\zeta$ целое, то след

$$\operatorname{Sp}(\alpha\zeta^{-k}-\alpha\zeta)=la_k-\sum_{i=0}^{l-2}a_i+\sum_{i=0}^{l-2}a_i=la_k$$

является целым рациональным числом $(0\leqslant k\leqslant l-2)$. Положим $la_k=b_k$, $1-\zeta=\lambda$ и рассмотрим число

$$l\alpha=b_0+b_1\zeta+\ldots+b_{l-2}\zeta^{l-2}=c_0+c_1\lambda+\ldots+c_{l-2}\lambda^{l-2},$$

где вместе с b_k все c_k — также целые рациональные числа. Покажем, что коэффициенты c_k все делятся на l. Если для $c_0, \ldots, c_{k-1}$ $(0\leqslant k<l-2)$ это уже установлено, то мы рассмотрим последнее равенство как сравнение по модулю λ^{k+1} (в кольце целых чисел поля K). Так как $l\equiv 0 \pmod{\lambda^{k+1}}$ (лемма 1 § 1 гл. III), то это сравнение дает нам $c_k\lambda^k\equiv 0 \pmod{\lambda^{k+1}}$, откуда легко следует, что c_k делится на λ, а значит, по лемме 2 § 1 гл. III c_k делится и на l. Таким образом, все коэффициенты c_k делятся на l. Но в таком случае вместе с ними на l должны делиться и все коэффициенты b_k, т. е. все a_k должны быть целыми. Теорема 1 доказана.

Следствие. *Дискриминант l-кругового поля при простом $l>2$ равен* $(-1)^{\frac{l-1}{2}} l^{l-2}$.

Действительно, ввиду формул (1) дискриминант поля K равен определителю

$$\det\left(\mathrm{Sp}\,\zeta^{i+j}\right)_{1\leqslant i,j\leqslant l-1}=\begin{vmatrix} -1 & -1 & \dots & -1 & l-1 \\ -1 & -1 & \dots & l-1 & -1 \\ \dots & \dots & \dots & \dots & \dots \\ -1 & l-1 & \dots & -1 & -1 \\ l-1 & -1 & \dots & -1 & -1 \end{vmatrix}$$

порядка $l-1$ (вместо базиса теоремы 1 здесь взят базис $\zeta, \zeta^2, \dots, \zeta^{l-1}$).

Формулу (16) § 2 для случая l-кругового поля K мы можем теперь переписать в виде

$$h=\frac{l^{l/2}}{2^{m-1}\pi^m \mathrm{R}}\prod_{\chi\neq\chi_0} L(1,\chi), \tag{2}$$

где R — регулятор поля K, $m=(l-1)/2$ и χ пробегает все числовые характеры по модулю l, отличные от единичного характера χ_0.

Так как по формуле (2) все величины, стоящие вне произведения, вещественны и положительны, то эта формула, очевидно, сохранится, если все сомножители $L(1,\chi)$ в произведении мы заменим их модулями $|L(1,\chi)|$.

По простому модулю l все числовые характеры $\neq\chi_0$ примитивны, поэтому при дальнейшем преобразовании выражения для h мы можем воспользоваться теоремой 3 § 2. Выделим для этого отдельно все четные и нечетные характеры. Пусть g — некоторый фиксированный первообразный корень по модулю l и θ — первообразный корень степени $l-1$ из 1. Группа числовых характеров по модулю l циклична и имеет порядок $l-1$. Если через χ мы обозначим тот из характеров по модулю l, для которого $\chi(g)=\theta^{-1}$, то все его степени $\chi, \chi^2, \dots, \chi^{l-1}=\chi_0$ исчерпают собой всю группу характеров по модулю l, при этом все характеры χ^{2k} будут четными, а χ^{2k-1} — нечетными, так как

$$\chi^s(-1)=\chi(g^{(l-1)/2})^s=\theta^{(l-1)s/2}=(-1)^s.$$

Ввиду формулы (20) § 2 и теоремы 4 § 2 гл. I для четных характеров χ^{2k} $(1\leqslant k\leqslant (l-3)/2)$ мы имеем

$$|L(1,\ \chi^{2k})|=$$

$$=\frac{|\tau(\chi^{2k})|}{l}\left|\sum_{r=0}^{l-2}\bar{\chi}^{2k}(g^r)\ln\left|1-\zeta^{g^r}\right|\right|=\frac{1}{\sqrt{l}}\left|\sum_{r=0}^{l-2}\theta^{2kr}\ln\left|1-\zeta^{g^r}\right|\right|.$$

Если мы возьмем $r=\frac{l-1}{2}+s$, где $0\leqslant s<\frac{l-1}{2}=m$, то ввиду

соотношения

$$1-\zeta^{g^{m+s}}=1-\zeta^{-g^s} \tag{3}$$

имеем равенство $\theta^{2k(m+s)}\ln|1-\zeta^{g^{m+s}}|=\theta^{-ks}\ln|1-\zeta^{g^s}|$, а потому

$$|L(1,\chi^{2k})|=\frac{2}{\sqrt{l}}\left|\sum_{r=0}^{m-1}\theta^{2kr}\ln|1-\zeta^{g^r}|\right|.$$

Аналогично формулу (21) § 2 мы можем применить к нечетным характерам χ^{2k-1}. Обозначим через g_s наименьший положительный вычет числа g^s по модулю l. Тогда

$$\sum_{r=1}^{l-1}\overline{\chi}^{2k-1}(r)\,r=\sum_{s=0}^{l-2}\chi^{2k-1}(g^s)^{-1}g_s=\sum_{s=0}^{l-2}g_s\theta^{(2k-1)s}=F\left(\theta^{2k-1}\right),$$

где через F обозначен многочлен $F(X)=\sum_{s=0}^{l-2}g_sX^s$. Следовательно,

$$|L(1,\chi^{2k-1})|=\frac{\pi\sqrt{l}}{l^2}\,|F(\theta^{2k-1})|.$$

Подставляя найденные значения для $|L(1,\chi^{2k})|$, $1\leqslant k\leqslant m-1$, и $|L(1,\chi^{2k-1})|$, $1\leqslant k\leqslant m$, в равенство (2), получаем

$$h=h_0h^*, \tag{4}$$

где нами положено

$$h_0=\frac{2^{m-1}}{\mathrm{R}}\prod_{k=1}^{m-1}\left|\sum_{r=0}^{m-1}\theta^{2kr}\ln|1-\zeta^{g^r}|\right|, \tag{5}$$

$$h^*=\frac{1}{(2l)^{m-1}}\,|F(\theta)F(\theta^3)\ldots F(\theta^{l-2})|. \tag{6}$$

В следующих пунктах мы докажем, что каждое из чисел h_0 и h^* является натуральным числом. Формула (4) дает нам, следовательно, представление числа h в виде произведения двух натуральных множителей.

Замечание 1. Иногда h^* обозначают через h_1, а h_0 — через h_2 и называют их соответственно первым и вторым множителем числа h.

Замечание 2. Множитель h_0 равен числу классов дивизоров подполя $\mathbb{Q}(\zeta+\zeta^{-1})$ степени $(l-1)/2$, состоящего из всех вещественных чисел поля $\mathbb{Q}(\zeta)$ (см. задачи 1—4).

2. Множитель h_0. Введем для краткости записи обозначение

$$a_r=\ln|1-\zeta^{g^r}|,\quad r\geqslant 0.$$

Ввиду равенства (3), справедливого при любом $s\geqslant 0$, мы имеем $a_{m+r}=a_r$. Это значит, что значения a_r зависят лишь от вычета

числа r по модулю $m=(l-1)/2$. Если мы положим

$$A=\prod_{k=1}^{m-1}\left(\sum_{r=0}^{m-1}\theta^{2kr}a_r\right),$$

то формула (5) перепишется в виде

$$h_0=\frac{2^{m-1}}{\mathrm{R}}|A|. \tag{7}$$

Покажем, что произведение $(a_0+a_1+\ldots+a_{m-1})A$ с точностью до знака равно определителю

$$\Delta=\det(a_{i+j})_{0\leqslant i,j\leqslant m-1}=\begin{vmatrix} a_0 & a_1 & \cdots & a_{m-1}\\ a_1 & a_2 & \cdots & a_0\\ \cdots & \cdots & \cdots & \cdots\\ a_{m-1} & a_0 & \cdots & a_{m-2}\end{vmatrix}.$$

Рассмотрим циклическую группу G порядка m, порожденную первообразным корнем θ^2 степени m из 1. Функции χ_k, $0\leqslant k\leqslant m-1$, $\chi_k(\theta^{2r})=\theta^{2rk}$, являются, очевидно, характерами группы G. Определим на группе G функцию f, полагая $f(\theta^{2r})=a_r$. Тогда, согласно задаче 13 § 5 Дополнения, наше произведение примет вид

$$\prod_{k=0}^{m-1}\left(\sum_{r=0}^{m-1}\theta^{2kr}a_r\right)=\prod_{k=0}^{m-1}\left(\sum_{r=0}^{m-1}\chi_k(\theta^{2r})f(\theta^{2r})\right)=$$

$$=\det\left(f(\theta^{2(i-j)})\right)=\det(a_{i-j})_{0\leqslant i,j\leqslant m-1}.$$

Замечая, что матрицы (a_{i-j}) и (a_{i+j}) отличаются между собой лишь расположением столбцов, мы и приходим к желаемому результату.

Сумма $a_0+a_1+\ldots+a_{m-1}$ отлична от нуля, так как

$$a_0+a_1+\ldots+a_{m-1}=\ln\left|\prod_{r=0}^{m-1}(1-\zeta^{g^r})\right|=\ln\sqrt{l} \tag{8}$$

ввиду соотношения (5) § 1 гл. III и формулы (3). Если поэтому в определителе Δ мы выделим множитель (8), то, сократив на него, получим новое выражение для A. Прибавив в Δ все столбцы к какому-нибудь одному, мы получим столбец, все элементы которого равны сумме (8). Следовательно, с точностью до знака выражение A равно определителю Δ', получающемуся из Δ заменой одного его столбца на единицы. Если теперь в Δ' мы вычтем первую строчку из остальных, то этим докажем, что модуль $|A|$ равен абсолютной величине любого из миноров порядка $m-1$ матрицы

$$(a_{i+j}-a_j)_{\substack{1\leqslant i\leqslant m-1\\ 0\leqslant j\leqslant m-1}}. \tag{9}$$

Рассмотрим первообразный корень

$$\eta = -\zeta^{(l+1)/2} = \cos\frac{\pi}{l} + i\sin\frac{\pi}{l}$$

степени $2l$ из 1. Так как $\eta^2 = \zeta$, то

$$\frac{1-\zeta^k}{1-\zeta} = \eta^{k-1}\frac{\eta^k - \eta^{-k}}{\eta - \eta^{-1}} = \eta^{k-1}\frac{\sin(k\pi/l)}{\sin(\pi/l)}.$$

При $k \not\equiv 0 \pmod l$ отношение слева является единицей поля K (см. доказательство леммы 1 § 1 гл. III); следовательно, числа

$$\theta_k = \frac{\sin(k\pi/l)}{\sin(\pi/l)} \tag{10}$$

при всех $k \not\equiv 0 \pmod l$ также являются единицами в K. Эти единицы, очевидно, вещественны и при $1 \leqslant k < l$ положительны.

Для поля K мы имеем $m = (l-1)/2$ пар комплексных изоморфизмов в поле комплексных чисел. Поскольку среди чисел ζ, ζ^g, ..., $\zeta^{g^{m-1}}$ нет сопряженных, то изоморфизмы

$$\sigma_j\colon\ \zeta \to \zeta^{g^j},\quad j = 0, 1, \ldots, m-1,$$

попарно не сопряжены (для каждого σ_j сопряженным будет изоморфизм $\zeta \to \zeta^{-g^j} = \zeta^{g^{m+j}}$).

Обозначим через $\bar r$ абсолютную величину абсолютно наименьшего вычета числа g^r по модулю l. Тогда

$$(1-\zeta^{g^r})/(1-\zeta) = \pm\,\eta^{g^r-1}\theta_{\bar r}.$$

Подвергая это равенство действию автоморфизма σ_j, мы получим

$$(1-\zeta^{g^{r+j}})/(1-\zeta^{g^j}) = \pm\,(\sigma_j\eta)^{g^r-1}\,\sigma_j(\theta_{\bar r}),$$

откуда, переходя к модулям и логарифмируя, находим, что

$$a_{r+j} - a_j = \ln\left|\sigma_j(\theta_{\bar r})\right|. \tag{11}$$

Покажем, что когда r принимает значения 1, ..., $m-1$, то $\bar r$ пробегает числа 2, ..., m. В самом деле, если $g^i \equiv \pm g^j \pmod l$, $1 \leqslant i \leqslant j \leqslant m-1$, то $g^{j-i} \equiv \pm 1 \pmod l$ и $0 \leqslant j-i \leqslant (l-3)/2$, а это возможно лишь при $j-i=0$. Отсюда следует, что все значения $\bar r$ попарно различны, а так как они удовлетворяют неравенству $2 \leqslant \bar r \leqslant m = (l-1)/2$ и число их равно $m-1$, то каждое из чисел 2, ..., m является некоторым $\bar r$.

В силу равенства (11), мы получаем, таким образом, что матрица (9) отличается от матрицы

$$\left(\ln\left|\sigma_j(\theta_k)\right|\right)_{\substack{2<k\leqslant m\\ 0<j<m-1}} \tag{12}$$

лишь расположением строчек, а значит, модуль $|A|$ равен также абсолютной величине любого из миноров порядка $m-1$ матрицы (12).

Обратимся теперь к системе основных единиц поля K. Согласно лемме 4 § 1 гл. III всякая единица поля K является произведением степени ζ на вещественную единицу. В силу этого основные единицы $\varepsilon_1, \ldots, \varepsilon_{m-1}$ мы можем выбрать вещественными и положительными. Ясно, что тогда всякая вещественная положительная единица представляется в виде $\varepsilon_1^{c_1} \ldots \varepsilon_{m-1}^{c_{m-1}}$ с целыми рациональными c_i. Рассматривавшиеся нами в п. 3 § 3 гл. II функции $l_j(\alpha)$, $\alpha \in K$, в данном случае имеют вид $l_j(\alpha) = \ln|\sigma_j(\alpha)|^2 = 2\ln|\sigma_j(\alpha)|$, $0 \leqslant j \leqslant m-1$. Составим для основных единиц $\varepsilon_1, \ldots, \varepsilon_{m-1}$ матрицу

$$(\ln|\sigma_j(\varepsilon_i)|)_{\substack{1 \leqslant i \leqslant m-1 \\ 0 \leqslant j \leqslant m-1}}. \tag{13}$$

Так как матрица (6) § 4 гл. II получается из (13) умножением всех строчек на 2, то по определению регулятора R абсолютная величина любого из миноров порядка $m-1$ матрицы (13) равна $R/2^{m-1}$.

Все единицы θ_k вида (10) при $k = 2, \ldots, m$ вещественны и положительны, поэтому их выражения через основные единицы имеют вид $\theta_k = \prod_{i=1}^{m-1} \varepsilon_i^{c_{ki}}$, $k = 2, \ldots, m$, с целыми рациональными c_{ki}. В силу равенств $\ln|\sigma_j(\theta_k)| = \sum_{i=1}^{m-1} c_{ki} \ln|\sigma_j(\varepsilon_i)|$ матрица (12) является произведением матрицы (c_{ki}) на матрицу (13). Отсюда следует, что каждый минор порядка $m-1$ матрицы (12) равен произведению $\det(c_{kj})$ на соответствующий минор матрицы (13), а значит, $|A| = |\det(c_{kj})| R/2^{m-1}$. Сопоставляя это с равенством (7), получаем окончательно

$$h_0 = |\det(c_{kj})|.$$

Так как все c_{kj} целые рациональные и $h_0 \neq 0$, то этим доказано, что h_0 — натуральное число. Более того, ввиду леммы 1 § 6 гл. II мы получили также следующий результат.

Теорема 2. *Множитель h_0 числа классов дивизоров l-кругового поля K равен индексу $(E : E_0)$ группы E_0, порожденной единицами*

$$\theta_k = \frac{\sin(k\pi/l)}{\sin(\pi/l)}, \qquad k = 2, \ldots, \frac{l-1}{2},$$

поля K, в группе E всех вещественных положительных единиц поля K.

В связи с замечанием 2 в конце п. 1 этот результат интересно сопоставить с теоремой 2 предшествующего параграфа.

Замечание. Доказанная нами теорема 2, несмотря на свое изящество, мало пригодна для фактического вычисления числа h_0. Дело в том, что для вычисления индекса $(E : E_0)$ необходимо знать систему основных единиц поля $K_0 = \mathbb{Q}(\zeta + \zeta^{-1})$, а ее нахождение при больших l является трудно осуществимой задачей даже для современных вычислительных машин. В силу этого информацию о $h_0(l)$ приходится извлекать, используя косвенные соображения. Известно [105], например, что если L — подполе поля K_0, то $h(L)$ — делитель числа $h(K_0)$. Пользуясь этим утверждением, мы можем в отдельных случаях доказать, что $h_0 > 1$. Так, число классов дивизоров вещественного квадратичного поля $\mathbb{Q}(\sqrt{257})$ равно 3 (см. замечание 1 к табл. 3 в конце книги), поэтому согласно задаче 4 § 4 число $h_0(257)$ делится на 3 (этот факт был известен еще Куммеру). Другое соображение основано на оценке снизу для дискриминантов полей данной степени (см. [113], [114]). Именно, зная оценки снизу для дискриминантов вполне вещественных полей в зависимости от степени, можно указать для некоторых малых степеней оценку сверху для числа классов h данного вполне вещественного поля. Индивидуальное просеивание возможных значений для h (с привлечением известных общих теорем) позволяет в ряде случаев найти точное значение для h. Этот подход развит в работе [105]. К сожалению, он применим лишь для небольшого числа полей небольших степеней.

В [105] установлено, что $h_0(l) = 1$ для всех нечетных простых $l \leqslant 67$. Получен также следующий условный результат. Пусть H — гильбертово поле классов над K, т. е. максимальное абелево неразветвленное расширение поля K. В [102] доказано, что $h_0(l) = 1$ для $71 \leqslant l \leqslant 157$ и $h_0(163) = 4$ при условии, что для поля H справедлива обобщенная гипотеза Римана о нулях дзета-функции Дедекинда $\zeta_H(s)$.

Вандивер выдвинул гипотезу, что $h_0(l)$ никогда не делится на l. Сейчас справедливость этой гипотезы проверена [142] для всех простых $l < 125\,000$ (на основе критерия Вандивера, см. конец п. 1 § 7 гл. V). Долгое время предполагалось, что для всех l справедливо неравенство $h_0(l) < l$. Если бы это было так, то справедливость гипотезы Вандивера вытекала бы отсюда тривиальным образом. Однако в последнее время [121] найдено простое число $l = 11\,290\,018\,777$, для которого $h_0(l) > l$. Именно, так как $l \equiv 1 \pmod 4$, то $\mathbb{Q}(\sqrt{l})$ содержится в l-круговом поле. Число классов дивизоров этого вещественного квадратичного подполя равно $2685 = 3 \cdot 5 \cdot 179$. Далее, $l \equiv 1 \pmod 3$, поэтому l-круговое поле содержит циклическое кубическое подполе. В [121] удалось вычислить число классов этого кубического поля, и оно оказалось равным $6\,209\,212 = 4 \cdot 223 \cdot 6961$. Согласно сказанному выше для нашего l число $h_0(l)$ делится на $2685 \cdot 6\,209\,212$.

3. Множитель h^*. Докажем, что число h^*, определяемое равенством (6), также является натуральным числом. Произведение $B = F(\theta)F(\theta^3)\ldots F(\theta^{l-2})$ является, с одной стороны, целым алгебраическим числом поля $\mathbb{Q}(\theta)$, где θ — первообразный корень степени $l-1$ из 1. С другой стороны, оно рационально, так как ввиду (4) и (6) $|B| = \frac{h}{h_0}(2l)^{m-1}$. Следовательно, B целое рациональное, и нам остается проверить, что B делится на 2^{m-1} и на l^{m-1} (по условию $l \neq 2$). Проверим сначала первое.

Как и в п. 1, через g_s мы обозначаем наименьший положительный вычет числа g^s по модулю l, где g — фиксированный первообразный корень по модулю l. Так как

$$g_{m+s} + g_s \equiv g^{m+s} + g^s = g^s(g^{(l-1)/2} + 1) \equiv 0 (\mathrm{mod}\, l),$$

то $g_{m+s} + g_s = l$. Отсюда следует, что числа g_{m+s} и g_s разной четности. Будем рассматривать в кольце целых чисел поля $\mathbb{Q}(\theta)$ сравнения по модулю 2. Ввиду равенства $\theta^m = -1$ при нечетном k мы имеем

$$F(\theta^k) = \sum_{s=0}^{m-1} (g_s\theta^{ks} + g_{m+s}\theta^{k(m+s)}) = \sum_{s=0}^{m-1} (g_s - g_{m+s})\,\theta^{ks} \equiv \sum_{s=0}^{m-1} \theta^{ks} (\mathrm{mod}\, 2),$$

откуда $F(\theta^k)(1-\theta^k) \equiv 0 (\mathrm{mod}\, 2)$. Это показывает, что произведение

$$B(1-\theta)(1-\theta^3)\ldots(1-\theta^{l-2})$$

делится на 2^m. С другой стороны, так как θ и θ^2 — первообразные корни степени $l-1$ и $(l-1)/2$ соответственно, то

$$l-1 = \prod_{k=1}^{l-2}(1-\theta^k), \quad \frac{l-1}{2} = \prod_{s=1}^{m-1}(1-\theta^{2s}),$$

откуда $(1-\theta)(1-\theta^3)\ldots(1-\theta^{l-2}) = 2$.

Этим и доказано, что B делится на 2^{m-1}.

Для доказательства делимости B на l^{m-1} найдем сначала разложение числа l на простые дивизоры поля $\mathbb{Q}(\theta)$. Так как l взаимно просто с $l-1$ и $l \equiv 1 (\mathrm{mod}\, l-1)$, то по теореме 2 § 2 число l раскладывается в произведение $\varphi(l-1)$ различных простых дивизоров, причем норма каждого из них равна l. Пусть $\mathfrak{q}$ — один из этих простых дивизоров. Числа 0, 1, θ, ..., θ^{l-2} попарно несравнимы по модулю $\mathfrak{q}$ (см. доказательство леммы 3 § 2), поэтому они образуют полную систему вычетов по модулю $\mathfrak{q}$. Ввиду сравнения

$$1 - g^{l-1} = \prod_{k=0}^{l-2}(1-\theta^k g) \equiv 0 \ (\mathrm{mod}\, l) \qquad (14)$$

$\mathfrak{q}$ должно быть делителем некоторой разности $1-\theta^k g$. Если $1-\theta^k g \equiv 0 \pmod{\mathfrak{q}}$ и $1-\theta^s g \equiv 0 \pmod{\mathfrak{q}}$, то $\theta^k \equiv \theta^s \pmod{\mathfrak{q}}$, а значит, $\theta^k = \theta^s$. Таким образом, $\mathfrak{q}$ является делителем одной и только одной разности $1-\theta^k g$ из разложения (14). Покажем, что k здесь взаимно просто с $l-1$. Если $(k, l-1) = d$, то, возводя сравнение $1 \equiv \theta^k g \pmod{\mathfrak{q}}$ в степень $(l-1)/d$, мы получим, что $g^{(l-1)/d} - 1$ делится на $\mathfrak{q}$, а значит, делится и на l. Последнее же возможно только при $d = 1$.

Если целое $\alpha \in \mathbb{Q}(\theta)$ делится на $\mathfrak{q} \mid l$, то $N(\alpha)$ делится на $N(\mathfrak{q}) = l$. Обратно, из делимости $N(\alpha)$ на l следует, что α делится хоть на один из простых дивизоров, входящих в l. Все $\varphi(l-1)$ разностей $1-\theta^k g$, для которых k взаимно просто с $l-1$, имеют, очевидно, одну и ту же норму, и эта норма делится на l, поэтому каждая из этих разностей делится на некоторый простой дивизор, входящий в l.

Мы доказали, таким образом, что при любом k, взаимно простом с $l-1$, существует, и притом только один, простой дивизор, делящий l (обозначим его через $\mathfrak{q}_k$), для которого

$$1 - \theta^k g \equiv 0 \pmod{\mathfrak{q}_k}, \tag{15}$$

а также что для всех s, не взаимно простых с $l-1$, разность $1-\theta^s g$ не делится ни на один из простых дивизоров $\mathfrak{q}_k$. Разложение числа l в поле $\mathbb{Q}(\theta)$ мы можем записать в виде

$$l = \prod_{(k, l-1)=1} \mathfrak{q}_k,$$

где k пробегает приведенную систему вычетов по модулю $l-1$.

Вернемся к вопросу о делимости числа B на l^{m-1}. Так как в кольце целых чисел поля $\mathbb{Q}(\theta)$ имеет место сравнение

$$F(\theta^k)(1-g\theta^k) \equiv \sum_{s=0}^{l-2} (g\theta^k)^s (1-g\theta^k) =$$

$$= 1 - (g\theta^k)^{l-1} = 1 - g^{l-1} \equiv 0 \pmod{l},$$

то $F(\theta^k)(1-g\theta^k)$ делится на l. По доказанному отсюда следует, что $F(\theta^k)$ делится на l при $(k, l-1) > 1$ и делится на $l\mathfrak{q}_k^{-1}$ при $(k, l-1) = 1$. Условимся при $(k, l-1) > 1$ под $\mathfrak{q}_k$ понимать единичный дивизор. Тогда можно будет сказать, что $F(\theta^k)$ делится на $l\mathfrak{q}_k^{-1}$ при любом k. Произведение $B = F(\theta)F(\theta^3)\ldots F(\theta^{l-2})$ делится, следовательно, на

$$l^m \prod_{k=1,3,\ldots,l-2} \mathfrak{q}_k^{-1} = l^m \prod_{(k, l-1)=1} \mathfrak{q}_k^{-1} = l^{m-1},$$

и тот факт, что h^* есть целое число, доказан.

Замечание. Явные формулы, полученные нами для чисел h классов дивизоров круговых и квадратичных полей естественно приводят к вопросу: для каких полей алгебраических чисел k имеют место аналогичные формулы. Тот факт, что полученные нами формулы для h связаны с характерами групп Галуа, показыва-

ет, что здесь существенна нормальность поля k над $\mathbb{Q}$ и коммутативность его группы Галуа. И действительно, можно легко вывести совершенно аналогичные формулы для любого поля k, являющегося абелевым расширением поля рациональных чисел $\mathbb{Q}$. Надо только воспользоваться законами разложения простых рациональных чисел в таких полях k, которые дает нам теория полей классов.

Общая теория полей классов дает нам законы разложения простых дивизоров $\mathfrak{p}$ произвольного поля алгебраических чисел k в конечном абелевом расширении K/k. Можно поэтому попытаться искать формулы для отношения $h(K)/h(k)$ чисел классов дивизоров этих полей. В этом направлении известны только разрозненные результаты. Формулы для отношения $h(K)/h(k)$ мы имеем в случае, когда k — квадратичное мнимое поле. Результаты здесь похожи на теорему 2: формулы имеют вид индекса группы, порожденной некоторыми специальными единицами, в группе всех единиц поля K (см. [49], [50], [116]). Другой интересный случай, в котором имеют место аналогичные формулы, обнаружил Гекке. Он высказал очень правдоподобные предположения, согласно которым отношение $h(K)/h(k)$ должно иметь совсем элементарное выражение, аналогичное формуле (7) п. 1 § 4 или формуле (6) п. 1 настоящего параграфа, если k — чисто вещественное расширение поля рациональных чисел, а K — его чисто мнимое квадратичное расширение. Условия, накладываемые на k и K, означают, что при любом изоморфном вложении $\varphi: k \to \mathbb{C}$ поля k в поле комплексных чисел $\mathbb{C}$ поле $\varphi(k)$ содержится в поле вещественных чисел, и, далее, если $K = k(\sqrt{\mu})$, то $\varphi(\mu) < 0$ для любого вложения φ. Сам Гекке доказал высказанную гипотезу в работе [80] для случая вещественных квадратичных полей k. Случай кубических полей рассматривался Рейдемейстером в статье [117]. Однако, как замечает Зигель (см. [130], сноска в конце введения), в работе [117] имеется ряд неясных мест.

4. Условие взаимной простоты h^* с l. В п. 3 § 7 гл. III мы видели, насколько важно было бы иметь критерий, позволяющий узнавать, взаимно просто ли число h с l или нет, т. е. является ли простое число l регулярным или иррегулярным. Так как $h = h_0 h^*$, то число l будет регулярным тогда и только тогда, когда оба множителя h_0 и h^* не делятся на l. В этом пункте мы найдем условие, необходимое и достаточное для того, чтобы множитель h^* не делился на l. Так как в следующем параграфе мы увидим, что h_0 также не делится на l, если $(h^*, l) = 1$, то это условие будет одновременно и критерием регулярности l.

Сохраняя обозначения предшествующего пункта, рассмотрим отношение

$$\frac{B}{l^{m-1}} = \prod_{k=1,3,\ldots,l-2} \frac{F(\theta^k)\, q_k}{l} \tag{16}$$

(мы здесь главный дивизор (α) отождествляем с числом α). Ввиду формулы (6) число h^* делится на l тогда и только тогда, когда целое рациональное число (16) делится на какой-нибудь простой дивизор $\mathfrak{q}_s$, $(s, l-1)=1$, скажем на $\mathfrak{q}_{l-2}=\mathfrak{q}_{-1}$, т. е. когда хоть один из целых дивизоров $F(\theta^k)\mathfrak{q}_k l^{-1}$ $(k=1, 3, \ldots, l-2)$ делится на $\mathfrak{q}_{-1}$. Для этого в свою очередь необходимо и достаточно, чтобы хоть при одном $k=1, 3, \ldots, l-2$ дивизор $F(\theta^k)\mathfrak{q}_k$ делился на $\mathfrak{q}_{-1}^2$. Покажем, что при $k=l-2\equiv -1 (\mathrm{mod}\, l-1)$ последнее условие не имеет места. В самом деле, $\theta^{-1}g\equiv 1(\mathrm{mod}\,\mathfrak{q}_{-1})$ согласно (15), поэтому

$$F(\theta^{-1})\equiv\sum_{r=0}^{l-2}(\theta^{-1}g)^r\equiv l-1\equiv -1\ (\mathrm{mod}\,\mathfrak{q}_{-1}),$$

т. е. $F(\theta^{-1})$ не делится на $\mathfrak{q}_{-1}$, а значит, $F(\theta^{-1})\mathfrak{q}_{-1}$ не делится на $\mathfrak{q}_{-1}^2$. Таким образом, для делимости h^* на l необходимо и достаточно, чтобы хоть при одном $k=1, 3, \ldots, l-4$ число $F(\theta^k)$ делилось на $\mathfrak{q}_{-1}^2$.

До сих пор на выбор первообразного корня g по модулю l мы не накладывали никаких ограничений. Теперь же мы предположим, что g удовлетворяет сравнению

$$g^{l-1}\equiv 1\ (\mathrm{mod}\, l^2)$$

(если g этому условию не удовлетворяет, то вместо него надо взять $g+xl$ с надлежащим x). Так как сравнение (14) выполняется теперь по модулю l^2, то $1-\theta^k g$ делится на $\mathfrak{q}_k^2$ при любом k, взаимно простом с $l-1$. В частности,

$$\theta\equiv g\,(\mathrm{mod}\,\mathfrak{q}_{-1}^2).$$

При таком выборе g условие делимости $F(\theta^k)$ на $\mathfrak{q}_{-1}^2$ находится совсем просто. Действительно, в силу сравнения

$$F(\theta^k)=\sum_{s=0}^{l-2}g_s\theta^{sk}\equiv\sum_{s=0}^{l-2}g_s g^{sk}\ (\mathrm{mod}\,\mathfrak{q}_{-1}^2)$$

число $F(\theta^k)$ делится на $\mathfrak{q}_{-1}^2$ тогда и только тогда, когда

$$\sum_{s=0}^{l-2}g_s g^{sk}\equiv 0\ (\mathrm{mod}\, l^2). \tag{17}$$

Желая условие (17) преобразовать к более удобному виду, рассмотрим сравнения

$$g_s\equiv g^s+la_s(\mathrm{mod}\, l^2),\qquad 0\leqslant s\leqslant l-2, \tag{18}$$

где a_s — целые числа. Если обе части сравнения (18) мы возведем в степень $k+1$ $(k=1, 3, \ldots, l-4)$, то получим

$$g_s^{k+1}\equiv g^{s(k+1)}+(k+1)g^{sk}la_s\equiv g^{s(k+1)}+(k+1)g^{sk}(g_s-g^s)\ (\mathrm{mod}\, l^2),$$

т. е.

$$g_s^{h+1} \equiv (k+1)\, g_s g^{sh} - k g^{s(h+1)} \pmod{l^2}. \tag{19}$$

Просуммируем сравнения (19) по всем $s = 0, 1, \ldots, l-2$. Так как $g^{h+1} \not\equiv 1 \pmod{l}$ при $k+1 \leqslant l-3$ и $g^{l-1} \equiv 1 \pmod{l^2}$, то

$$\sum_{s=0}^{l-2} g^{s(h+1)} = \frac{g^{(l-1)(h+1)} - 1}{g^{h+1} - 1} \equiv 0 \pmod{l^2}$$

и, следовательно, $\sum\limits_{s=0}^{l-2} g_s^{h+1} \equiv (k+1) \sum\limits_{s=0}^{l-2} g_s g^{sh} \pmod{l^2}$. Но $k+1 \not\equiv 0 \pmod{l}$, поэтому условие (17) равносильно сравнению $S_{k+1} = \sum\limits_{s=0}^{l-2} g_s^{h+1} = \sum\limits_{n=1}^{l-1} n^{h+1} \equiv 0 \pmod{l^2}$.

Нами доказана, таким образом, следующая теорема:

Теорема 3. *Для того чтобы число h^* не делилось на l, необходимо и достаточно, чтобы ни одно из чисел*

$$S_k = \sum_{n=1}^{l-1} n^k, \qquad k = 2, 4, \ldots, l-3, \tag{20}$$

не делилось на l^2.

Заметим, что все числа S_k при $k \not\equiv 0 \pmod{l-1}$ делятся на l (см. сравнение (10) § 8).

Переформулируем теорему 3 в терминах чисел Бернулли (определение чисел Бернулли и их некоторые свойства изложены в § 8). Так как числа 2, 4, ..., $l-3$ не делятся на $l-1$, то по теореме Штаудта (теорема 4 § 8) числа Бернулли $B_2, B_4, \ldots, B_{l-3}$ являются l-целыми (не содержат l в знаменателе). Далее, для сумм S_k мы имеем сравнения

$$S_k \equiv B_k l \pmod{l^2}, \qquad k = 2, 4, \ldots, l-3, \tag{21}$$

(в кольце l-целых чисел; см. сравнение (11) § 8). Следовательно, справедлива

Теорема 4. *Число h^* не делится на l тогда и только тогда, когда числители чисел Бернулли $B_2, B_4, \ldots, B_{l-3}$ не делятся на l.*

Например, так как числители чисел $B_2, B_4, B_6, B_8, B_{10}, B_{12}, B_{14}$ не делятся на 17, то число $l = 17$ регулярно.

Замечание. Для определения взаимной простоты числа h^* с l нет надобности находить точные значения чисел Бернулли. Достаточно рекуррентные соотношения (2) § 8 рассмотреть как сравнения по модулю l и из этих сравнений найти последовательно $B_2, B_4, \ldots, B_{l-3}$. Число h^* будет взаимно просто с l тогда и только тогда, когда все эти числа не делятся на l.

5. Замечание об операторной структуре группы классов дивизоров. В последние годы найдены глубокие результаты, с новой точки зрения освещающие строение группы классов дивизоров l-кругового поля $K = \mathbb{Q}(\zeta), \zeta^l = 1$. Именно, применяя к диви-

зорам поля K автоморфизмы его группы Галуа G, мы превращаем группу дивизоров $\mathfrak{D}$ в G-операторную группу (см. задачу 20 § 5 гл. III). Так как подгруппа главных дивизоров инвариантна относительно автоморфизмов из G, то и группа классов дивизоров $\mathfrak{C}$ поля K приобретает структуру G-операторной группы. То же, разумеется, относится и к ее l-примарной компоненте $\mathfrak{C}_l$. Строение последней G-операторной группы и описывается упомянутыми результатами (см. [84], [28]). Хотя они относятся к случаю l^n-кругового поля при произвольном n, мы приведем их лишь при $n = 1$.

Эти результаты получены, правда, при одном ограничительном предположении: число h_0 классов дивизоров вещественного подполя поля K не должно делится на l. Возможно, что на самом деле это условие не накладывает на l никаких ограничений: есть основания предполагать, что h_0 не делится на l для всех l (в этом состоит гипотеза, высказанная Вандивером, см. замечание в конце п. 2). Во всяком случае, как уже упоминалось в конце п. 2, h_0 не делится на l для $l < 125\,000$. Приняв условие $h_0 \not\equiv 0 \pmod{l}$, можно доказать следующий поразительный факт:

Примарная l-компонента $\mathfrak{C}_l$ группы классов дивизоров l-кругового поля является G-операторной группой с одной образующей.

Поясним точный смысл этого утверждения. Пусть L — кольцо l-целых рациональных чисел и $\Lambda = L[G]$ — групповое кольцо группы G над L. Умножение на элементы из G превращает Λ в G-операторную группу (G-модуль). Сформулированная теорема означает, что $\mathfrak{C}_l$ как G-операторная группа является гомоморфным образом G-группы Λ.

Можно даже в явном виде указать идеал J кольца Λ, являющийся ядром этого гомоморфизма. Для каждого $a = 1, \ldots, p-1$ через σ_a обозначим такой автоморфизм поля $K = \mathbb{Q}(\zeta)$, что $\sigma_a(\zeta) = \zeta^a$, и положим $\omega = \sum_{a=1}^{l-1} a\sigma_a^{-1}$. Тогда

$$J = \left(\Lambda \frac{\omega}{l}\right) \cap \Lambda, \tag{22}$$

где пересечение рассматривается в групповом кольце $\mathbb{Q}[G]$ над полем рациональных чисел. Таким образом, имеет место G-операторный изоморфизм

$$\mathfrak{C}_l \approx \Lambda/J. \tag{23}$$

Из этой формулы можно получить еще более явные следствия. Пусть l^m — показатель абелевой l-группы $\mathfrak{C}_l$. Группа $\mathfrak{C}_l$ может рассматриваться как мультипликативно записанный модуль над фактор-кольцом $\mathbb{Z}/l^m\mathbb{Z}$. В группе обратимых элементов последнего кольца содержится мультипликативная циклическая группа порядка $l-1$, и поэтому существует $l-1$ гомоморфизмов группы G в мультипликативную группу кольца $\mathbb{Z}/l^m\mathbb{Z}$. Эти гомомор-

физмы φ_r ($r = 1, \ldots, l-1$) однозначно характеризуются условием

$$\varphi_r(\sigma_a) \equiv a^r \pmod{l}.$$

Для каждого r через $\mathfrak{A}_r$ обозначим подгруппу группы $\mathfrak{C}_l$, состоящую из тех элементов x, для которых $\sigma(x) = x^{\varphi_r(\sigma)}$ при всех $\sigma \in G$. Для группы $\mathfrak{C}_l$ имеет место разложение в прямое произведение G-операторных подгрупп $\mathfrak{C}_l = \prod_{r=1}^{l-1} \mathfrak{A}_r$. Из формул (22) и (23) можно вывести, что все $\mathfrak{A}_r$ — циклические l-примарные группы, причем $\mathfrak{A}_r \neq 1$ тогда и только тогда, когда r нечетно, $r > 1$ и число Бернулли B_{l-r} делится на l.

Без использования гипотезы Вандивера определены лишь порядки групп $\mathfrak{A}_r$. Предположим сначала, что r нечетно. Согласно задаче 4 § 3 гл. I поле l-адических чисел $\mathbb{Q}_l$ содержит корни степени $l-1$ из 1, при этом каждому целому l-адическому числу a, не делящемуся на l, однозначно соответствует корень θ, $\theta^{l-1} = 1$, такой, что $a \equiv \theta \pmod{l}$. Это дает возможность рассматривать гомоморфизмы φ_r как характеры группы G (или группы обратимых классов вычетов по модулю l), значения которых содержатся в $\mathbb{Q}_l$. А тогда все обобщенные числа Бернулли B_{n,φ_r} (см. § 8, замечание 1) также можно трактовать как элементы поля $\mathbb{Q}_l$. Доказано, что порядок группы $\mathfrak{A}_r$ равен $|\mathfrak{A}_r| = l^{m_r}$, $m_r = \nu_l(B_{1,\varphi_r})$.

Пусть теперь r четно. В l-примарной компоненте фактор-группы E/E_0 (обозначения теоремы 2) характер φ_r выделяет подгруппу $\mathfrak{B}_r$ (так же, как выше, была определена группа $\mathfrak{A}_r$). Доказано, что порядки групп $\mathfrak{A}_r$ и $\mathfrak{B}_r$ совпадают (если гипотеза Вандивера справедлива, то $\mathfrak{A}_r = \mathfrak{B}_r$ — единичная подгруппа).

Эти результаты получены на основе глубоких связей между круговыми полями и модулярными функциями (см. [69]).

Задачи

1. Пусть K_0 — подполе, состоящее из всех вещественных чисел l-кругового поля $\mathbb{Q}(\zeta)$, $\zeta^l = 1$. Показать, что K_0 совпадает с $\mathbb{Q}(\zeta + \zeta^{-1})$ и имеет степень $(l-1)/2$. Доказать, далее, что дискриминант поля K_0 равен $l^{(l-3)/2}$, а его регулятор R_0 связан с регулятором R поля $\mathbb{Q}(\zeta)$ соотношением $R = 2^{(l-3)/2} R_0$.

2. Пусть p простое, отличное от l, и f наименьшее натуральное, для которого $p^f \equiv 1 \pmod{l}$. Доказать, что в поле K_0 число p разлагается в произведение $\frac{l-1}{2f}$ простых дивизоров степеней f при f нечетном и в произведение $(l-1)/f$ простых дивизоров степеней $f/2$ при f четном.

3. Доказать, что для дзета-функции $\zeta_{K_0}(s)$ поля K_0 имеет место соотношение

$$\lim_{s \to 1+0} (s-1)\, \zeta_{K_0}(s) = \prod_{\substack{\chi \neq \chi_0 \\ \chi(-1)=1}} L(1, \chi),$$

где χ пробегает все четные числовые характеры по модулю l, отличные от единичного характера χ_0.

4. Доказать, что число классов дивизоров вещественного подполя $\mathbb{Q}(\zeta+\zeta^{-1})$ l-кругового поля равно множителю h_0 числа классов поля $\mathbb{Q}(\zeta)$.

5. Доказать для множителя h^* формулу

$$h^* = \frac{1}{(2l)^{m-1}} \left| \det \left(g_{m+i+j} - g_{i+j}\right)_{0 \leqslant i,j \leqslant m-1} \right|,$$

где g_s — наименьший положительный вычет числа g^s по модулю $l = 2m+1$ (g — первообразный корень по модулю l).

6. Вычислить множитель h^* при $l = 7$.

7. Показать, что простое число 37 иррегулярно.

§ 6. Условие регулярности

Целью этого параграфа является доказательство того, что в случае, когда множитель h^* числа классов дивизоров l-кругового поля не делится на l, множитель h_0 также не делится на l и, значит, простое число l регулярно. Попутно мы докажем здесь также, что для регулярного l всякая единица поля $K = \mathbb{Q}(\zeta)$, сравнимая по модулю l с целым рациональным числом, является l-й степенью. На этом утверждении, известном под названием леммы Куммера, основывается доказательство второго случая теоремы Ферма для регулярных показателей. Как условие регулярности, так и лемма Куммера являются, как мы увидим, простыми следствиями того факта, что при $l \nmid h^*$ в $\mathfrak{l}$-адическом пополнении $K_\mathfrak{l}$ поля $K = \mathbb{Q}(\zeta)$, $\mathfrak{l} = (1-\zeta)$, значения $\log \theta_k^{l-1}$ $(k = 2, 3, \ldots, (l-1)/2)$ образуют базис совокупности целых «вещественных» $\mathfrak{l}$-адических чисел с нулевым следом (единицы θ_k определены равенствами (10) § 5).

1. Поле $\mathfrak{l}$-адических чисел. Круговое поле $K = \mathbb{Q}(\zeta)$, $\zeta = \cos\frac{2\pi}{l} + i\sin\frac{2\pi}{l}$, при простом $l \geqslant 3$ имеет, как мы знаем, степень $l-1$, и в нем разложение l на простые множители имеет вид $l = \mathfrak{l}^{l-1}$, где $\mathfrak{l} = (1-\zeta)$ — простой дивизор первой степени.

Рассмотрим $\mathfrak{l}$-адическое пополнение $K_\mathfrak{l}$ поля K. Элементы этого пополнения будем называть $\mathfrak{l}$-адическими числами. Полное поле $K_\mathfrak{l}$ содержит подполе, естественным образом изоморфное полю l-адических чисел $\mathbb{Q}_l$ (это подполе совпадает с замыканием поля $\mathbb{Q}$ в $K_\mathfrak{l}$). В силу этого естественного изоморфизма можно считать, что $\mathbb{Q}_l \subset K_\mathfrak{l}$.

Так как $\mathfrak{l}$ является единственным простым дивизором, делящим l, то ввиду теоремы 1 § 2 гл. IV степень расширения $K_\mathfrak{l}/\mathbb{Q}_l$ равна $l-1 = (K:\mathbb{Q})$. По этой же причине (см. (6) § 2 гл. IV) для любого $\alpha \in K$ имеет место равенство

$$N_{K/\mathbb{Q}}(\alpha) = N_{K_\mathfrak{l}/\mathbb{Q}_l}(\alpha). \tag{1}$$

Лемма 1. *В кольце целых* $\mathfrak{l}$*-адических чисел существует такой простой элемент* λ*, что:*

1) $\lambda^{l-1}+l=0$,

2) $\lambda \equiv \zeta - 1 (\mathrm{mod}\, \lambda^2)$.

Условиями 1) *и* 2) *элемент* λ *определен однозначно.*

Ввиду равенства (5) § 1 гл. III мы имеем

$$\frac{l}{(1-\zeta)^{l-1}} = (1+\zeta)(1+\zeta+\zeta^2)\ldots(1+\zeta+\ldots+\zeta^{l-2}).$$

Перейдем здесь к сравнению по модулю простого элемента $1-\zeta$ поля $K_{\mathfrak{l}}$ (напомним, что $v_{\mathfrak{l}}(1-\zeta)=1$). Поскольку $\zeta \equiv 1 (\mathrm{mod}\, 1-\zeta)$ и $(l-1)!+1 \equiv 0 (\mathrm{mod}\, l)$ (теорема Вильсона), то

$$\frac{l}{(1-\zeta)^{l-1}} \equiv 2\cdot 3\ldots(l-1) \equiv -1 (\mathrm{mod}\, 1-\zeta).$$

Покажем, что $\mathfrak{l}$-адическая единица $\alpha = -l/(1-\zeta)^{l-1}$, сравнимая с 1 по модулю $1-\zeta$, может быть представлена в виде $\alpha=\gamma^{l-1}$. Рассмотрим для этого многочлен $F(X)=X^{l-1}-\alpha$. Так как $F(1) \equiv 0 (\mathrm{mod}\, 1-\zeta)$ и $F'(1) \not\equiv 0 (\mathrm{mod}\, 1-\zeta)$, то в $K_{\mathfrak{l}}$ существует единица γ, для которой $F(\gamma)=0$ (см. конец п. 2 § 1 гл. IV). Таким образом, $\alpha=\gamma^{l-1}$, что и утверждалось. Полагая теперь $\lambda=(\zeta-1)\gamma$, мы получаем простой элемент λ с требуемыми свойствами. Всякое другое λ_1, удовлетворяющее первому условию леммы, имеет вид $\lambda\theta$, где θ — корень степени $l-1$ из 1. Но из сравнения $\lambda\theta \equiv \lambda (\mathrm{mod}\, \lambda^2)$ следует, что $\theta \equiv 1 (\mathrm{mod}\, \lambda)$. Если бы корень θ был отличен от 1, то $l-1$ делилось бы на λ, что невозможно. Следовательно, $\theta=1$ и, значит, $\lambda_1=\lambda$. Лемма 1 доказана полностью.

В дальнейшем без специальных оговорок под λ будет пониматься простой элемент поля $K_{\mathfrak{l}}$, однозначно определенный условиями леммы 1.

Для каждого k, взаимно простого с l, соответствие $\zeta \to \zeta^k$ определяет автоморфизм σ_k расширения $K/\mathbb{Q}$. Если σ — любой из этих автоморфизмов, то функция $v'(\alpha)=v_{\mathfrak{l}}(\sigma(\alpha))$, $\alpha \in K$, является показателем поля K, и этот показатель является продолжением l-адического показателя v_l поля $\mathbb{Q}$. Но для v_l существует только одно продолжение на поле K, а именно $v_{\mathfrak{l}}$. Следовательно, $v'=v_{\mathfrak{l}}$, а значит, $v_{\mathfrak{l}}(\sigma(\alpha))=v_{\mathfrak{l}}(\alpha)$ при любом $\alpha \in K$. Отсюда легко следует, что при автоморфизме σ всякая фундаментальная последовательность элементов из K (относительно метрики, соответствующей простому дивизору $\mathfrak{l}$) переходит опять в фундаментальную последовательность. Это дает возможность продолжить автоморфизмы $\sigma=\sigma_k$ поля K на поле $K_{\mathfrak{l}}$. Именно, если $\xi = \lim\limits_{n\to\infty} \alpha_n$ $(\alpha_n \in K)$, то можно положить

$$\sigma(\xi) = \lim_{n\to\infty} \sigma(\alpha_n)$$

(легко проверяется, что $\sigma(\xi)$ не зависит от выбора последовательности $\{\alpha_n\}$, а также, что отображение $\xi \to \sigma(\xi)$ является автоморфизмом расширения $K_\mathfrak{l}/\mathbb{Q}_l$).

Так как для расширения $K_\mathfrak{l}/\mathbb{Q}_l$ степень инерции равна 1, а индекс ветвления $l-1$, то по теореме 4 § 1 гл. IV все целые $\mathfrak{l}$-адические числа однозначно представляются в виде

$$a_0 + a_1\lambda + \ldots + a_{l-2}\lambda^{l-2} \tag{2}$$

с целыми l-адическими a_i.

Подполе вещественных чисел поля K состоит из тех $\alpha \in K$, которые не меняются при автоморфизме $\sigma_{-1}: \zeta \to \zeta^{-1}$. Посмотрим, какие $\mathfrak{l}$-адические числа инвариантны относительно σ_{-1}. Так как $\lambda^{l-1} = -l$, то и $(\sigma_{-1}(\lambda))^{l-1} = -l$, а значит, $\sigma_{-1}(\lambda) = \lambda\theta$, где θ — корень степени $l-1$ из 1. Согласно задаче 4 § 3 гл. I корень θ содержится в $\mathbb{Q}_l$, поэтому

$$\sigma_{-1}^2(\lambda) = \sigma_{-1}(\sigma_{-1}(\lambda)) = \sigma_{-1}(\theta\lambda) = \theta\sigma_{-1}(\lambda) = \theta^2\lambda,$$

а так как, с другой стороны, $\sigma_{-1}^2(\lambda) = \lambda$, то $\theta = \pm 1$. Если бы $\theta = 1$, то произвольное $\mathfrak{l}$-адическое число, представляющееся в виде (2) с l-адическими коэффициентами a_i, не менялось бы при действии автоморфизма σ_{-1}, а это на самом деле не так. Следовательно, $\theta = -1$ и $\sigma_{-1}(\lambda) = -\lambda$. Таким образом, при действии автоморфизма σ_{-1} в поле $K_\mathfrak{l}$ не будут меняться лишь $\mathfrak{l}$-адические числа вида

$$\sum_{i=0}^{m-1} b_i\lambda^{2i}, \qquad b_i \in \mathbb{Q}_l, \ m = \frac{l-1}{2}. \tag{3}$$

Все эти числа образуют подполе в $K_\mathfrak{l}$ степени $m = \frac{l-1}{2}$ над $\mathbb{Q}_l$. Будем их называть для удобства «вещественными» $\mathfrak{l}$-адическими числами.

Вычислим след $\mathfrak{l}$-адического числа (2) (относительно расширения $K_\mathfrak{l}/\mathbb{Q}_l$). Для любого $i = 1, \ldots, l-2$ матрица линейного преобразования $\xi \to \lambda^i\xi$ $(\xi \in K_\mathfrak{l})$ в базисе $1, \lambda, \ldots, \lambda^{l-2}$ будет иметь на главной диагонали нулевые элементы (поскольку $\lambda^{l-1} = -l$), поэтому $\mathrm{Sp}_{K_\mathfrak{l}/\mathbb{Q}_l}(\lambda^i) = 0$ (при $i = 1, \ldots, l-2$). Отсюда вытекает, что след числа (2) равен $a_0(l-1)$. Все $\mathfrak{l}$-адические числа нулевого следа (относительно $\mathbb{Q}_l$) характеризуются, следовательно, тем, что для них в разложении (2) коэффициент a_0 равен нулю.

Нас в дальнейшем будет интересовать совокупность $\mathfrak{M}$ всех «вещественных» целых $\mathfrak{l}$-адических чисел с нулевым следом. На основании вышеизложенного можно заключить, что $\mathfrak{M}$ совпадает

со всеми линейными комбинациями

$$\sum_{i=1}^{m-1} b_i \lambda^{2i} \tag{4}$$

с целыми l-адическими коэффициентами b_i.

На поле $K_\mathfrak{l}$ мы можем рассматривать функции $\ln \varepsilon$ и $\exp \alpha$, определяемые степенными рядами (см. п. 2 § 5 гл. IV). Так как индекс ветвления e расширения $K_\mathfrak{l}/\mathbb{Q}_l$ равен $l-1$, то для этого расширения число $\left[\frac{e}{l-1}\right]+1$ равно 2, а значит, ряд $\exp \alpha$ сходится для всех целых $\alpha \in K_\mathfrak{l}$, делящихся на λ^2. Функция $\log \varepsilon$ определена, как мы знаем, для всех главных единиц поля $K_\mathfrak{l}$.

Если ε — главная единица поля $K_\mathfrak{l}$, т. е. $\varepsilon \equiv 1 (\mathrm{mod}\, \lambda)$, то при любом автоморфизме σ_k мы имеем также $\sigma_k(\varepsilon) \equiv 1 (\mathrm{mod}\, \lambda)$, а значит, $\ln \sigma_k(\varepsilon)$ имеет смысл. Но тогда (следствие 1 теоремы 11 § 2 Дополнения)

$$\mathrm{Sp}_{K_\mathfrak{l}/\mathbb{Q}_l} \ln \varepsilon =$$

$$= \sum_{k=1}^{l-1} \sigma_k (\ln \varepsilon) = \sum_k \ln (\sigma_k (\varepsilon)) = \ln \left(\prod_k \sigma_k (\varepsilon) \right) = \ln \left(N_{K_\mathfrak{l}/\mathbb{Q}_l} \varepsilon \right).$$

Предположим теперь, что ε — единица поля K. Ясно, что ε будет единицей и в поле $K_\mathfrak{l}$, однако $\log \varepsilon$ может не иметь смысла, так как ε, вообще говоря, не будет главной единицей в $K_\mathfrak{l}$. Мы будем иметь, однако, сравнение $\varepsilon \equiv a (\mathrm{mod}\, \lambda)$ при некотором не делящемся на l целом рациональном числе a. Но $a^{l-1} \equiv 1 (\mathrm{mod}\, l)$, поэтому $\varepsilon^{l-1} \equiv 1 (\mathrm{mod}\, \lambda)$, т. е. ε^{l-1} уже будет главной единицей в $K_\mathfrak{l}$. Логарифм $\log \varepsilon^{l-1}$ имеет, следовательно, смысл, при этом ввиду формулы (1)

$$\mathrm{Sp}_{K_\mathfrak{l}/\mathbb{Q}_l} (\ln \varepsilon^{l-1}) = \ln \left(N_{K_\mathfrak{l}/\mathbb{Q}_l} \varepsilon^{l-1} \right) = \ln \left(N_{K/\mathbb{Q}} \varepsilon^{l-1} \right) = 0,$$

т. е. целое l-адическое число $\ln \varepsilon^{l-1}$ имеет нулевой след. Если ε — вещественная единица поля K, то $\ln \varepsilon^{l-1}$, очевидно, также будет «вещественным».

Итак, для любой вещественной единицы ε поля K l-адическое число $\ln \varepsilon^{l-1}$ принадлежит множеству $\mathfrak{M}$, т. е. оно может быть представлено в виде (4). В частности, это справедливо и для единиц θ_k ($k = 2, 3, \ldots, m = (l-1)/2$), определенных формулами (10) § 5. Таким образом, мы имеем

$$\ln \theta_k^{l-1} = \sum_{i=1}^{m-1} b_{ki} \lambda^{2i}, \quad 2 \leqslant k \leqslant m, \tag{5}$$

с целыми l-адическими коэффициентами b_{ki}.

Нашей задачей является доказательство того, что в случае, когда множитель h^* числа классов дивизоров поля K не делится на l, l-адические числа $\ln \theta_k^{l-1}$ образуют базис $\mathfrak{M}$ над кольцом целых l-адических чисел в том смысле, что всякое $\xi \in \mathfrak{M}$ однозначно представляется в виде их линейной комбинации с целыми l-адическими коэффициентами. Для этого, очевидно, достаточно показать, что $\det(b_{ki})$ является l-адической единицей, т. е. что $\det(b_{ki}) \not\equiv 0 \pmod{l}$.

2. Некоторые вспомогательные сравнения. Ряд $\exp x$ в поле $K_\mathfrak{l}$ сходится лишь для целых x, делящихся на λ^2. В связи с этим в некоторых случаях вместо ряда $\exp x$ целесообразно рассматривать многочлен

$$E(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots + \frac{x^{l-1}}{(l-1)!},$$

получающийся из $\exp x$ отбрасыванием всех членов степени $\geqslant l$ (вместо l можно было бы взять любое натуральное число, но нам будет полезным именно такое определение). Так как коэффициенты $\frac{1}{k!}$ при $k \leqslant l-1$ являются целыми l-адическими числами, то $E(x)$ будет главной единицей поля $K_\mathfrak{l}$ при любом целом $x \equiv 0 \pmod{\lambda}$.

Мы знаем, что формальное произведение рядов $\exp x$ и $\exp y$ равно ряду $\exp(x+y)$. Отсюда легко следует, что

$$E(x)E(y) = E(x+y) + F(x, y), \tag{6}$$

где $F(x, y)$ — многочлен с целыми l-адическими коэффициентами, все члены которого имеют степень $\geqslant l$.

Лемма 2. *В кольце целых $\mathfrak{l}$-адических чисел справедливо сравнение* $E(\lambda)^l \equiv 1 \pmod{\lambda^{2l-1}}$.

Положим $E(x) = 1 + xg(x)$, где $g(x) = 1 + \frac{x}{2!} + \ldots + \frac{x^{l-2}}{(l-1)!}$ — многочлен с целыми l-адическими коэффициентами. Тогда

$$E(x)^l = 1 + C_l^1 xg(x) + \ldots + C_l^{l-1}(xg(x))^{l-1} + x^l g(x)^l = \\ = 1 + lh(x) + x^l g(x)^l,$$

где $h(x)$ — многочлен опять-таки с целыми l-адическими коэффициентами. С другой стороны, ввиду (6) имеем также

$$E(x)^l = E(lx) + x^l M(x),$$

а значит,

$$lh(x) = \frac{lx}{1!} + \frac{(lx)^2}{2!} + \ldots + \frac{(lx)^{l-1}}{(l-1)!} + x^l H(x), \tag{7}$$

где $H(x) = M(x) - g(x)^l$. Сравнивая в этом равенстве коэффициенты при одинаковых степенях x, видим, что все коэффициенты

$H(x)$ — целые l-адические числа, делящиеся на l. Сокращая (7) на l, приходим к равенству

$$h(x) = x + \frac{lx^2}{2!} + \ldots + \frac{l^{l-2}x^{l-1}}{(l-1)!} + x^l G(x),$$

где $G(x)$ имеет целые l-адические коэффициенты. Полагая здесь $x = \lambda$, получаем сравнение $h(\lambda) \equiv \lambda (\mathrm{mod}\, \lambda^l)$, а значит,

$$lh(\lambda) \equiv l\lambda (\mathrm{mod}\, \lambda^{2l-1}). \tag{8}$$

Далее, так как $g(\lambda) \equiv 1 (\mathrm{mod}\, \lambda)$, то $g(\lambda)^l \equiv 1 (\mathrm{mod}\, \lambda^l)$, откуда

$$\lambda^l g(\lambda)^l \equiv \lambda^l (\mathrm{mod}\, \lambda^{2l}). \tag{9}$$

В силу (8) и (9) имеем теперь

$$E(\lambda)^l = 1 + lh(\lambda) + \lambda^l g(\lambda)^l \equiv 1 + l\lambda + \lambda^l = 1 (\mathrm{mod}\, \lambda^{2l-1})$$

(так как $l\lambda + \lambda^l = 0$), что и требовалось доказать.

Лемма 3. *При любом натуральном k имеет место сравнение*

$$E(k\lambda) \equiv \zeta^k (\mathrm{mod}\, \lambda^l).$$

В силу формулы (6) $E(k\lambda) \equiv E(\lambda)^k (\mathrm{mod}\, \lambda^l)$, поэтому достаточно доказать лемму для случая $k = 1$.

По определению простого элемента λ мы имеем $\zeta \equiv 1 + \lambda (\mathrm{mod}\, \lambda^2)$. С другой стороны, $E(\lambda) \equiv 1 + \lambda (\mathrm{mod}\, \lambda^2)$, поэтому $\zeta^{-1} E(\lambda) \equiv 1 (\mathrm{mod}\, \lambda^2)$. Положим

$$\zeta^{-1} E(\lambda) = 1 + \lambda^2 \gamma,$$

где γ целое l-адическое. Возводя это равенство в l-ю степень и учитывая лемму 2, получаем сравнение

$$\gamma \left(l\lambda^2 + \frac{l(l-1)}{2} \gamma \lambda^4 + \ldots + \gamma^{l-1} \lambda^{2l} \right) \equiv 0 \left(\mathrm{mod}\, \lambda^{2l-1} \right).$$

Выражение, стоящее в скобках, делится точно на λ^{l+1}, поэтому $\gamma \equiv 0 (\mathrm{mod}\, \lambda^{l-2})$, откуда $\zeta^{-1} E(\lambda) \equiv 1 (\mathrm{mod}\, \lambda^l)$, что и доказывает лемму.

Рассмотрим также многочлен

$$L(1+x) = x - \frac{x^2}{2} + \ldots + (-1)^{l-2} \frac{x^{l-1}}{l-1}, \tag{9*}$$

получающийся из ряда $\log(1+x)$ отбрасыванием членов степени $\geqslant l$.

Лемма 4. *Если целое l-адическое число α делится на λ^2, то*

$$L(1+\alpha) \equiv \ln(1+\alpha) (\mathrm{mod}\, \lambda^l).$$

Действительно, при $n \geqslant 1$ имеем

$$\nu_l\left(\frac{\alpha^n}{n}\right) \geqslant 2n - \nu_l(n) \geqslant 2n - (l-1)\frac{\ln n}{\ln l} \geqslant$$

$$\geqslant l + (n-l) + \frac{(l-1)\,n}{\ln l}\left(\frac{\ln l}{l-1} - \frac{\ln n}{n-1}\right) \geqslant l$$

(см. п. 2 § 5 гл. IV).

Лемма 5. *Если* ε_1 *и* ε_2 *— главные* l*-адические единицы, то*

$$L(\varepsilon_1\varepsilon_2) \equiv L(\varepsilon_1) + L(\varepsilon_2) (\mathrm{mod}\, \lambda^l).$$

Так как ряд $\log(1 + x + y + xy)$ равен сумме рядов $\log(1+x)$ и $\log(1+y)$, то

$$L(1 + x + y + xy) = L(1+x) + L(1+y) + G(x, y),$$

где многочлен $G(x, y)$ содержит члены степени $\geqslant l$ с целыми l-адическими коэффициентами. Утверждение леммы 5 следует теперь из того, что $G(x, y) \equiv 0 (\mathrm{mod}\, \lambda^l)$, если только x и y делятся на λ.

Лемма 6. *В кольце целых* l*-адических чисел справедливо сравнение*

$$L(\xi) \equiv \lambda (\mathrm{mod}\, \lambda^l).$$

Для доказательства воспользуемся формальным равенством $\log \exp x = x$. Из этого равенства легко следует, что

$$L(E(x)) = x + H(x),$$

где $H(x)$ — многочлен, все члены которого имеют степень $\geqslant l$ и целые l-адические коэффициенты. Положив здесь $x = \lambda$ и воспользовавшись леммой 3 при $k = 1$, мы и получим требуемое сравнение.

Замечание. Пусть $\mathfrak{A}$ — мультипликативная группа классов вычетов группы главных l-адических единиц по модулю λ^l и $\mathfrak{x}$ — аддитивная группа классов вычетов целых l-адических чисел, делящихся на λ, по тому же модулю λ^l. Легко показать, что отображение $\varepsilon \to L(\varepsilon)$ (на главных l-адических единицах ε) индуцирует изоморфизм группы $\mathfrak{A}$ на группу $\mathfrak{x}$. Обратный изоморфизм $\mathfrak{x} \to \mathfrak{A}$ индуцируется при этом отображением $\alpha \to E(\alpha)$ $(\alpha \equiv 0 (\mathrm{mod}\, \lambda))$.

3. Базис вещественных целых l-адических чисел в случае $(h^*, l) = 1$. Вернемся к вопросу, поставленному в конце п. 1. Чтобы выяснить, делится ли $\det(b_{ki})$ на l или нет, нам достаточно знать коэффициенты b_{ki} лишь по модулю l. Ясно, что два целых l-адических числа вида (2) сравнимы между собой по модулю l тогда и только тогда, когда у них соответствующие коэффициенты при степенях λ сравнимы по модулю l (в кольце целых l-адических чисел). Отсюда следует, что для вычисления по модулю l коэффициентов b_{ki} вместо $\ln \theta_k^{l-1}$ мы можем взять любое сравнимое с ним по модулю l (т. е. модулю λ^{l-1}) целое l-адическое число.

Сохраним здесь все обозначения п. 2 § 5. Главная единица θ_k^{l-1} вещественна; следовательно, она сравнима с 1 по модулю λ^2, а значит, по лемме 4

$$\ln \theta_k^{l-1} \equiv L\left(\theta_k^{l-1}\right) \pmod{\lambda^l}. \tag{10}$$

Займемся вычислением $L\left(\theta_k^{l-1}\right)$. Так как $\theta_k = \frac{\zeta^k - 1}{\zeta - 1}\eta^{1-k}$, то

$$\theta_k^l = \left(1 + \zeta + \ldots + \zeta^{k-1}\right)^l (-1)^{1-k}.$$

Но $\zeta \equiv 1 \pmod{\lambda}$, поэтому

$$1 + \zeta + \ldots + \zeta^{k-1} \equiv k \pmod{\lambda},$$

откуда $(1 + \zeta + \ldots + \zeta^{k-1})^l \equiv k^l \pmod{\lambda^l}$, а так как $k^l \equiv k \pmod{\lambda^{l-1}}$, то

$$(1 + \zeta + \ldots + \zeta^{k-1})^l \equiv k \pmod{\lambda^{l-1}}.$$

Таким образом,

$$\theta_k^{l-1} \equiv \theta_k^{-1} k (-1)^{1-k} \equiv k \frac{\zeta - 1}{\zeta^k - 1}(-\eta)^{k-1} \pmod{\lambda^{l-1}},$$

или

$$\theta_k^{l-1} \equiv \frac{\zeta - 1}{\lambda}\left(\frac{\zeta^k - 1}{k\lambda}\right)^{-1} \zeta^{(k-1)(l+1)/2} \pmod{\lambda^{l-1}}.$$

По лемме 5 мы имеем

$$L\left(\theta_k^{l-1}\right) \equiv L\left(\frac{\zeta - 1}{\lambda}\right) - L\left(\frac{\zeta^k - 1}{k\lambda}\right) + (k-1)\frac{l+1}{2} L(\zeta) \pmod{\lambda^{l-1}}.$$

Но по лемме 3 $\frac{\zeta^k - 1}{k\lambda} \equiv \frac{E(k\lambda) - 1}{k\lambda} \pmod{\lambda^{l-1}}$, поэтому, учитывая лемму 6, получаем

$$L\left(\theta_k^{l-1}\right) \equiv L\left(\frac{E(\lambda) - 1}{\lambda}\right) - \frac{\lambda}{2} - L\left(\frac{E(k\lambda) - 1}{k\lambda}\right) + \frac{k\lambda}{2} \pmod{\lambda^{l-1}}.$$

Докажем теперь, что

$$L\left(\frac{E(x) - 1}{x}\right) - \frac{x}{2} = \sum_{h=1}^{m-1} \frac{B_{2h} x^{2h}}{(2h)!\, 2h} + x^{l-1} R(x), \tag{11}$$

где многочлен $R(x)$ имеет целые l-адические коэффициенты, а B_{2h} — числа Бернулли (см. § 8 этой главы). Воспользуемся тождеством $\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$. Так как $B_1 = -1/2$, а все остальные числа Бернулли с нечетным индексом равны нулю, то наше тождество можно переписать в виде

$$\frac{e^x}{e^x - 1} - \frac{1}{2} - \frac{1}{x} = \sum_{h=1}^{\infty} \frac{B_{2h}}{(2h)!} x^{2h-1}.$$

После интегрирования получим

$$\ln\frac{e^x-1}{x}-\frac{x}{2}=\sum_{k=1}^{\infty}\frac{B_{2k}}{(2k)!\,2k}x^{2k} \tag{12}$$

(свободный член ряда равен нулю, так как при $x=0$ функция, стоящая слева, обращается в нуль). Из формулы (12) легко теперь получить равенство (11). Подставляя в (11) вместо x значение $k\lambda$, находим

$$L\left(\frac{E(k\lambda)-1}{k\lambda}\right)-\frac{k\lambda}{2}\equiv\sum_{i=1}^{m-1}\frac{B_{2i}k^{2i}\lambda^{2i}}{(2i)!2i}\pmod{\lambda^{l-1}},$$

а значит,

$$L(\theta_k^{l-1})\equiv\sum_{i=1}^{m-1}\frac{B_{2i}(1-k^{2i})\lambda^{2i}}{(2i)!\,2i}\pmod{\lambda^{l-1}}. \tag{12*}$$

Этим доказано, что коэффициенты b_{ki} в равенствах (5) удовлетворяют сравнениям

$$b_{ki}\equiv\frac{B_{2i}(1-k^{2i})}{(2i)!\,2i}\pmod{l},\quad 2\leqslant k\leqslant m=\frac{l-1}{2},\quad 1\leqslant i\leqslant m-1.$$

Но тогда $\det(b_{ki})$ сравним по модулю l с определителем

$$\prod_{i=1}^{m-1}\frac{(-1)^{m-1}B_{2i}}{(2i)!\,2i}\begin{vmatrix}2^2-1 & 2^4-1 & \dots & 2^{l-3}-1\\ 3^2-1 & 3^4-1 & \dots & 3^{l-3}-1\\ \dots & \dots & \dots & \dots\\ m^2-1 & m^4-1 & \dots & m^{l-3}-1\end{vmatrix}.$$

Выписанный определитель легко сводится к определителю Вандермонда. Он равен произведению

$$\prod_{1\leqslant s<r\leqslant m}(r^2-s^2)=\prod_{s<r}(r+s)(r-s),$$

в котором все множители не делятся на l. Если теперь $h^*\not\equiv 0\pmod{l}$, то числители чисел Бернулли $B_2,\dots,B_{l-3}$ не делятся на l, и мы получаем, что $\det(b_{ki})\not\equiv 0\pmod{l}$.

Этим нами доказана следующая теорема:

Теорема 1. *Если* $h^*\not\equiv 0\pmod{l}$, *то целые «вещественные» l-адические числа с нулевым следом однозначно представляются в виде линейных комбинаций*

$$\sum_{k=2}^{m}a_k\ln\theta_k^{l-1} \tag{13}$$

с целыми l-адическими коэффициентами a_k.

Замечание. Полученному результату можно дать другую интерпретацию, которая приводит к постановке более общего и

важного вопроса. Пусть $K_0 = \mathbb{Q}\left(\cos\frac{2\pi}{l}\right)$ — подполе вещественных чисел l-кругового поля (задача 1 § 5). Замыкание $\overline{K}_0$ поля K_0 в поле $K_\mathfrak{l}$ совпадает, очевидно, с подполем «вещественных» l-адических чисел, в котором мы имеем фундаментальный базис $1, \lambda^2, \ldots, \lambda^{2(m-1)}$. Теорема 1 в других терминах означает, что система $m-1$ независимых единиц θ_k^{l-1} $(k=2, \ldots, m)$ поля K_0 остается независимой при погружении ее в группу главных единиц поля $\overline{K}_0$ (которая рассматривается как мультипликативно записанный модуль над кольцом $\mathbb{Z}_l$ целых l-адических чисел; задача 11 § 5 гл. IV).

Отмеченный только что факт связан с понятием p-адического регулятора. В п. 4 § 4 гл. II был введен обычный «вещественный» регулятор произвольного поля алгебраических чисел. Для его определения выбирается какая-нибудь система основных единиц поля. Точно таким же образом может быть определен регулятор $\mathrm{R}(\varepsilon_1, \ldots, \varepsilon_r)$ любой системы из $r=s+t-1$ единиц. (Ясно, что единицы $\varepsilon_1, \ldots, \varepsilon_r$ будут независимыми тогда и только тогда, когда их регулятор отличен от нуля.) Следуя определению обычного регулятора, вводим следующее понятие.

Пусть F — вполне вещественное поле алгебраических чисел степени n над $\mathbb{Q}$ и p — произвольное простое число. Для поля F мы имеем n различных изоморфизмов $\sigma_1, \ldots, \sigma_n$ в алгебраическое замыкание поля p-адических чисел $\mathbb{Q}_p$. Пусть, далее, $\varepsilon_1, \ldots, \varepsilon_r$ $(r=n-1)$ — система независимых единиц поля F. Все образы $\sigma_i(\varepsilon_j)$ являются, очевидно, единицами в некотором конечном расширении поля $\mathbb{Q}_p$, а значит, согласно замечанию к задаче 12 § 5 гл. IV, имеют смысл p-адические логарифмы $\ln\sigma_i(\varepsilon_j)$. Следуя рассуждениям п. 4 § 4 гл. II, легко убедиться, что в матрице

$$(\ln\sigma_i(\varepsilon_j)), \qquad 1\leqslant i\leqslant n, \quad 1\leqslant j\leqslant r,$$

все миноры порядка $r=n-1$ отличаются друг от друга лишь множителем ± 1. Это определенное с точностью до знака общее значение миноров порядка r указанной матрицы и называется p-адическим регулятором системы единиц $\varepsilon_1, \ldots, \varepsilon_r$ поля F и обозначается через $\mathrm{R}_p(\varepsilon_1, \ldots, \varepsilon_r)$. Если $\varepsilon_1, \ldots, \varepsilon_r$ — система основных единиц поля F, то ее p-адический регулятор, зависящий только от F, называется p-адическим регулятором вполне вещественного поля F и обозначается через $\mathrm{R}_p(F)$. Это — некоторое число из конечного расширения поля p-адических чисел $\mathbb{Q}_p$ (определенное с точностью до знака). Ясно, что p-адический регулятор произвольной системы $\varepsilon_1, \ldots, \varepsilon_r$ независимых единиц в F связан с p-адическим регулятором поля F соотношением

$$\mathrm{R}_p(\varepsilon_1, \ldots, \varepsilon_r) = a\mathrm{R}_p(F),$$

где a — индекс подгруппы, порожденной единицами $\varepsilon_1, \ldots, \varepsilon_r$ и

корнями из 1, в группе всех единиц. (Относительно обобщений на случай произвольных полей алгебраических чисел см. [38].)

Вернемся к теореме 1. Автоморфизмы $\sigma_1, \ldots, \sigma_m$ расширения $K_0/\mathbb{Q}$ можно рассматривать как изоморфизмы поля K_0 в замыкание $\overline{K}_0$. Припишем к системе (5) равенство $1=1$. Подвергая полученную систему равенств действию автоморфизмов $\sigma_1, \ldots, \sigma_m$ и переходя к определителям, легко получим, что

$$m\mathrm{R}_l\left(\theta_2^{l-1}, \ldots, \theta_m^{l-1}\right) = \det\left(b_{hi}\right)\sqrt{D},$$

где D — дискриминант базиса $1, \lambda^2, \ldots, \lambda^{2(m-1)}$ поля $\overline{K}_0$ над $\mathbb{Q}_l$. Из последнего равенства и теоремы 1 следует утверждение: если l — регулярное простое число и K_0 — вещественное подполе l-кругового поля, то l-адический регулятор $\mathrm{R}_l(K_0)$ отличен от нуля.

Леопольдтом высказана гипотеза о том, что для любого вполне вещественного поля алгебраических чисел F и для любого простого числа p всегда $\mathrm{R}_p(F) \neq 0$. Возникшая таким образом «проблема p-адического регулятора» оказалась связанной с многими вопросами теории полей алгебраических чисел. Однако до сих пор эта проблема остается нерешенной. Решена она (положительно) лишь в некоторых весьма частных случаях, например, для вещественных подполей полей деления круга.

В случае, когда в F имеется только один простой дивизор $\mathfrak{P}$, делящий p, условие $\mathrm{R}_p(F) \neq 0$ равносильно тому, что всякая независимая система единиц вполне вещественного поля F остается независимой (над кольцом $\mathbb{Z}_p$) при погружении ее в группу главных единиц пополнения $F_{\mathfrak{P}}$.

4. Критерий регулярности и лемма Куммера. Полученная теорема 1 теперь уже легко позволяет доказать следующую теорему.

Теорема 2. *Если для l-кругового поля $R(\zeta)$ множитель h^* числа классов дивизоров не делится на l, то множитель h_0 также не делится на l.*

Доказательство. Допуская, что $h_0 = (E : E_0)$ делится на l (см. обозначения теоремы 2 § 5), мы найдем вещественную положительную единицу $\varepsilon \in E$, которая сама не содержится в E_0, но $\varepsilon^l \in E_0$, т. е.

$$\varepsilon^l = \prod_{k=2}^{m} \theta_k^{c_k} \tag{14}$$

с целыми рациональными c_k, причем не все c_k делятся на l (в противном случае единица ε принадлежала бы E_0). Возводя равенство (14) в степень $l-1$, а затем логарифмируя (в поле K_l), получим

$$l \ln \varepsilon^{l-1} = \sum_{k=2}^{m} c_k \ln \theta_k^{l-1}. \tag{15}$$

С другой стороны, так как значение $\ln \varepsilon^{l-1}$ принадлежит $\mathfrak{M}$, то

для него должно существовать представление вида (13), сравнивая которое с (15), заключаем, что все отношения $\frac{c_k}{l}$ — целые l-адические числа. Это, однако, невозможно, так как не все c_k делятся на l. Полученное противоречие и доказывает теорему 2.

Следствие. *Простое число $l \geqslant 3$ регулярно тогда и только тогда, когда числители чисел Бернулли $B_2, B_4, \ldots, B_{l-3}$ не делятся на l.*

Теорема 3 (лемма Куммера). *Пусть l — регулярное простое рациональное число. Если некоторая единица ε l-кругового поля $\mathbb{Q}(\zeta)$ сравнима по модулю l с целым рациональным числом, то она является l-й степенью другой единицы.*

Доказательство. Пусть $\varepsilon \equiv a \pmod{l}$. Покажем прежде всего, что ε — вещественная единица. Если $\varepsilon = \zeta^k \varepsilon_1$ с вещественной единицей ε_1, то $\varepsilon_1 \equiv b \pmod{\lambda^2}$ с целым рациональным b и $\zeta^k \equiv 1 + k\lambda \pmod{\lambda^2}$. Из сравнения $a \equiv b(1 + k\lambda) \pmod{\lambda^2}$ следует теперь, что $k \equiv 0 \pmod{l}$, и наше утверждение доказано. Так как $-1 = (-1)^l$, то можно предположить, что $\varepsilon > 0$, т. е. $\varepsilon \in E$. Из сравнения $\varepsilon^{l-1} \equiv a^{l-1} \equiv 1 \pmod{l}$ следует, что $\ln \varepsilon^{l-1} \equiv 0 \pmod{l}$, а потому в силу теоремы 1

$$\ln \varepsilon^{l-1} = \sum_{k=2}^{m} l c_k \ln \theta_k^{l-1} \tag{16}$$

с целыми l-адическими c_k. С другой стороны, так как подгруппа E_0 имеет конечный индекс в E, то $\varepsilon^a \in E_0$ при некотором натуральном a и, следовательно,

$$\varepsilon^a = \prod_{k=2}^{m} \theta_k^{d_k} \tag{17}$$

с целыми рациональными d_k. Мы можем, очевидно, считать, что показатели $a, d_2, \ldots, d_m$ взаимно просты в совокупности (так как в группе E нет элементов конечного порядка, то на их общий делитель в (17) можно сократить). Возводя равенство (17) в степень $l - 1$, а затем логарифмируя (в поле K_1), мы получим

$$a \ln \varepsilon^{l-1} = \sum_{k=2}^{m} d_k \ln \theta_k^{l-1}.$$

Сравнивая это с равенством (16), приходим к равенствам

$$d_k \equiv l a c_k, \qquad k = 2, \ldots, m.$$

Так как числа ac_k целые l-адические, то отсюда следует, что все d_k делятся на l, а значит, ε^a является l-й степенью: $\varepsilon^a = \varepsilon_1^l$, где $\varepsilon_1 \in E_0$. Одновременно ввиду условия $(a, d_2, \ldots, d_m) = 1$ мы по-

лучаем, что a взаимно просто с l, поэтому $1 = au + lv$ при целых рациональных u и v, откуда

$$\varepsilon = (\varepsilon^a)^u (\varepsilon^v)^l = (\varepsilon_1^u \varepsilon^v)^l,$$

а это и требовалось доказать.

Задачи

1. Пусть p — простое число вида $4n + 1$, $\zeta = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$, $\lambda = \zeta - 1$, $m = \frac{p-1}{2}$. Положим

$$\xi = \prod_{k=1}^{p-1} \theta_k^{-\left(\frac{k}{p}\right)},$$

где $\theta_k = \sin\frac{k\pi}{p}\left(\sin\frac{\pi}{p}\right)^{-1}$, $1 \leqslant k \leqslant p-1$. Показать, что в p круговом поле $\mathbb{Q}(\zeta)$ имеет место сравнение

$$L(\xi^{p-1}) \equiv \frac{2B_m}{m!}\lambda^m \equiv -2B_m\sqrt{p} \pmod{\lambda^{m+1}}.$$

Здесь L обозначает функцию, определенную равенством (9*), а B_m — число Бернулли. (Использовать сравнение (12*) и сравнение задачи 14 § 4.)

2. Пусть $\varepsilon = T + U\sqrt{p} > 1$ — основная единица и h — число классов дивизоров квадратичного поля $\mathbb{Q}(\sqrt{p})$, где простое $p \equiv 1 \pmod 4$. Основываясь на предшествующей задаче и теореме 2 § 4, доказать сравнение

$$hU \equiv TB_m \pmod p, \qquad m = \frac{p-1}{2}$$

(см. [46] и [55]).

§ 7. Второй случай теоремы Ферма для регулярных показателей

1. Теорема Ферма.

Теорема 1. *Для регулярного простого числа $l \geqslant 3$ уравнение*

$$x^l + y^l = z^l \tag{1}$$

неразрешимо в целых отличных от нуля рациональных числах x, y, z.

Доказательство. Допустим, что целые взаимно простые числа x, y и z (отличные от нуля) удовлетворяют уравнению (1). Так как первый случай теоремы Ферма нами уже разобран в п. 3 § 7 гл. III, то сейчас мы предположим, что одно (и только одно) из этих чисел делится на l. Будем считать, что z делится на l (если, например, y делится на l, то равенство (1) мы перепишем в виде $x^l + (-z)^l = (-y)^l$).

Пусть $z = l^k z_0$, где $(z_0, l) = 1$, $k \geqslant 1$. Так как в l-круговом поле $\mathbb{Q}(\zeta)$ для числа l мы имеем разложение $l = (1-\zeta)^{l-1}\varepsilon$, где ε — единица поля $\mathbb{Q}(\zeta)$ (лемма 1 § 1 гл. III), то в поле $\mathbb{Q}(\zeta)$ равенство (1) может быть записано в виде

$$x^l + y^l = \varepsilon(1-\zeta)^{lm} z_0^l, \tag{2}$$

где $m = k(l-1) > 0$. Для доказательства теоремы достаточно показать, что равенство вида (2) невозможно. Мы докажем несколько больше. А именно, будет установлено, что равенство вида (2) невозможно не только в целых рациональных числах x, y и z_0, взаимно простых с l, но даже и в том случае, когда под x, y и z_0 будем понимать любые целые числа поля $\mathbb{Q}(\zeta)$, взаимно простые с $1-\zeta$. Допуская противное, т. е. допуская, что равенства вида (2) все же существуют, выберем из них то, у которого показатель $m \geqslant 1$ наименьший. Чтобы не вводить новых обозначений, будем считать, что этим равенством является (2). Числа x, y и z_0 теперь обозначают, стало быть, некоторые целые числа из $\mathbb{Q}(\zeta)$, взаимно простые с $1-\zeta$, а ε — некоторую единицу поля $\mathbb{Q}(\zeta)$.

Как и в § 6, через $\mathfrak{l}$ мы обозначим простой дивизор $(1-\zeta)$ поля $\mathbb{Q}(\zeta)$. Разложим левую часть равенства (2) на линейные множители и перейдем в этом равенстве к дивизорам. Мы получим

$$\prod_{k=0}^{l-1}(x + \zeta^k y) = \mathfrak{l}^{lm}\mathfrak{a}^l, \tag{3}$$

где дивизор $\mathfrak{a} = (z_0)$ взаимно прост с $\mathfrak{l}$. Так как $lm \geqslant l > 0$, то из (3) следует, что хоть один из множителей слева делится на $\mathfrak{l}$. Но $x + \zeta^i y = x + \zeta^k y - \zeta^k(1-\zeta^{i-k})y$, поэтому все числа

$$x + \zeta^k y \qquad (0 \leqslant k \leqslant l-1) \tag{4}$$

делятся на $\mathfrak{l}$. Если бы при $0 \leqslant k < i \leqslant l-1$ имело место сравнение $x + \zeta^k y \equiv x + \zeta^i y \pmod{\mathfrak{l}^2}$, то мы имели бы также $\zeta^k y(1-\zeta^{i-k}) \equiv 0 \pmod{\mathfrak{l}^2}$, а это невозможно, так как $\zeta^k y$ взаимно просто с $\mathfrak{l}$, а $1-\zeta^{i-k}$ ассоциировано с $1-\zeta$. Таким образом, числа (4) попарно несравнимы по модулю $\mathfrak{l}^2$, а значит, отношения

$$(x + \zeta^k y)/(1-\zeta), \qquad k = 0, 1, \ldots, l-1$$

попарно несравнимы по модулю $\mathfrak{l}$. Но $N(\mathfrak{l}) = l$, поэтому эти отношения образуют полную систему вычетов по модулю $\mathfrak{l}$ и одно из них, следовательно, делится на $\mathfrak{l}$. Отсюда следует, что среди чисел (4) одно (и только одно) делится на $\mathfrak{l}^2$. Так как в равенстве (2) вместо y мы можем взять любое из чисел $\zeta^k y$, то можно считать, что именно $x + y$ делится на $\mathfrak{l}^2$ и, значит, все остальные числа $x + \zeta^k y$, делясь на $\mathfrak{l}$, не делятся на $\mathfrak{l}^2$. Из того, что левая часть равенства (3) делится по крайней мере на $\mathfrak{l}^{l-1}\mathfrak{l}^2 = \mathfrak{l}^{l+1}$, следует теперь, что $m > 1$.

Обозначим через $\mathfrak{m}$ общий наибольший делитель дивизоров (x) и (y). Поскольку x и y не делятся на $\mathfrak{l}$, то и $\mathfrak{m}$ не делится на $\mathfrak{l}$. Ясно, что $(x+\zeta^k y)$ делится на $\mathfrak{l}\mathfrak{m}$, а $(x+y)$ делится даже на $\mathfrak{l}^{l(m-1)+1}\mathfrak{m}$. Положим

$$(x+y)=\mathfrak{l}^{l(m-1)+1}\mathfrak{m}\mathfrak{c}_0, \qquad (x+\zeta^k y)=\mathfrak{l}\mathfrak{m}\mathfrak{c}_k, \quad k=1, \ldots, l-1$$

и докажем, что дивизоры $\mathfrak{c}_0, \mathfrak{c}_1, \ldots, \mathfrak{c}_{l-1}$ попарно взаимно просты. В самом деле, если бы $\mathfrak{c}_i$ и $\mathfrak{c}_k$ $(0\leqslant i<k\leqslant l-1)$ имели общий делитель $\mathfrak{p}$, то из делимости $x+\zeta^i y$ и $x+\zeta^k y$ на $\mathfrak{l}\mathfrak{m}\mathfrak{p}$ следовало бы, что $\zeta^i y(1-\zeta^{k-i})$ и $x(1-\zeta^{k-i})$ также делятся на $\mathfrak{l}\mathfrak{m}\mathfrak{p}$, откуда в свою очередь вытекала бы делимость x и y на $\mathfrak{m}\mathfrak{p}$, что противоречит определению $\mathfrak{m}$.

Записывая (3) в виде $\mathfrak{m}^l\mathfrak{l}^{lm}\mathfrak{c}_0\mathfrak{c}_1\ldots\mathfrak{c}_{l-1}=\mathfrak{l}^{lm}\mathfrak{a}^l$, делаем вывод (поскольку $\mathfrak{c}_k$ попарно взаимно просты), что

$$\mathfrak{c}_k=\mathfrak{a}_k^l \qquad (0\leqslant k\leqslant l-1),$$

а значит,

$$(x+y)=\mathfrak{l}^{l(m-1)+1}\mathfrak{m}\mathfrak{a}_0^l, \tag{5}$$

$$(x+\zeta^k y)=\mathfrak{l}\mathfrak{m}\mathfrak{a}_k^l \qquad (1\leqslant k\leqslant l-1). \tag{6}$$

Выразив $\mathfrak{m}$ из (5) и подставив в (6), получим

$$(x+\zeta^k y)\mathfrak{l}^{l(m-1)}=(x+y)(\mathfrak{a}_k\mathfrak{a}_0^{-1})^l, \tag{7}$$

откуда следует, что дивизор $(\mathfrak{a}_k\mathfrak{a}_0^{-1})^l$ главный (ибо $\mathfrak{l}=(1-\zeta)$). Воспользуемся теперь регулярностью числа l. Так как число классов дивизоров поля $\mathbb{Q}(\zeta)$ не делится на l, то по следствию теоремы 3 § 7 гл. III дивизор $\mathfrak{a}_k\mathfrak{a}_0^{-1}$ также главный, т. е.

$$\mathfrak{a}_k\mathfrak{a}_0^{-1}=\left(\frac{\alpha_k}{\beta_k}\right), \qquad 1\leqslant k\leqslant l-1, \tag{8}$$

где α_k и β_k — целые числа поля $\mathbb{Q}(\zeta)$. Дивизоры $\mathfrak{a}_k$ $(1\leqslant k\leqslant l-1)$ и $\mathfrak{a}_0$ взаимно просты с $\mathfrak{l}$, поэтому можно считать, что числа α_k и β_k не делятся на $\mathfrak{l}$. Равенство главных дивизоров эквивалентно равенству соответствующих чисел с точностью до множителя, являющегося единицей. Следовательно, в силу (7) и (8) мы имеем

$$(x+\zeta^k y)(1-\zeta)^{l(m-1)}=(x+y)\left(\frac{\alpha_k}{\beta_k}\right)^l\varepsilon_k, \qquad 1\leqslant k\leqslant l-1, \tag{9}$$

где ε_k — единица поля $\mathbb{Q}(\zeta)$.

Обратимся теперь к следующему очевидному равенству:

$$(x+\zeta y)(1+\zeta)-(x+\zeta^2 y)=\zeta(x+y).$$

Умножив его на $(1-\zeta)^{l(m-1)}$ и воспользовавшись равенствами

(9) при $k=1$ и $k=2$, получим

$$(x+y)\left(\frac{\alpha_1}{\beta_1}\right)^l \varepsilon_1(1+\zeta) - (x+y)\left(\frac{\alpha_2}{\beta_2}\right)^l \varepsilon_2 = (x+y)\,\zeta(1-\zeta)^{l(m-1)}{}_2$$

откуда

$$(\alpha_1\beta_2)^l - \frac{\varepsilon_2}{\varepsilon_1(1+\zeta)}(\alpha_2\beta_1)^l = \frac{\zeta}{\varepsilon_1(1+\zeta)}(1-\zeta)^{l(m-1)}(\beta_1\beta_2)^l.$$

Мы получили, таким образом, равенство вида

$$\alpha^l + \varepsilon_0\beta^l = \varepsilon'(1-\zeta)^{l(m-1)}\gamma^l, \tag{10}$$

где α, β и γ — целые числа из $\mathbb{Q}(\zeta)$, не делящиеся на $\mathfrak{l}$, а ε_0 и ε' — единицы поля $\mathbb{Q}(\zeta)$. Преобразуем его к виду (2).

Выше мы видели, что $m>1$, следовательно, $m-1>0$ и $l(m-1)\geqslant l$, а значит, $\alpha^l+\varepsilon_0\beta^l\equiv 0 \pmod{\mathfrak{l}^l}$. Так как β взаимно просто с $\mathfrak{l}$, то существует такое целое β', что $\beta\beta'\equiv 1 \pmod{\mathfrak{l}^l}$. Умножив последнее сравнение на β'^l, получаем

$$\varepsilon_0 \equiv \omega^l \pmod{\mathfrak{l}^l},$$

где $\omega=-\alpha\beta'$ — целое число поля $\mathbb{Q}(\zeta)$. Так как $N(\mathfrak{l})=l$, то всякое целое число из $\mathbb{Q}(\zeta)$ сравнимо по модулю $\mathfrak{l}$ с целым рациональным числом. Но если $\omega\equiv a \pmod{\mathfrak{l}}$, то $\omega^l\equiv a^l \pmod{l\mathfrak{l}^l}$, а значит, единица ε_0 сравнима по модулю $\mathfrak{l}^l$ с целым рациональным числом. По лемме Куммера (теорема 3 § 6; здесь мы опять пользуемся регулярностью l) единица ε_0 является l-й степенью в $\mathbb{Q}(\zeta)$, т. е. $\varepsilon_0=\eta^l$, где η — также единица поля $\mathbb{Q}(\zeta)$. Равенство (10) принимает теперь вид

$$\alpha^l + (\eta\beta)^l = \varepsilon'(1-\zeta)^{l(m-1)}\gamma^l.$$

Мы получили равенство такого же типа, как и (2), с той, однако, разницей, что показатель m заменен здесь на $m-1$. Но это невозможно, так как m было выбрано наименьшим. Полученное противоречие показывает, что уравнение (1) не имеет решений в целых отличных от нуля x, y и z, среди которых одно делится на l, т. е. что для регулярного показателя l справедлив второй случай теоремы Ферма. Теорема 1, таким образом, доказана.

Что касается второго случая теоремы Ферма для иррегулярных показателей, то здесь к настоящему времени известно очень мало, и вопрос о справедливости теоремы Ферма в общем случае остается открытым. Наиболее существенные результаты в этом направлении принадлежат Вандиверу. Им получены достаточные признаки, выполнение которых обеспечивает справедливость второго случая теоремы Ферма для данного конкретного иррегулярного l. Один из этих признаков (наиболее пригодный для фактического использования) состоит в следующем.

Пусть l — некоторое иррегулярное простое число. Согласно критерию Куммера (следствие теоремы 2 § 6) числитель по край-

ней мере одного из чисел Бернулли B_{2a}, $2 \leqslant 2a \leqslant l-3$, делится на l. Пара $(l, 2a)$ в этом случае называется иррегулярной. Пусть $(l, 2a_1), \ldots, (l, 2a_s)$ — все различные иррегулярные пары для данного l (так что s равно индексу иррегулярности $ii(l)$ числа l). Фиксируем иррегулярную пару $(l, 2a)$. Выберем натуральное k так, чтобы число $p = 1 + kl$ было простым и меньшим $l^2 - l$ (такое k всегда найдется), и натуральное t так, чтобы $t^k \not\equiv 1 \pmod p$. Полагаем, далее,

$$d = \sum_{r=1}^{m} r^{l-2a}, \qquad m = \frac{l-1}{2},$$

$$Q_{2a} = \frac{1}{t^{kd/2}} \prod_{r=1}^{m} (t^{kr} - 1)^{r^{l-1-2a}}.$$

Критерий Вандивера утверждает, что если для каждой иррегулярной пары $(l, 2a)$, т. е. для каждого $a = a_1, \ldots, a_s$ имеем $Q_{2a}^k \not\equiv 1 \pmod p$, то для рассматриваемого l второй множитель h_0 числа классов l-кругового поля не делится на l и для этого l справедлив второй случай теоремы Ферма.

Практическое использование критерия Вандивера возможно только благодаря применению быстродействующих вычислительных машин. В настоящее время с помощью вычислительных машин справедливость теоремы Ферма проверена [142] для всех показателей $l < 125\,000$. Любопытно при этом отметить, что для всех иррегулярных l из указанного промежутка критерий Вандивера привел к положительному ответу при $t = 2$ и при наименьшем допустимом значении k.

Заметим, что все имеющиеся критерии по проверке второго случая теоремы Ферма для конкретных показателей l действуют лишь при условии, что h_0 не делится на l. Если окажется, что гипотеза Вандивера неверна и будет обнаружено простое l, делящее h_0, то для него у нас пока нет никаких средств решить вопрос о справедливости второго случая теоремы Ферма.

Теорема Ферма о решениях уравнения $x^n + y^n = z^n$ в целых числах может рассматриваться как вопрос о рациональных решениях уравнения $x^n + y^n = 1$. С этой точки зрения теорема Ферма — это частный случай общей теории о рациональных решениях уравнения $F(x, y) = 0$, где $F(x, y)$ — многочлен с рациональными коэффициентами. В этой общей теории в последнее время получен весьма существенный результат, из которого, в частности, следует, что для любого показателя $n \geqslant 3$ число целых рациональных решений уравнения $x^n + y^n = z^n$ во всяком случае конечно (если, разумеется, не различать пропорциональные решения). Другими словами, на кривой Ферма $x^n + y^n = 1$ при $n \geqslant 3$ имеется лишь конечное число рациональных точек.

Результат, о котором идет речь, получен Фалтингсом в работе [76]. Его формулировка в общем случае выглядит следующим образом. Пусть $F(x, y)$ — абсолютно неприводимый многочлен, коэффициенты которого — алгебраические числа. Кривая, определяемая уравнением $F(x, y) = 0$, имеет некоторую геометрическую характеристику, называемую родом. Род кривой есть неотрицательное целое рациональное число g. Теорема Фалтингса утверждает, что если $g \geqslant 2$, то уравнение $F(x, y) = 0$ имеет лишь конечное число решений в любом фиксированном поле алгебраических чисел K (конечной степени над $\mathbb{Q}$). Если многочлен $F(x, y)$ имеет степень n и кривая $F(x, y) = 0$ не имеет особых точек (в том числе и бесконечно удаленных), то ее род g равен $(n-1)(n-2)/2$. Следовательно, уравнение Ферма $x^n + y^n = 1$ при $n \geqslant 4$ имеет конечное число решений не только в поле рациональных чисел $\mathbb{Q}$, но и в любом фиксированном поле алгебраических чисел K.

Теорема Туэ, которая была доказана нами в п. 3 § 3 гл. IV, также является весьма частным случаем теоремы Фалтингса, из которой следует, что уравнение $f(x, y) = c$, где $f(x, y)$ — форма степени $n > 3$ без кратных сомножителей, имеет лишь конечное число решений в любом заданном поле алгебраических чисел K, даже если рассматривать произвольные, не обязательно целые, содержащиеся в K значения для x и y. (Случай формы f степени $n = 3$ под теорему Фалтингса не подходит.) То же самое относится и к теореме Зигеля, приведенной в конце п. 3 § 6 гл. IV. Если кривая $F(x, y) = 0$ имеет род $g \geqslant 2$, то утверждение о конечности числа решений уравнения $F(x, y) = 0$ в любом фиксированном поле алгебраических чисел также следует из теоремы Фалтингса.

Уравнения степени $n \leqslant 3$ вообще являются исключениями в общей теории неопределенных уравнений с двумя неизвестными. Случай многочлена первой степени тривиален. Уравнение второй степени, левая часть которого не распадается на линейные множители, определяет кривую рода $g = 0$. Если в этом уравнении перейти к однородным координатам, то мы придем к вопросу о представлении нуля квадратичной формой от трех переменных. Для случая поля рациональных чисел этот вопрос был разобран нами в п. 2 § 7 гл. I. Но если для квадратичной формы от трех переменных мы знаем хотя бы одно представление нуля, то мы можем с помощью простых формул найти все ее представления нуля, и среди них будет бесконечно много непропорциональных представлений (см. теорему 7 и замечание к ней в п. 3 § 1 Дополнения).

Если кривая степени 3 не имеет особых точек, то ее род равен 1 (случай, когда особые точки существуют, исследуется совсем просто). Для кривых рода 1 (их называют также эллиптическими кривыми) к настоящему времени имеется хорошо

разработанная глубокая теория с многочисленными приложениями. Одна из ее особенностей — это возможность введения на множестве рациональных точек эллиптической кривой групповой операции. С теорией эллиптических кривых и ее арифметическими приложениями можно познакомиться, например, по обзорным статьям Дж. Касселса [12] и Тейта [37].

Примерами уравнений 3-й степени с бесконечным числом рациональных решений являются $x^3+y^3=6$ и $x^3+y^3=9$ (см. [9], с. 340). Из последнего примера вытекает также, что кривая Ферма $x^3+y^3=1$ имеет бесконечно много точек с координатами из поля $\mathbb{Q}(\sqrt[3]{3})$.

2. Бесконечность числа иррегулярных простых чисел. В пределах имеющихся таблиц число регулярных простых чисел больше числа иррегулярных. Однако неизвестно, будет ли это верно для любого промежутка $(1, N)$. Более того, до настоящего времени открытым является вопрос о том, будет ли вообще число регулярных чисел бесконечным. В связи с этим представляет интерес следующая теорема (см. [85] и [68]).

Теорема 2. *Число иррегулярных простых чисел бесконечно.*

Доказательство теоремы 2 основывается на некоторых свойствах чисел Бернулли. Эти свойства сформулированы и доказаны нами в следующем параграфе.

Пусть $p_1, \ldots, p_s$ — произвольная конечная система иррегулярных простых чисел. Теорема 2 будет доказана, если мы найдем иррегулярное простое число p, отличное от $p_1, \ldots, p_s$. Положим

$$n = r(p_1-1)\ldots(p_s-1).$$

Так как для числа Бернулли B_{2k} мы имеем

$$\left|\frac{B_{2k}}{2k}\right| \to \infty \quad \text{при} \quad k \to \infty$$

(см. конец § 8), то при достаточно большом натуральном r рациональное число B_n/n будет по абсолютной величине больше 1. Пусть p — простое число, входящее в его числитель (при несократимой записи). Если бы $(p-1)\mid n$, то по теореме Штаудта (теорема 4 § 8) число p входило бы в знаменатель B_n, а это не так по выбору p. Таким образом, $(p-1)\nmid n$ и, следовательно, p отлично от $p_1, \ldots, p_s$ (и отлично от 2). Обозначим через m остаток от деления n на $p-1$, так что $n = m + a(p-1)$. Ясно, что m четно и $2 \leqslant m \leqslant p-3$. Вместе с n число m также не делится на $p-1$. Воспользовавшись теперь так называемым сравнением Куммера (теорема 5 § 8), мы получаем в кольце p-целых рациональных чисел сравнение

$$B_m/m \equiv B_n/n \pmod{p}.$$

Но $B_n/n \equiv 0 \pmod{p}$, поэтому $B_m/m \equiv 0 \pmod{p}$ и $B_m \equiv 0 \pmod{p}$.

Так как m равно здесь одному из чисел $2, 4, \ldots, p-3$, то по следствию теоремы 2 § 6 число p иррегулярно. Теорема 2 доказана.

Некоторое уточнение теоремы 2, проливающее также свет и на вопрос о распределении иррегулярных простых чисел, дает следующий результат [108]. Пусть $m>2$ — произвольное натуральное число и $G=(\mathbb{Z}/m\mathbb{Z})^*$ — мультипликативная группа приведенных (обратимых) классов вычетов по модулю m. Пусть, далее, H — произвольная собственная подгруппа группы G ($H\neq G$). Тогда в объединении тех классов приведенных вычетов по модулю m, которые не входят в H, содержится бесконечно много иррегулярных простых чисел p. В частности, бесконечно много таких иррегулярных p, которые $\not\equiv 1 \pmod m$, $m>2$, или $\not\equiv \pm 1 \pmod m$, $\varphi(m)>2$. В то же время пока мы не знаем ни одного такого $m>2$, для которого класс чисел $\equiv 1 \pmod m$ содержал бы бесконечно много иррегулярных p (автор приведенной выше работы доказал, что объединение двух единичных классов $\equiv 1 \pmod 3$ и $\equiv 1 \pmod 4$ содержит бесконечно много иррегулярных p). В связи с отмеченными результатами упомянем, что имеющиеся в настоящее время таблицы иррегулярных простых чисел (см. [86], [87] и [142]) дают основание предположить, что для любого модуля $m>2$ иррегулярные простые числа асимптотически равномерно распределены по всем $\varphi(m)$ классам приведенных вычетов по модулю m (для всех простых чисел такая равномерность распределения установлена в п. 3 § 3 гл. V).

Задачи

1. Доказать, что уравнение $x^3+y^3=5z^3$ не имеет решений в целых отличных от нуля рациональных числах.

2. Доказать бесконечность числа иррегулярных простых чисел вида $4n+3$ (использовать задачи 9 и 10 § 8).

§ 8. Числа Бернулли

Докажем здесь те свойства чисел Бернулли, которыми нам приходилось пользоваться в предшествующих параграфах.

Все рассматриваемые ниже степенные ряды сходятся в некоторой окрестности начала координат, и их радиусы сходимости легко могут быть определены. Мы не будем, однако, интересоваться вопросами сходимости, так как для наших целей достаточно рассматривать эти ряды формально (исключение составляет лишь доказательство теоремы 6).

Определение. *Рациональные числа* B_m ($m\geqslant 1$), *определяемые разложением*

$$\frac{t}{e^t-1}=1+\sum_{m=1}^{\infty}\frac{B_m}{m!}t^m, \tag{1}$$

называются числами Бернулли.

Условимся в следующих сокращенных обозначениях. Если $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ — многочлен, то под $f(B)$ мы будем понимать число $a_0 + a_1 B_1 + \ldots + a_n B_n$. Аналогично, если $f(x, t)$ — степенной ряд вида $\sum_{n=0}^{\infty} f_n(x)\, t^n$, где $f_n(x)$ — многочлены, то под $f(B, t)$ будем понимать ряд $\sum_{n=0}^{\infty} f_n(B)\, t^n$. Пользуясь этими обозначениями, разложение (1), например, определяющее числа Бернулли, можно записать в виде

$$\frac{t}{e^t - 1} = e^{Bt}.$$

Легко видеть, далее, что для любого числа a

$$e^{at} e^{Bt} = e^{(a+B)t}$$

(для доказательства следует перемножить ряды, стоящие слева).

Теорема 1. *Для чисел Бернулли имеет место рекуррентное соотношение*

$$(1 + B)^m - B^m = 0 \quad при \quad m \geqslant 2, \tag{2}$$

которое в развернутой форме имеет вид

$$1 + \sum_{k=1}^{m-1} C_m^k B_k = 0, \qquad m \geqslant 2.$$

Для доказательства перепишем равенство (1) в виде

$$t = e^{(1+B)t} - e^{Bt}.$$

Сравнивая здесь коэффициенты при членах $t^m/m!$ $(m \geqslant 2)$, мы и получаем соотношение (2).

При $m = 2$ формула (2) дает нам $1 + 2B_1 = 0$, а значит, $B_1 = -1/2$.

Теорема 2. *Все числа Бернулли с нечетными индексами, кроме B_1, равны нулю*:

$$B_{2m+1} = 0 \quad при \quad m \geqslant 1. \tag{3}$$

Равенства (3) равносильны, очевидно, тому, что функция

$$\frac{t}{e^t - 1} + \frac{t}{2} = 1 + \sum_{m=2}^{\infty} \frac{B_m}{m!}\, t^m$$

четная, а это легко проверяется.

Приведем значения первых двенадцати чисел Бернулли с четными индексами:

$$B_2 = \frac{1}{6}, \quad B_4 = -\frac{1}{30}, \quad B_6 = \frac{1}{42}, \quad B_8 = -\frac{1}{30}, \quad B_{10} = \frac{5}{66},$$

$$B_{12} = -\frac{691}{2730}, \quad B_{14} = \frac{7}{6}, \quad B_{16} = -\frac{3617}{510}, \quad B_{18} = \frac{43\,867}{798},$$

$$B_{20} = -\frac{174\,611}{330}, \quad B_{22} = \frac{854\,513}{138}, \quad B_{24} = -\frac{236\,364\,091}{2730}.$$

Числа Бернулли связаны с суммами степеней чисел натурального ряда. Положим

$$S_k(n) = 1^k + 2^k + \ldots + (n-1)^k.$$

Теорема 3. *Для сумм $S_k(n)$ имеет место формула*

$$(m+1)S_m(n) = (n+B)^{m+1} - B^{m+1}, \qquad m \geqslant 1, \tag{4}$$

или в развернутом виде

$$(m+1)\,S_m(n) = \sum_{k=0}^{m} C_{m+1}^k B_k n^{m+1-k}, \qquad m \geqslant 1 \quad (B_0 = 1). \tag{5}$$

Действительно, выражение, стоящее в правой части равенства (4), равно коэффициенту при $\frac{t^{m+1}}{(m+1)!}$ в ряде $e^{(n+B)t} - e^{Bt}$. С другой стороны,

$$e^{(n+B)t} - e^{Bt} = e^{Bt}(e^{nt} - 1) = t\frac{e^{nt}-1}{e^t - 1} = t\sum_{r=0}^{n-1} e^{rt} =$$

$$= nt + \sum_{m=1}^{\infty}\left(\sum_{r=1}^{n-1} r^m\right)\frac{t^{m+1}}{m!} = nt + \sum_{m=1}^{\infty}\frac{(m+1)\,S_m(n)\,t^{m+1}}{(m+1)!},$$

что и доказывает формулу (4).

Заметим, что при $n = 1$ формула (4) совпадает с равенством (2).

Теорема 4 (теорема Штаудта). *Пусть p — простое число и m — четное число. Если $(p-1) \nmid m$, то B_m является p-целым* (т. е. B_m не содержит p в знаменателе). *Если же $(p-1) \mid m$, то pB_m есть p-целое число и $pB_m \equiv -1 \pmod p$.*

Положим в формуле (5) $n = p^r$ $(r \geqslant 1)$ и перепишем ее в виде

$$\frac{S_m(p^r)}{p^r} - B_m = \sum_{k=0}^{m-1} \frac{1}{m+1} C_{m+1}^k B_k p^{r(m-k)}. \tag{6}$$

Очевидно, что при достаточно большом r сумма, стоящая справа,

будет p-целым числом. Далее, при $k \geqslant 1$ мы имеем

$$S_m(p^{k+1}) = \sum_{u=0}^{p^k-1} \sum_{v=0}^{p-1} (u + vp^k)^m \equiv$$

$$\equiv p \sum_{u=0}^{p^k-1} u^m + mp^k \sum_u u^{m-1} \sum_v v \equiv pS_m(p^k) \pmod{p^{k+1}},$$

а значит, разность

$$\frac{S_m(p^{k+1})}{p^{k+1}} - \frac{S_m(p^k)}{p^k}, \quad k \geqslant 1, \tag{7}$$

является числом целым. Из того факта, что числа (6) и (7) p-целые, следует теперь, что разность $\dfrac{S_m(p)}{p} - B_m$ также есть p-целое число.

Нами доказано, таким образом, что pB_m является p-целым и

$$pB_m \equiv S_m(p) \pmod{p} \tag{8}$$

в кольце p-целых чисел.

С другой стороны, имеют место сравнения:

$$S_m(p) \equiv -1 \pmod{p}, \quad \text{если} \quad (p-1) \mid m; \tag{9}$$

$$S_m(p) \equiv 0 \pmod{p}, \quad \text{если} \quad (p-1) \nmid m. \tag{10}$$

В самом деле, если $(p-1) \mid m$, то $x^m \equiv 1 \pmod{p}$ при $1 \leqslant x \leqslant p-1$, а значит,

$$S_m(p) = \sum_{x=1}^{p-1} x^m \equiv \sum_{x=1}^{p-1} 1 = p - 1 \equiv -1 \pmod{p}.$$

Если же $(p-1) \nmid m$, то, выбрав первообразный корень g по модулю p, мы будем иметь

$$S_m(p) = \sum_{x=1}^{p-1} x^m \equiv \sum_{r=0}^{p-2} g^{mr} = \frac{g^{(p-1)m} - 1}{g^m - 1} \equiv 0 \pmod{p},$$

так как $g^{p-1} \equiv 1 \pmod{p}$ и $g^m \not\equiv 1 \pmod{p}$.

Сопоставляя теперь (8) и (10), мы получаем, что если $(p-1) \nmid m$, то $pB_m \equiv 0 \pmod{p}$, а значит, B_m является p-целым. Из сравнений (8) и (9) следует второе утверждение теоремы 4.

В случае $m \leqslant p-1$ число $p-1$ не является делителем чисел $k < m$, поэтому все B_k при $k < m$ являются p-целыми, и, значит, все слагаемые в сумме, стоящей справа в равенстве (6), делятся на p^2. Следовательно, справедливо следующее утверждение.

Следствие. *Если* $p \neq 2$ *и* $m \leqslant p-1$ (m *четное*), *то*

$$pB_m \equiv S_m(p) \pmod{p^2}. \tag{11}$$

Теорема 5 (сравнение Куммера). *Если p простое и $p-1$ не делит четное положительное m, то число $\frac{B_m}{m}$ является p-целым и имеет место сравнение*

$$\frac{B_{m+p-1}}{m+p-1} \equiv \frac{B_m}{m} \pmod{p}. \tag{12}$$

Другими словами, отношения $\frac{B_m}{m}$ (при $(p-1) \nmid m$) имеют период $p-1$ по модулю p.

Приведем доказательство, основанное на одном сравнении Вороного (см. [7], т. 1, с. 7—23).

Воспользуемся опять формулой (6). Из этой формулы следует сравнение

$$S_m(p^r) \equiv p^r B_m \pmod{p^{2r-\sigma_m}}, \tag{13}$$

где σ_m — наименьшее целое неотрицательное число такое, что все рациональные числа $\frac{1}{m+1} B_k p^{\sigma_m}$ $(0 \leqslant k \leqslant m-1)$ являются p-целыми. Пусть a — целое число, взаимно простое с p. Для каждого $i = 1, \ldots, p^r - 1$ через b_i обозначим наименьший положительный вычет произведения ai по модулю p^r:

$$ai = b_i + p^r q_i, \qquad 0 < b_i < p^r. \tag{14}$$

Ясно, что все b_i — это те же числа $1, \ldots, p^r - 1$, но расположенные в другом порядке. Из (14) следует, что

$$a^m i^m \equiv b_i^m + m b_i^{m-1} q_i \cdot p^r \pmod{p^{2r}}$$

и, следовательно,

$$a^m S_m(p^r) \equiv S_m(p^r) + m \left(\sum_{i=1}^{p^r-1} b_i^{m-1} q_i \right) p^r \pmod{p^{2r}},$$

т. е. $(a^m - 1) S_m(p^r) \equiv m \left(\sum_{i=1}^{p^r-1} b_i^{m-1} q_i \right) p^r \pmod{p^{2r}}$. Вместе с (13) это дает нам сравнение

$$(a^m - 1) B_m \equiv m \left(\sum_{i=1}^{p^r-1} b_i^{m-1} q_i \right) \pmod{p^{r-\sigma_m}}.$$

Будем теперь считать, что $r > \sigma_m + \nu_p(m)$, и в качестве a возьмем первообразный корень по модулю p. Тогда $a^m - 1$ не будет делиться на p (поскольку $p-1$ не делит m по условию), и мы получаем, что B_m/m является p-целым числом.

Далее, пусть $m' \equiv m \pmod{p-1}$, и пусть r выбрано бо́льшим, чем $\sigma_m + \nu_p(m)$ и $\sigma_{m'} + \nu_p(m')$. Тогда

$$(a^m - 1)\frac{B_m}{m} \equiv \sum_{i=1}^{p^r-1} b_i^{m-1} q_i \pmod{p}$$

и

$$(a^{m'} - 1)\frac{B_{m'}}{m'} \equiv \sum_{i=1}^{p^r-1} b_i^{m'-1} q_i \pmod{p}.$$

Но $x^m \equiv x^{m'} \pmod{p}$ при любом целом x, поэтому $B_{m'}/m' \equiv B_m/m \pmod{p}$, и теорема 5 доказана.

Теорема 6. *Для чисел Бернулли B_{2m} имеет место формула*

$$B_{2m} = (-1)^{m-1}\frac{2\,(2m)!}{(2\pi)^{2m}}\,\zeta(2m), \tag{15}$$

где $\zeta(2m)$ — значение ζ-функции Римана $\zeta(s)$ при $s = 2m$.

Для доказательства воспользуемся разложением функции $\frac{1}{e^t - 1}$ на простейшие дроби:

$$\frac{1}{e^t - 1} = -\frac{1}{2} + \sum_{n=-\infty}^{+\infty} \frac{1}{t - 2\pi i n} = -\frac{1}{2} + \frac{1}{t} + \sum_{n=1}^{\infty} \frac{2t}{t^2 + (2\pi n)^2}. \tag{16}$$

Это разложение можно, например, вывести из чаще встречающегося в учебниках разложения для котангенса

$$\operatorname{ctg} z = \frac{1}{z} + \sum_{n=1}^{\infty} \frac{2z}{z^2 - (\pi n)^2},$$

воспользовавшись тем, что $\operatorname{ctg} z = i\,\frac{e^{iz} + e^{-iz}}{e^{iz} - e^{-iz}} = i + \frac{2i}{e^{2iz} - 1}$. Из (16) следует, что

$$\frac{t}{e^t - 1} = 1 - \frac{t}{2} + 2\sum_{n=1}^{\infty} \frac{t^2}{t^2 + (2\pi n)^2},$$

и так как $\dfrac{t^2}{t^2 + (2\pi n)^2} = \sum\limits_{m=1}^{\infty} (-1)^{m-1}\left(\dfrac{t}{2\pi n}\right)^{2m}$, то

$$\frac{t}{e^t - 1} = 1 - \frac{t}{2} + 2\sum_{n=1}^{\infty}\sum_{m=1}^{\infty} (-1)^{m-1}\frac{t^{2m}}{(2\pi n)^{2m}} =$$

$$= 1 - \frac{t}{2} + \sum_{m=1}^{\infty} (-1)^{m-1}\frac{2\zeta(2m)}{(2\pi)^{2m}}\,t^{2m}.$$

Сопоставив это равенство с разложением (1) и приравняв коэффициенты, мы и получим равенство (15).

Из формулы (15) можно получить представление о росте чисел $|B_{2m}|$ при возрастании индекса. Так как $\zeta(2m) > 1$ и $(2m)! > (2m/e)^{2m}$ (это следует из известной формулы Стирлинга), то $|B_{2m}| > 2\left(\frac{m}{\pi e}\right)^{2m}$. В частности, мы получаем, что

$$\left|\frac{B_{2m}}{2m}\right| \to \infty \quad \text{при} \quad m \to \infty.$$

Замечание 1. Формуле (15) можно придать более естественную с теоретико-числовой точки зрения форму, исключив из нее трансцендентные величины. Как хорошо известно, функция $\zeta(s)$ допускает аналитическое продолжение на всю плоскость комплексного переменного s, является на ней мероморфной функцией с единственным полюсом первого порядка в точке $s = 1$ (с вычетом 1) и удовлетворяет функциональному уравнению

$$2^{s-1}\pi^s \zeta(1-s) = \cos\frac{s\pi}{2}\,\Gamma(s)\,\zeta(s), \tag{17}$$

где $\Gamma(s)$ — гамма-функция. Положим здесь $s = 2m$. Так как $\Gamma(2m) = (2m-1)!$, то формула (15) преобразуется к виду $\zeta(1-2m) = -B_{2m}/(2m)$ $(m \geqslant 1)$. Если теперь принять во внимание, что при $m \geqslant 1$ одновременно $\zeta(-2m) = 0$ и $B_{2m+1} = 0$, то приходим к формуле

$$\zeta(1-n) = -B_n/n, \qquad n > 1. \tag{18}$$

Формулы (18) указывают нам на наличие глубоких свойств функции $\zeta(s)$, выражающихся в арифметической природе некоторых ее значений.

Формулы, аналогичные формуле (18), имеют место и для значений L-функций $L(s, \chi)$, рассматривавшихся в § 2 настоящей главы. Именно, если χ — примитивный числовой характер по модулю $m > 1$, то $L(s, \chi)$ допускает аналитическое продолжение до голоморфной функции на всей комплексной плоскости и для любого натурального $n \geqslant 1$ имеет место формула

$$L(1-n, \chi) = -B_{n,\chi}/n. \tag{19}$$

В этой формуле $B_{n,\chi}$ — обобщенные числа Бернулли, связанные с числовым характером χ (все они содержатся в поле, получающемся присоединением к $\mathbb{Q}$ всех значений характера χ).

Обобщенные числа Бернулли оказались весьма полезными в теории круговых полей. В частности, с их помощью можно дать более простые выражения для множителя $h^*(l)$ числа классов. Приведем определение обобщенных чисел Бернулли $B_{n,\chi}$ и сформулируем некоторые их простейшие свойства.

Пусть m — произвольное натуральное число (допускается $m=1$) и χ — фиксированный примитивный числовой характер по модулю m. Числа $B_{n,\chi}$ определяются разложением по степеням t мероморфной функции, стоящей слева:

$$\sum_{a=1}^{m} \frac{\chi(a)\, te^{at}}{e^{mt}-1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}.$$

Если $m=1$ и $\chi=1$ — единичный характер (т. е. $\chi(a)=1$ при всех целых рациональных a), то $B_{n,1}=B_n$ при $n\geqslant 2$, $B_{1,1}=1/2$. Аналогом соотношения (2) (в развернутой форме) для чисел $B_{n,\chi}$ является формула

$$\sum_{k=1}^{n-1} C_n^k B_{k,\chi} m^{n-k} = n \sum_{a=1}^{m} \chi(a)\, a^{n-1}, \qquad n\geqslant 1.$$

В частности, при $\chi\neq 1$ $(m>1)$ имеем

$$B_{0,\chi}=0, \qquad B_{1,\chi}=\frac{1}{m}\sum_{a=1}^{m}\chi(a)\, a.$$

Далее, $B_{n,\chi}=0$, если $\chi(-1)\neq(-1)^n$, т. е. если характер χ и число n разной четности, кроме случая $n=1$ и $\chi=1$ (это аналог теоремы 2). Обобщением для (5) является формула

$$(n+1)\left(\sum_{a=1}^{rm}\chi(a)\, a^n\right) = \sum_{k=0}^{n} C_{n+1}^k B_{k,\chi}(rm)^{n+1-k}.$$

Пользуясь обобщенными числами Бернулли, мы можем формулу (21) § 2 для нечетного примитивного характера χ по модулю m переписать в виде $L(1,\chi)=\frac{\pi i\tau(\chi)}{m} B_{1,\bar{\chi}}$. Отсюда получается новое выражение для первого множителя h^* числа классов дивизоров l-кругового поля:

$$h^*=h^*(l)=2l\prod_{\chi(-1)=-1}\left(-\frac{1}{2}B_{1,\chi}\right),$$

где χ пробегает все нечетные характеры по простому модулю l.

Замечание 2. Сравнение Куммера (12) допускает обобщение на случай модуля, являющегося степенью простого числа p. Именно, если m и n — четные натуральные числа, не делящиеся на $p-1$ и удовлетворяющие сравнению $m\equiv n \pmod{(p-1)p^N}$, то

$$(1-p^{m-1})B_m/m \equiv (1-p^{n-1})B_n/n \pmod{p^{N+1}}. \tag{20}$$

Доказательство сравнений (20) основывается на тех же соображениях, что и доказательство теоремы 5 (см. [38], с. 239). Этим сравнениям можно придать следующий смысл. Будем считать, что $p\neq 2$, и для четного $a=0,\ 2,\ \ldots,\ p-3$ через C_a обозначим

множество натуральных чисел m, сравнимых с a по модулю $p-1$. На числах $m \in C_a$ зададим функцию

$$F_a(m) = (1-p^{m-1})B_m/m. \tag{21}$$

Сравнения (20) означают, что при $a \neq 0$ функция $F_a(m)$ непрерывна на C_a в смысле p-адической метрики (значения $F_a(m)$ и $F_a(n)$ сколь угодно близки друг к другу, если только аргументы m и n достаточно близки). Но множество C_a всюду плотно в кольце целых p-адических чисел $\mathbb{Z}_p$, поэтому функцию $F_a(m)$ можно продолжить до непрерывной функции на $\mathbb{Z}_p$ с целыми p-адическими значениями.

Леопольдт [99] обратил внимание на следующее обстоятельство. В силу формулы (18) функция F_a может быть задана также равенством

$$F_a(m) = -(1-p^{m-1})\zeta(1-m), \qquad m \in C_a.$$

Распространение функции F_a с C_a на $\mathbb{Z}_p$ можно интерпретировать теперь как p-адическое продолжение функции $-\left(1-\frac{1}{p^s}\right)\zeta(s)$, заданной на точках $1-m$, $m \in C_a$, на все кольцо целых p-адических чисел $\mathbb{Z}_p$. Обозначим это продолжение через $\zeta_{p,a}(s)$. Все функции $\zeta_{p,a}(s)$ при $a = 2, 4, \ldots, p-3$ являются аналитическими функциями от p-адического аргумента $s \in \mathbb{Z}_p$. (Связи между введенными функциями будут отмечены в замечании 3.)

Некоторое усовершенствование приведенной конструкции позволяет построить функцию $\zeta_{p,0}(s)$ и при $a = 0$. Ее значения $\zeta_{p,0}(1-m)$ при $m \in C_0$ также совпадают с $-(1-p^{m-1})\zeta(1-m)$, однако эта функция будет голоморфной во всех точках $s \in \mathbb{Z}_p$, кроме точки $s = 1$, где она имеет особенность — полюс 1-го порядка.

Подчеркнем еще раз, что построенные нами функции $\zeta_{p,a}(s)$ (число их равно $(p-1)/2$) являются p-адическими продолжениями функции $-\left(1-\frac{1}{p^s}\right)\zeta(s)$, а не дзета-функции Римана $\zeta(s)$. Этому обстоятельству, т. е. необходимости введения указанного множителя, можно дать следующее эвристическое объяснение (но не строгое обоснование). Умножение $\zeta(s)$ на множитель $1-\frac{1}{p^s}$ означает, что из эйлерова произведения для $\zeta(s)$ выброшен сомножитель, соответствующий простому числу p. При переходе от эйлерова произведения к ряду $\sum n^{-s}$ это соответствует удалению из ряда всех слагаемых с n, делящимися на p. А присутствие таких слагаемых явно привело бы к p-адической расходимости ряда. (Выбрасывание из ряда членов, влекущих очевидную расходимость, является обычным приемом регуляризации расходящихся рядов; специфика нашего случая заключается в

том, что эту операцию мы производим при $s = 1 - m$, т. е. вне области сходимости $\operatorname{Re} s > 1$ ряда $\sum n^{-s}$.)

Замечание 3. Аналогичным образом могут быть построены p-адические продолжения и для L-рядов $L(s, \chi)$ с произвольным примитивным характером χ. Основную роль в этом построении играют обобщенные числа Бернулли $B_{n,\chi}$ и формула (19).

Согласно задаче 3 § 3 гл. I отображение $c \to \gamma(c) = \lim\limits_{n\to\infty} c^{p^n}$, $c \in \mathbb{Z}$, $(c, p) = 1$, является примитивным характером по модулю p, значения которого $\gamma(c)$ содержатся в кольце целых p-адических чисел. Рассматривая произвольный числовой характер χ, мы можем считать, что все его значения $\chi(a)$, а значит, и все числа $B_{n,\chi}$ содержатся в некотором конечном расширении поля $\mathbb{Q}_p$. Имеет место следующий результат.

Для произвольного примитивного числового характера χ и произвольного простого числа p существует p-адическая функция $L_p(s, \chi)$, определенная на целых p-адических числах s (кроме точки $s = 1$ в случае единичного характера $\chi = 1$), обладающая свойством

$$L_p(1 - n, \chi) = -(1 - (\chi\gamma^{-n})(p) \cdot p^{n-1}) B_{n,\chi\gamma^{-n}}/n, \quad n \geqslant 1. \tag{22}$$

Если $\chi \neq 1$, то $L_p(s, \chi)$ — аналитическая функция. Если же $\chi = 1$, то $L_p(s, 1)$ — мероморфная функция целого p-адического аргумента s с единственным полюсом 1-го порядка в точке $s = 1$. Для нечетного характера χ функция $L_p(s, \chi)$ равна тождественно нулю. Если же χ — четный характер, то $L_p(s, \chi)$ — ненулевая функция.

Для характера $\chi = \gamma^a$ и для $m \in C_a$ имеем

$$L_p(1 - m, \gamma^a) = -(1 - p^{m-1}) B_m/m = F_a(m).$$

Таким образом, построенные в замечании 2 функции $\zeta_{p,a}(s)$ совпадают с $L_p(s, \gamma^a)$.

Пусть теперь F — вещественное абелево расширение поля рациональных чисел степени n, соответствующее конечной подгруппе X группы числовых характеров $\hat{x}$ (см. замечание в конце п. 1 § 2). Так как F — вполне вещественное поле, то, согласно замечанию к теореме 1 § 6, для F и для произвольного простого числа p определен p-адический регулятор $\mathrm{R}_p(F)$. Справедлива, оказывается, следующая формула:

$$\frac{2^{n-1} h(F) \mathrm{R}_p(F)}{\sqrt{D(F)}} = \prod_{\chi \in X, \chi \neq 1} \left(1 - \frac{\chi(p)}{p}\right)^{-1} L_p(1, \chi), \tag{23}$$

в которой $h(F)$ — число классов дивизоров и $D(F)$ — дискриминант поля F (p-адический регулятор и квадратный корень из дискриминанта определены с точностью до знака, поэтому в равенстве (23) необходимо надлежащее согласование этих знаков).

Приведенная формула является p-адическим аналогом формулы, указанной в конце п. 3 § 2. Там же отмечалось, что для вещественных подполей деления круга p-адический регулятор отличен от нуля. Следовательно, для четных числовых характеров χ всегда $L_p(1, \chi) \neq 0$.

В p-адическом поле число 1 может быть представлено в виде предела чисел вида $1-n$ с натуральными n. Поэтому ввиду формулы (22) значения $L_p(1, \chi)$ могут быть p-адически аппроксимированы обобщенными числами Бернулли. Это дает возможность вывести сравнения (по модулю p^N), связывающие левую часть формулы (23) с числами $B_{n,\chi}$.

По поводу замечаний 1, 2 и 3 см. работы [98], [99], [90], [28], [31].

Замечание 4. Клинген и Зигель показали, что для любого вполне вещественного поля алгебраических чисел K значения дзета-функции Дедекинда $\zeta_K(s)$ в целых отрицательных точках всегда являются рациональными числами. Это открывает возможность построения p-адических продолжений и для таких функций (см. [131], [36]).

Задачи

1. Доказать, что $(x+B)^m = (x-1-B)^m$, $m \geqslant 1$.
2. Доказать, что $\left(\frac{1}{2}+B\right)^m = \left(\frac{1}{2^{m-1}}-1\right)B_m$.
3. Пусть p — простое число $\neq 2$. Доказать, что
$$\sum_{x=1}^{(p-1)/2} x^{\frac{p-1}{2}} \equiv 2\left(\left(\frac{2}{p}\right)-2\right)B_{(p+1)/2} \pmod p.$$
4. Пусть $p > 3$ — простое число вида $4k+3$. Доказать, что число h классов дивизоров мнимого квадратичного поля $\mathbb{Q}(\sqrt{-p})$ удовлетворяет сравнению
$$h \equiv -2B_{(p+1)/2} \pmod p.$$
5. Доказать, что при простом $p > 3$
$$1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{p-1} \equiv 0 \pmod{p^2}.$$
6. Доказать формулу
$$(kx+B)^m = k^{m-1}\sum_{s=0}^{k-1}\left(x+\frac{s}{k}+B\right)^m$$
(k и m — натуральные числа).
7. Для функции $\operatorname{tg} x$ имеет место разложение
$$\operatorname{tg} x = \sum_{n=1}^{\infty} T_n \frac{x^{2n-1}}{(2n-1)!},$$

где $T_n = 2^{2n}(2^{2n}-1)\dfrac{|B_{2n}|}{2n}$. Доказать, что все коэффициенты T_n — натуральные числа.

8. Доказать, что при $m > 1$

$$2B_{2m} \equiv 1 \pmod 4.$$

9. Пусть q — такое простое число, что $2q+1$ составное (например, $q \equiv 1 \pmod 3$). Доказать, что числитель числа Бернулли B_{2q} содержит (в несократимой записи) простое число вида $4n+3$.

10. Пусть $p_1, \ldots, p_s$ — простые числа, бо́льшие 3, $M = (p_1-1)\ldots(p_s-1)$ и q — натуральное число, удовлетворяющее сравнению $q \equiv 1 \pmod M$. Доказать, что ни одно из простых чисел $p_1, \ldots, p_s$ не входит в числитель дроби $B_{2q}/(2q)$.

§ 1. Квадратичные формы над произвольным полем характеристики $\neq 2$

В этом параграфе мы изложим ряд общих сведений о квадратичных формах над произвольным полем. В случае общеизвестных фактов мы ограничимся лишь формулировкой результатов. Через K будем обозначать, без дополнительных оговорок, произвольное поле, характеристика которого отлична от 2. Для любой прямоугольной матрицы A через A' обозначается транспонированная с A матрица.

1. Эквивалентность квадратичных форм. *Квадратичной формой над полем* K называется однородный многочлен второй степени с коэффициентами из K. Всякую квадратичную форму f можно записать в виде $f = \sum_{i,j=1}^{n} a_{ij}x_ix_j$, где $a_{ij} = a_{ji}$. Симметрическая матрица $A = (a_{ij})$ называется *матрицей квадратичной формы* f. Заданием своей матрицы квадратичная форма вполне определена с точностью до наименования переменных. Определитель $d = \det A$ называется определителем квадратичной формы f. Если $d = 0$, то форма f называется особенной, в противном случае — неособенной. Обозначая через X столбец из переменных $x_1, x_2, \ldots, x_n$, мы можем квадратичную форму f записать в виде $f = X'AX$.

Пусть вместо переменных $x_1, \ldots, x_n$ введены новые переменные $y_1, \ldots, y_n$ по формулам

$$x_i = \sum_{j=1}^{n} c_{ij}y_j, \qquad 1 \leqslant i \leqslant n, \quad c_{ij} \in K.$$

В матричной форме это линейное преобразование можно записать в виде $X = CY$, где Y — столбец из переменных $y_1, \ldots, y_n$, а C — матрица (c_{ij}). Подставив в квадратичную форму f вместо $x_1, \ldots, x_n$ их выражения через $y_1, \ldots, y_n$, мы получим (после выполнения всех необходимых действий) новую квадратичную форму g (также над полем K) от переменных $y_1, \ldots, y_n$. Матрица A_1 квадратичной формы g равна

$$A_1 = C'AC. \tag{1}$$

Две квадратичные формы f и g называются *эквивалентными*, $f \sim g$, если существует неособенное линейное преобразование пе-

ременных, при котором одна из этих форм переходит в другую (с точностью до наименования переменных). Из формулы (1) вытекает

Теорема 1. *Если две квадратичные формы эквивалентны, то их определители отличаются друг от друга на не равный нулю множитель, являющийся квадратом в K.*

Пусть γ — произвольный элемент из K. Если в K существуют элементы $\alpha_1, \ldots, \alpha_n$, для которых $f(\alpha_1, \ldots, \alpha_n) = \gamma$, то говорят, что квадратичная форма f *представляет* γ. Другими словами, элемент γ представим формой f, если он является значением этой формы при некоторых значениях переменных. Легко видеть, что эквивалентные квадратичные формы представляют одни и те же элементы поля K.

Мы говорим, далее, что форма f *представляет в поле K нуль*, если существуют не равные одновременно нулю значения переменных $x_i = \alpha_i \in K$ $(1 \leqslant i \leqslant n)$, при которых $f(\alpha_1, \ldots, \alpha_n) = 0$. Свойство формы представлять нуль сохраняется, очевидно, при переходе к эквивалентной форме.

Теорема 2. *Если квадратичная форма f от n переменных представляет элемент $\alpha \neq 0$, то она эквивалентна форме вида $\alpha x_1^2 + g(x_2, \ldots, x_n)$, где g — квадратичная форма от $n-1$ переменных.*

Относительно доказательства этой теоремы заметим лишь следующее. Если $f(\alpha_1, \ldots, \alpha_n) = \alpha$, то не все α_i равны нулю, поэтому мы можем построить неособенную матрицу C, первая строчка которой будет состоять из $\alpha_1, \ldots, \alpha_n$. Если теперь форму f мы подвергнем линейному преобразованию переменных с матрицей C, то получим форму, у которой коэффициент при квадрате первой переменной будет равен α. Далее доказательство проводится, как обычно.

Если матрица квадратичной формы диагональна (т. е. все коэффициенты при произведениях различных переменных равны нулю), то такую форму будем называть также *диагональной*. Из теоремы 2 легко следует

Теорема 3. *Всякая квадратичная форма над полем K при помощи неособенного линейного преобразования переменных может быть преобразована в диагональную форму. Другими словами, всякая квадратичная форма эквивалентна некоторой диагональной форме.*

В терминах матриц теорема 3 означает, что для любой симметрической матрицы A существует такая неособенная матрица C, что матрица $C'AC$ диагональна.

2. Прямая сумма квадратичных форм. Так как наименование переменных не играет существенной роли, то мы можем считать, что две данные квадратичные формы f и g не имеют общих переменных. В этом случае форма $f+g$ называется *прямой суммой* форм f и g и обозначается через $f \dotplus g$ (не смешивать с обычным

сложением квадратичных форм, содержащих одни и те же переменные). Очевидно, что если $g \sim h$, то $f+g \sim f+h$. Оказывается, последний факт допускает обращение.

Теорема 4 (теорема Витта). *Пусть f, g и h — неособенные квадратичные формы над полем K. Если формы $f+g$ и $f+h$ эквивалентны, то формы g и h также эквивалентны.*

Доказательство. Пусть f_0 — диагональная форма, эквивалентная форме f. Тогда, как отмечено выше, $f+g \sim f_0+g$ и $f+h \sim f_0+h$, откуда $f_0+g \sim f_0+h$. Таким образом, мы можем считать, что f — диагональная форма. Легко видеть теперь, что для доказательства теоремы достаточно рассмотреть случай, когда $f = ax_0^2$, $a \neq 0$. Обозначим через A и B матрицы форм g и h соответственно. Так как формы ax_0^2+g и ax_0^2+h эквивалентны, то существует матрица $C = \begin{pmatrix} \gamma & S \\ T & Q \end{pmatrix}$ такая, что

$$\begin{pmatrix} \gamma & T' \\ S' & Q' \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & A \end{pmatrix} \begin{pmatrix} \gamma & S \\ T & Q \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & B \end{pmatrix}.$$

(Здесь S обозначает строчку, а T — столбец.) Из этого равенства получаем

$$\gamma^2 a + T'AT = a, \tag{2}$$

$$\gamma aS + T'AQ = 0, \tag{3}$$

$$S'aS + Q'AQ = B. \tag{4}$$

Нам надо доказать, что существует неособенная матрица C_0, такая, что $C_0'AC_0' = B$. Матрицу C_0 будем искать в виде

$$C_0 = Q + \xi TS,$$

где элемент ξ должен быть надлежащим образом подобран. В силу (2) и (3) имеем

$$C_0'AC_0 = (Q' + \xi S'T')A(Q + \xi TS) =$$
$$= Q'AQ + \xi S'T'AQ + \xi Q'ATS + \xi^2 S'T'ATS =$$
$$= Q'AQ + a[(1-\gamma^2)\xi^2 - 2\gamma\xi]S'S.$$

Согласно равенству (4) последнее выражение будет равно матрице B, если $(1-\gamma^2)\xi^2 - 2\gamma\xi = 1$. Полученное уравнение, которое можно записать также в виде $\xi^2 - (\gamma\xi + 1)^2 = 0$, относительно неизвестной ξ при любом $\gamma \in K$ имеет в поле K решение ξ_0 (напомним, что характеристика K не равна 2). Таким образом, мы нашли матрицу $C_0 = Q + \xi_0 TS$, для которой $C_0'AC_0 = B$. Так как по предположению матрица B неособенная, то C_0 — также неособенная. Теорема 4, таким образом, доказана.

3. Представление элементов поля.

Теорема 5. *Если неособенная квадратичная форма представляет нуль в поле K, то она представляет также все элементы из K.*

Доказательство. Так как эквивалентные формы представляют одни и те же элементы поля, то достаточно доказать теорему для диагональной формы $f = a_1x_1^2 + \ldots + a_nx_n^2$. Пусть $a_1\alpha_1^2 + \ldots + a_n\alpha_n^2 = 0$ — представление нуля, и пусть γ — произвольный элемент поля K. Мы можем считать, что $\alpha_1 \neq 0$. Придадим переменным $x_1, \ldots, x_n$ значения:

$$x_1 = \alpha_1(1+t), \qquad x_k = \alpha_k(1-t), \qquad k = 2, \ldots, n,$$

где t — новая переменная. Подставив эти значения переменных в нашу форму f, получим

$$f^* = f^*(t) = 2a_1\alpha_1^2t - 2a_2\alpha_2^2t - \ldots - 2a_n\alpha_n^2t = 4a_1\alpha_1^2t.$$

Если мы теперь положим $t = \dfrac{\gamma}{4a_1\alpha_1^2}$, то получим значение $f^* = \gamma$.

Теорема 6. *Неособенная квадратичная форма f представляет элемент $\gamma \neq 0$ из K тогда и только тогда, когда форма $-\gamma x_0^2 + f$ представляет нуль.*

Доказательство. Необходимость условия очевидна. Допустим, что $-\gamma\alpha_0^2 + f(\alpha_1, \ldots, \alpha_n) = 0$, причем не все α_i равны нулю. Если $\alpha_0 \neq 0$, то $\gamma = f\left(\dfrac{\alpha_1}{\alpha_0}, \ldots, \dfrac{\alpha_n}{\alpha_0}\right)$. Если же $\alpha_0 = 0$, то форма f представляет нуль, а тогда, по теореме 5, она представляет все элементы поля K.

Замечание. Из доказательства теоремы 6 ясно, что мы получим все представления элемента γ формой f, если только нам будут известны все представления нуля формой $-\gamma x_0^2 + f$ (достаточно знать все те представления, для которых $x_0 \neq 0$). Таким образом, вопрос о представлениях неособенными квадратичными формами отличных от нуля элементов поля K целиком сводится к вопросу о представлениях нуля для неособенных форм, число переменных которых на единицу больше.

Теорема 7. *Если для формы f, представляющей нуль, известно какое-нибудь одно представление нуля, то можно найти неособенное линейное преобразование переменных, при котором форма f преобразуется к виду $y_1y_2 + g(y_3, \ldots, y_n)$.*

Доказательство. Следуя доказательству теоремы 5, прежде всего находим такие $\alpha_1, \ldots, \alpha_n$, что $f(\alpha_1, \ldots, \alpha_n) = 1$. По теореме 2 мы можем преобразовать f к виду $x_1^2 + f_1(x_2, \ldots, x_n)$. Так как для формы $x_1^2 + f_1$ мы знаем представление нуля, то найдутся, очевидно, такие $\beta_2, \ldots, \beta_n$, что $f_1(\beta_2, \ldots, \beta_n) = -1$.

Опять применяя теорему 2, приводим f_1 к виду $-x_2^2+g(y_3, \ldots, y_n)$. Полагая $x_1-x_2=y_1$, $x_1+x_2=y_2$, получаем требуемый результат.

Замечание. Предположим, что для всякой квадратичной формы над полем K, представляющей нуль в этом поле, мы умеем находить хотя бы одно представление нуля. Тогда любую неособенную форму мы сможем преобразовать к виду

$$y_1y_2+\ldots+y_{2s-1}y_{2s}+h(y_{2s+1}, \ldots, y_n), \tag{5}$$

где форма h уже не представляет нуля. Для произвольного представления нуля формой (5) значение хоть одной из переменных $y_1, y_2, \ldots, y_{2s-1}, y_{2s}$ отлично от нуля. Чтобы найти все те представления, для которых, например, $y_1=\alpha_1\neq 0$, мы должны переменным $y_3, \ldots, y_n$ придать произвольные значения $\alpha_3, \ldots, \alpha_n$, а значение для y_2 определить из уравнения

$$\alpha_1y_2+\alpha_3\alpha_4+\ldots+g(\alpha_{2s+1}, \ldots, \alpha_n)=0.$$

Таким образом, задача эффективного нахождения всех представлений нуля (в поле K) произвольной неособенной квадратичной формой будет решена, если только будет известен критерий, позволяющий узнавать, представляет данная форма нуль или нет, и, кроме того, если будет указан алгоритм, с помощью которого для всякой формы, представляющей нуль, можно будет найти хоть одно представление нуля.

Теорема 8. *Пусть поле K содержит более пяти элементов. Если диагональная форма $a_1x_1^2+\ldots+a_nx_n^2$, $a_i\in K$, представляет в поле K нуль, то для нее существует такое представление нуля, при котором значения всех переменных отличны от нуля.*

Доказательство. Докажем сначала, что если $a\xi^2=\lambda\neq 0$, то для любого $b\neq 0$ существуют такие отличные от нуля элементы α и β, что $a\alpha^2+b\beta^2=\lambda$. Для доказательства этого факта рассмотрим тождество

$$\frac{(t-1)^2}{(t+1)^2}+\frac{4t}{(t+1)^2}=1.$$

Умножив это тождество на $a\xi^2=\lambda$, мы получим

$$a\left(\xi\frac{t-1}{t+1}\right)^2+at\left(\frac{2\xi}{t+1}\right)^2=\lambda. \tag{6}$$

Выберем теперь в поле K элемент $\gamma\neq 0$ так, чтобы значение $t=t_0=\frac{b\gamma^2}{a}$ было отлично от ± 1. Поскольку каждое из уравнений $bx^2-a=0$ и $bx^2+a=0$ относительно x имеет в поле K не более двух решений, то всего в поле K имеем самое большее пять элементов, которые нельзя взять в качестве γ. Так как по условию поле K содержит более пяти элементов, то требуемый элемент γ

существует. Полагая в тождестве (6) $t = t_0$, получаем

$$a\left(\xi\frac{t_0-1}{t_0+1}\right)^2 + b\left(\frac{2\xi\gamma}{t_0+1}\right)^2 = \lambda,$$

и наше утверждение доказано. Теперь уже легко завершить доказательство теоремы. Если представление $a_1\xi_1^2 + \ldots + a_n\xi_n^2 = 0$ таково, что $\xi_1 \neq 0, \ldots, \xi_r \neq 0, \xi_{r+1} = \ldots = \xi_n = 0$, где $r \geqslant 2$, то, по доказанному, можно найти такие $\alpha \neq 0$ и $\beta \neq 0$, что $a_r\xi_r^2 = a_r\alpha^2 + a_{r+1}\beta^2$, и мы получаем представление, у которого число не равных нулю значений переменных на единицу больше. Повторяя этот прием несколько раз, мы наконец придем к такому представлению, у которого все значения переменных отличны от нуля.

4. Бинарные квадратичные формы. *Бинарными* называются квадратичные формы от двух переменных.

Теорема 9. *Все неособенные бинарные формы, представляющие нуль в поле K, эквивалентны между собой.*

Действительно, по теореме 7 все такие формы эквивалентны форме y_1y_2.

Теорема 10. *Для того чтобы бинарная квадратичная форма f с определителем $d \neq 0$ допускала представление нуля, необходимо и достаточно, чтобы элемент $-d$ был квадратом в K* (т. е. $-d = \alpha^2$, $\alpha \in K$).

Доказательство. Необходимость условия вытекает из теорем 1 и 7. Обратно, если $f = ax^2 + by^2$ и $-d = -ab = \alpha^2$, то $f(\alpha, a) = a\alpha^2 + ba^2 = 0$.

Теорема 11. *Для того чтобы две неособенные бинарные квадратичные формы f и g были эквивалентны над полем K, необходимо и достаточно, чтобы, во-первых, их определители отличались на множитель, являющийся квадратом в K, и, во-вторых, чтобы в K существовал хоть один отличный от нуля элемент, представимый одновременно обеими формами f и g.*

Доказательство. Необходимость обоих условий очевидна. Для доказательства достаточности выберем в K элемент $\alpha \neq 0$, представимый формами f и g. По теореме 2 формы f и g эквивалентны соответственно формам вида $f_1 = \alpha x^2 + \beta y^2$ и $g_1 = \alpha x^2 + \beta' y^2$. Но по первому условию $\alpha\beta$ должно отличаться от $\alpha\beta'$ на множитель, являющийся квадратом, поэтому $\beta' = \beta\gamma^2$, $\gamma \in K$, а значит, $f_1 \sim g_1$ и $f \sim g$.

Задачи

1. Доказать, что особенная квадратичная форма всегда представляет нуль.

2. Доказать, что для особенных квадратичных форм теорема 5, вообще говоря, не имеет места.

3. Доказать, что если бинарная форма $x^2 - \alpha y^2$ представляет элементы γ_1 и γ_2 из K, то она представляет и их произведение $\gamma_1\gamma_2$.

4. Показать, что теорема 8 перестает быть справедливой для полей, число элементов которых не превосходит пяти.

5. Рассмотрим разбиение всех неособенных квадратичных форм от $n = 0, 1, 2, \ldots$ переменных над данным полем K на так называемые *классы Витта* (нуль мы трактуем здесь как неособенную форму от пустого множества переменных и считаем, что эта форма не представляет нуля). Мы говорим, что формы f_1 и f_2 принадлежат одному и тому же классу Витта $[f_1] = [f_2]$, если при приведении этих форм к виду (5) формы h (не представляющие нуля) для обеих форм содержат одно и то же число переменных и эквивалентны. Сложение классов Витта определяется формулой $[f_1] + [f_2] = [f_1 + f_2]$. Показать, что относительно этого действия сложения классы Витта образуют группу.

6. Определить группу классов Витта для квадратичных форм над полем вещественных чисел и над полем комплексных чисел.

7. Доказать, что всякая квадратичная форма над конечным полем представляет нуль, если только число ее переменных не менее трех (характеристика $\neq 2$).

8. Доказать, что всякая неособенная квадратичная форма над конечным полем Σ характеристики $\neq 2$ от $n \geqslant 2$ переменных представляет все элементы $\alpha \neq 0$ из Σ.

9. Доказать, что над конечным полем (характеристики $\neq 2$) всякая квадратичная форма от n переменных с определителем $d \neq 0$ эквивалентна форме $x_1^2 + \ldots + x_{n-1}^2 + dx_n^2$.

10. Доказать, что две неособенные квадратичные формы от n переменных над конечным полем Σ характеристики $\neq 2$ с определителями d_1 и d_2 эквивалентны тогда и только тогда, когда $d_2 = d_1\xi^2$ при некотором $\xi \neq 0$ из Σ. Таким образом, для любого $n \geqslant 1$ над полем Σ существует ровно два класса эквивалентных квадратичных форм от n переменных.

11. Пусть Σ — конечное поле характеристики $\neq 2$. Доказать, что группа классов Витта над полем Σ есть циклическая группа 4-го порядка, если -1 не является квадратом в Σ, и есть прямое произведение двух циклических групп 2-го порядка, если $-1 = \xi^2$ ($\xi \in \Sigma$).

12. Доказать, что группа классов Витта над полем K (характеристики $\neq 2$) есть периодическая абелева группа показателя 2, если только в этом поле -1 является квадратом.

§ 2. Алгебраические расширения

Ряд теорем этого параграфа приведен без доказательств. Их доказательства читатель может найти, например, в книгах [5], [16].

1. Конечные расширения. Если поле Ω содержит поле k в качестве подполя, то говорят, что Ω является *расширением* поля k. Желая подчеркнуть, что Ω рассматривается как расширение поля k, пишут Ω/k. Если поле K есть подполе поля Ω, содержащее k, т. е. $k \subset K \subset \Omega$, то K называется промежуточным полем расширения Ω/k.

Всякое расширение Ω/k можно рассматривать как линейное (векторное) пространство над полем k (относительно действий сложения в Ω и умножения на элементы из k).

Определение. *Расширение K/k называется конечным, если поле K, рассматриваемое как линейное пространство над k, имеет конечную размерность. Эта размерность называется сте-*

пенью расширения K/k и обозначается через $(K:k)$. Всякий базис поля K как линейного пространства над k называется базисом расширения K/k.

Если расширение K/k конечно, то для всякого промежуточного поля K_0 расширения K_0/k и K/K_0, очевидно, также конечны. Справедливо и обратное утверждение.

Теорема 1. *Пусть K_0 — промежуточное поле расширения K/k. Если расширения K/K_0 и K_0/k конечны, то K/k также конечно и его степень равна произведению степеней расширений K/K_0 и K_0/k:*

$$(K:k) = (K:K_0)(K_0:k).$$

Доказательство. Пусть $\theta_1, \ldots, \theta_m$ — базис K/K_0, а $\omega_1, \ldots, \omega_n$ — базис K_0/k. Так как каждый элемент из K может быть представлен в виде линейной комбинации произведений $\omega_i\theta_j$, то расширение K/k конечно. Далее, легко видеть, что эти произведения линейно независимы над k, поэтому $(K:k) = mn$.

Для любого поля k через $k[t]$ обозначается кольцо многочленов от переменной t с коэффициентами из k.

Пусть Ω/k — расширение поля k. Элемент $\alpha \in \Omega$ называется *алгебраическим над k*, если он является корнем некоторого отличного от нуля многочлена $f(t)$ из кольца $k[t]$. Выберем среди всех многочленов $f(t)$ (для которых α является корнем) многочлен $\varphi(t) \neq 0$ наименьшей степени и со старшим коэффициентом 1. Так как каждый $f(t)$ делится на $\varphi(t)$ (в противном случае не равный нулю остаток от деления f на φ имел бы α своим корнем и имел бы степень, меньшую степени φ), то указанными условиями многочлен $\varphi(t)$ определен однозначно. Он называется *минимальным многочленом* алгебраического элемента $\alpha \in \Omega$ относительно поля k. Минимальный многочлен $\varphi \in k[t]$ всегда неприводим, так как из разложения $\varphi = gh$ следует, что α является корнем либо $g(t)$, либо $h(t)$. Любой элемент $a \in k$ алгебраичен над k, и его минимальным многочленом является $t - a$. Элемент $\xi \in \Omega$, не являющийся алгебраическим относительно k, называется *трансцендентным* над k.

Расширение Ω/k называется *алгебраическим*, если всякий элемент $\alpha \in \Omega$ алгебраичен относительно k.

Теорема 2. *Всякое конечное расширение K/k алгебраично.*

Теорема 3. *Пусть элемент α из расширения Ω/k алгебраичен над k, и пусть его минимальный многочлен $\varphi(t) \in k[t]$ имеет степень m. Тогда степени $1, \alpha, \ldots, \alpha^{m-1}$ линейно независимы над k и все их линейные комбинации*

$$a_0 + a_1\alpha + \ldots + a_{m-1}\alpha^{m-1} \qquad (1)$$

с коэффициентами a_i из k образуют промежуточное поле, обозначаемое через $k(\alpha)$. Расширение $k(\alpha)/k$ конечно и имеет степень m.

Для сложения двух элементов поля $k(\alpha)$, записанных в виде (1), мы должны, очевидно, сложить соответствующие коэффициенты. Чтобы произведение элементов $\xi = g(\alpha)$ и $\eta = h(\alpha)$, где $g(t)$ и $h(t)$ — многочлены из $k[t]$ степени $\leqslant m-1$, также представить в виде (1), надо разделить gh на φ с остатком:

$$g(t)h(t) = \varphi(t)q(t) + r(t),$$

где степень $r(t)$ не превосходит $m-1$; так как $\varphi(\alpha) = 0$, то $\xi\eta = r(\alpha)$. Таким образом, действие умножения в расширении $k(\alpha)/k$ вполне определено заданием минимального многочлена $\varphi(t)$ элемента α.

Пусть $\alpha_1, \ldots, \alpha_s$ — конечная система элементов поля Ω, алгебраических над k, и пусть $m_1, \ldots, m_s$ — степени их минимальных многочленов относительно k. Совокупность всех линейных комбинаций элементов

$$\alpha_1^{r_1} \ldots \alpha_s^{r_s}, \qquad 0 \leqslant r_1 < m_1, \ \ldots, 0 \leqslant r_s < m_s,$$

с коэффициентами из k является промежуточным полем. Оно обозначается через $k(\alpha_1, \ldots, \alpha_s)$ и называется полем, порожденным элементами $\alpha_1, \ldots, \alpha_s$. Его степень над k не превосходит произведения $m_1 \ldots m_s$.

Всякое конечное расширение K/k, содержащееся в Ω, может быть представлено в виде $K = k(\alpha_1, \ldots, \alpha_s)$ при некоторых $\alpha_1, \ldots, \alpha_s$.

Определение. *Конечное расширение K/k называется простым, если в нем существует такой элемент θ, что $K = k(\theta)$. Всякий элемент $\theta \in K$, для которого $K = k(\theta)$, называется примитивным элементом поля K относительно k.*

Примитивные элементы поля K над k характеризуются, очевидно, тем, что степени их минимальных многочленов равны степени расширения K/k.

Теорема 4. *Пусть Ω/k и Ω'/k — два расширения поля k, и пусть алгебраические над k элементы $\theta \in \Omega$ и $\theta' \in \Omega'$ имеют один и тот же минимальный многочлен $\varphi(t)$. Тогда существует, и притом только один, изоморфизм поля $k(\theta)$ на поле $k(\theta')$, при котором $\theta \to \theta'$ и $a \to a$ при $a \in k$.*

Пусть m — степень многочлена $\varphi(t)$. Изоморфизм $k(\theta) \to k(\theta')$, о котором говорится в теореме 4, совпадает с отображением

$$a_0 + a_1\theta + \ldots + a_{m-1}\theta^{m-1} \to a_0 + a_1\theta' + \ldots + a_{m-1}\theta'^{m-1} \qquad (2)$$

($a_0, \ldots, a_{m-1}$ — произвольные элементы поля k).

До сих пор мы рассматривали конечные расширения K/k, которые содержались в заранее заданном расширении Ω/k. Перейдем теперь к вопросу о построении конечных расширений над фиксированным основным полем k.

Теорема 5. *Пусть k — поле. Для любого неприводимого многочлена $\varphi(t)$ из кольца $k[t]$ степени n существует конечное расширение K/k степени n, в котором этот многочлен φ имеет корень. С точностью до изоморфизма, оставляющего элементы из k на месте, расширение K/k единственно. Если $\varphi(\theta)=0$, $\theta\in K$, то $K=k(\theta)$.*

Поле K (в случае $n>1$) строится следующим образом. Выберем некоторый новый объект θ и рассмотрим совокупность K всех формальных линейных комбинаций

$$a_0+a_1\theta+\ldots+a_{n-1}\theta^{n-1} \tag{3}$$

с коэффициентами a_i из k. Если через $g(t)$ мы обозначим многочлен $a_0+a_1t+\ldots+a_{n-1}t^{n-1}$, то выражение (3) можно будет записать также в виде $g(\theta)$. Пусть $\xi=g(\theta)$ и $\eta=h(\theta)$ — две линейные комбинации вида (3) (g и h — многочлены из $k[t]$ степеней $\leqslant n-1$). Обозначим через $s(t)$ сумму $g(t)+h(t)$, а через $r(t)$ — остаток от деления произведения $g(t)h(t)$ на $\varphi(t)$. Положим $\xi+\eta=s(\theta)$, $\xi\eta=r(\theta)$. Легко проверяется теперь, что относительно этих действий множество K является требуемым полем.

Следствие. *Для любого многочлена $f(t)\in k[t]$ существует конечное расширение K/k, в котором $f(t)$ раскладывается на линейные множители.*

Поле k, над которым не существует конечных расширений, отличных от k, называется алгебраически замкнутым. Алгебраическая замкнутость поля k характеризуется, очевидно, тем, что в кольце $k[t]$ все многочлены раскладываются на линейные множители.

2. Норма и след. Пусть K/k — конечное расширение степени n. Для произвольного $\alpha\in K$ отображение $\xi\to\alpha\xi$ ($\xi\in K$) является линейным преобразованием K (как линейного пространства над k). Характеристический многочлен $f_\alpha(t)$ этого линейного преобразования называется также *характеристическим многочленом элемента $\alpha\in K$* относительно расширения K/k. Если $\omega_1,\ldots,\omega_n$ — базис расширения K/k и

$$\alpha\omega_i=\sum_{j=1}^{n}a_{ij}\omega_j,\qquad a_{ij}\in k, \tag{4}$$

то, как известно, $f_\alpha(t)=\det(tE-(a_{ij}))$, где E — единичная матрица n-го порядка.

Теорема 6. *Характеристический многочлен $f_\alpha(t)$ элемента $\alpha\in K$ относительно расширения K/k равен степени его минимального многочлена $\varphi_\alpha(t)$ относительно k.*

Доказательство. Пусть

$$\varphi_\alpha(t)=t^m+c_1t^{m-1}+\ldots+c_m.$$

По теореме 3 степени 1, $\alpha,\ldots,\alpha^{m-1}$ образуют базис расширения $k(\alpha)/k$. Если $\theta_1,\ldots,\theta_s$ — базис $K/k(\alpha)$, то в качестве базиса K/k

можно взять произведения

$$\theta_1,\ \alpha\theta_1,\ \ldots,\ \alpha^{m-1}\theta_1;\ \ldots;\ \theta_s,\ \alpha\theta_s,\ \ldots,\ \alpha^{m-1}\theta_s.$$

Матрицей линейного преобразования $\xi \to \alpha\xi$ в этом базисе будет, очевидно, клеточно диагональная матрица, все s диагональных клеток которой совпадают с матрицей

$$\begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ -c_m & -c_{m-1} & -c_{m-2} & \ldots & -c_2 & -c_1 \end{pmatrix}.$$

Ее характеристический многочлен, как легко подсчитать, равен $t^m + c_1 t^{m-1} + \ldots + c_m$, т. е. равён $\varphi_\alpha(t)$. Следовательно, $f_\alpha = \varphi_\alpha^s$, и теорема 6 доказана.

Так как при переходе от одного базиса пространства к другому матрица линейного преобразования заменяется подобной матрицей, то определитель и след матрицы (a_{ij}), определяемой равенствами (4), не зависят от выбора базиса $\omega_1, \ldots, \omega_n$.

Определение. *Определитель* $\det(a_{ij})$ *матрицы* (a_{ij}) *из разложений* (4) *называется нормой, а ее след* $\mathrm{Sp}(a_{ij}) = \sum_{i=1}^{n} a_{ii}$ — *следом элемента* $\alpha \in K$ *относительно расширения* K/k. Норма и след обозначаются соответственно через $N_{K/k}(\alpha)$ и $\mathrm{Sp}_{K/k}(\alpha)$ или, короче, через $N(\alpha)$ и $\mathrm{Sp}(\alpha)$.

При $a \in k$ матрицей линейного преобразования $\xi \to a\xi$ ($\xi \in K$) будет диагональная матрица aE. Поэтому для элемента a из основного поля k имеем $N_{K/k}(a) = a^n$, $\mathrm{Sp}_{K/k}(a) = na$. Так как при умножении и сложении линейных преобразований их матрицы (при фиксированном базисе) умножаются и складываются, то для любых элементов α и β из K имеем формулы

$$N_{K/k}(\alpha\beta) = N_{K/k}(\alpha) N_{K/k}(\beta), \tag{5}$$

$$\mathrm{Sp}_{K/k}(\alpha + \beta) = \mathrm{Sp}_{K/k}(\alpha) + \mathrm{Sp}_{K/k}(\beta). \tag{6}$$

Матрица линейного преобразования $\xi \to a\alpha\xi$ ($a \in k$, $\alpha \in K$) получается из матрицы преобразования $\xi \to \alpha\xi$ умножением всех элементов на a. Поэтому имеет место также формула

$$\mathrm{Sp}_{K/k}(a\alpha) = a\,\mathrm{Sp}_{K/k}(\alpha), \qquad a \in k,\ \alpha \in K. \tag{7}$$

Если $\alpha \neq 0$, то ввиду неособенности преобразования $\xi \to \alpha\xi$ норма $N_{K/k}(\alpha)$ также отлична от нуля. Формула (5) означает, следовательно, что отображение $\alpha \to N_{K/k}(\alpha)$ является гомоморфизмом мультипликативной группы K^* поля K в мультипликативную группу k^* поля k. Что касается отображения $\alpha \to \mathrm{Sp}_{K/k}(\alpha)$, то ввиду (6) и (7) оно является линейной функцией на K со значениями в основном поле k.

Теорема 7. *Пусть Ω/k — расширение, в котором характеристический многочлен $f_\alpha(t)$ элемента $\alpha \in K$ относительно конечного расширения K/k целиком раскладывается на линейные множители:*

$$f_\alpha(t) = (t-\alpha_1)\dots(t-\alpha_n).$$

Тогда

$$N_{K/k}(\alpha) = \alpha_1\alpha_2\dots\alpha_n, \qquad \mathrm{Sp}_{K/k}(\alpha) = \alpha_1+\alpha_2+\dots+\alpha_n.$$

Доказательство. Если

$$f_\alpha(t) = \det(tE-(a_{ij})) = t^n + a_1t^{n-1}+\dots+a_n,$$

то $a_1 = -\mathrm{Sp}(a_{ij})$, $a_n = (-1)^n\det(a_{ij})$. С другой стороны, по формулам Виета

$$\alpha_1+\alpha_2+\dots+\alpha_n = -a_1,\ \alpha_1\alpha_2\dots\alpha_n = (-1)^n a_n,$$

это и доказывает теорему.

Теорема 8. *В обозначениях теоремы 7 для характеристического многочлена $f_\gamma(t)$ элемента $\gamma = g(\alpha) \in K$ ($g(t) \in k[t]$) в поле Ω имеет место разложение*

$$(t-g(\alpha_1))(t-g(\alpha_2))\dots(t-g(\alpha_n)). \tag{8}$$

Доказательство. Прежде всего заметим, что коэффициенты многочлена (8), являясь симметрическими выражениями от $\alpha_1, \dots, \alpha_n$, принадлежат полю k. Пусть $\varphi_\gamma(t)$ — минимальный многочлен элемента γ над k. Подвергая равенство $\varphi_\gamma(g(\alpha)) = 0$ действию изоморфизма $k(\alpha) \to k(\alpha_i)$ (при котором $\alpha \to \alpha_i$ и $a \to a$ при $a \in k$), мы получим $\varphi_\gamma(g(\alpha_i)) = 0$. Все корни многочлена (8) являются, таким образом, корнями неприводимого над k многочлена $\varphi_\gamma(t)$, а это возможно лишь при условии, что он является степенью $\varphi_\gamma(t)$. Для окончания доказательства остается применить теорему 6.

Пусть $k \subset K \subset L$ — цепочка конечных расширений. Выберем для K/k и L/K базисы $\omega_1, \dots, \omega_n$ и $\theta_1, \dots, \theta_m$ соответственно. Для произвольного $\gamma \in L$ положим

$$\gamma\theta_j = \sum_{s=1}^{m} \alpha_{js}\theta_s, \quad \alpha_{js} \in K, \qquad \alpha_{js}\omega_i = \sum_{r=1}^{n} a_{jsir}\omega_r, \quad a_{jsir} \in k.$$

Так как $\gamma\omega_i\theta_j = \sum_{s,r} a_{jsir}\omega_r\theta_s$, то $\mathrm{Sp}_{L/K}(\gamma) = \sum_{i,j} a_{jjii}$. С другой стороны, мы имеем также

$$\mathrm{Sp}_{K/k}(\mathrm{Sp}_{L/K}(\gamma)) = \mathrm{Sp}_{K/k}\Big(\sum_j \alpha_{jj}\Big) = \sum_{i,j} a_{jjii}.$$

Следовательно, для любого $\gamma \in K$

$$\mathrm{Sp}_{L/k}(\gamma) = \mathrm{Sp}_{K/k}(\mathrm{Sp}_{L/K}(\gamma)). \tag{9}$$

Аналогичная формула имеет место и для нормы (задача 2).

3. Сепарабельные расширения.

Определение. *Конечное расширение K/k называется сепарабельным, если линейная функция $\xi \to \mathrm{Sp}_{K/k}(\xi)$, $\xi \in K$, не равна тождественно нулю.*

Если характеристика поля k равна нулю, то $\mathrm{Sp}_{K/k}(1) = n = (K:k)$. Следовательно, все конечные расширения поля характеристики нуль сепарабельны. Это же, очевидно, справедливо и для тех конечных расширений поля характеристики p, степень которых не делится на p.

Выберем в конечном сепарабельном расширении K/k базис $\omega_1, \ldots, \omega_n$ и рассмотрим матрицу

$$(\mathrm{Sp}(\omega_i\omega_j))_{1\leqslant i,\, j\leqslant n}. \tag{10}$$

Если бы определитель этой матрицы был равен нулю, то в поле k нашлись бы элементы $c_1, \ldots, c_n$, не равные нулю одновременно, для которых

$$\sum_{j=1}^{n} c_j \mathrm{Sp}(\omega_i\omega_j) = 0, \qquad i = 1, \ldots, n.$$

Полагая $\gamma = c_1\omega_1 + \ldots + c_n\omega_n$, мы можем последние равенства переписать в виде

$$\mathrm{Sp}(\omega_i\gamma) = 0, \qquad i = 1, \ldots, n. \tag{11}$$

Пусть ξ — произвольный элемент из K. Так как $\gamma \neq 0$, то ξ можно представить в виде $\xi = a_1\omega_1\gamma + \ldots + a_n\omega_n\gamma$, $a_i \in k$, откуда ввиду (6), (7) и (11) получаем, что $\mathrm{Sp}\,\xi = 0$. Это, однако, противоречит сепарабельности K/k. Таким образом, для сепарабельных расширений матрица (10) всегда неособенная.

Определение. *Определитель* $\det(\mathrm{Sp}(\omega_i\omega_j))$ *называется дискриминантом базиса* $\omega_1, \ldots, \omega_n$ *конечного сепарабельного расширения K/k и обозначается через* $D(\omega_1, \ldots, \omega_n)$.

По доказанному дискриминант любого базиса конечного сепарабельного расширения является отличным от нуля элементом основного поля.

Пусть $\omega_1', \ldots, \omega_n'$ — другой базис расширения K/k, и пусть

$$\omega_i' = \sum_{j=1}^{n} c_{ij}\omega_j, \qquad i = 1, \ldots, n.$$

Матрица $(\mathrm{Sp}(\omega_i'\omega_j'))$ равна произведению $(c_{ij})(\mathrm{Sp}(\omega_i\omega_j))(c_{ij})'$ (штрих обозначает транспонированную матрицу), поэтому

$$D(\omega_1', \ldots, \omega_n') = (\det(c_{ij}))^2 D(\omega_1, \ldots, \omega_n). \tag{12}$$

Таким образом, дискриминанты двух различных базисов отличаются друг от друга на множитель, являющийся квадратом элемента из основного поля.

Зафиксируем для расширения K/k какой-нибудь базис $\omega_1, \ldots, \omega_n$. Тогда для произвольных элементов $c_1, \ldots, c_n$ поля k су-

ществует (и притом только один) элемент $\alpha \in K$, для которого

$$\mathrm{Sp}(\omega_i\alpha) = c_i, \qquad i = 1, \ldots, n. \tag{13}$$

Действительно, представив α в виде $\alpha = x_1\omega_1 + \ldots + x_n\omega_n$ $(x_j \in k)$ и подставив это выражение для α в равенства (13), мы получим для определения x_j систему n линейных уравнений с n неизвестными и с отличным от нуля определителем. В частности, в поле K можно найти n таких элементов $\omega_1^*, \ldots, \omega_n^*$, что

$$\mathrm{Sp}(\omega_i\omega_j^*) = \begin{cases} 1 & \text{при } i = j, \\ 0 & \text{при } i \neq j. \end{cases} \tag{14}$$

Эти n элементов ω_j^* линейно независимы над k, так как если $c_1\omega_1^* + \ldots + c_n\omega_n^* = 0$ $(c_i \in k)$, то, умножая это равенство на ω_i и переходя к следу, мы находим, что $c_i = 0$ при всех $i = 1, \ldots, n$.

Определение. *Базис* $\omega_1^*, \ldots, \omega_n^*$ *сепарабельного расширения* K/k, *однозначно определяемый равенствами* (14), *называется взаимным базисом для базиса* $\omega_1, \ldots, \omega_n$.

Взаимный базис дает возможность записать в явном виде значения для коэффициентов $a_i \in k$ в разложении

$$\alpha = a_1\omega_1 + \ldots + a_n\omega_n$$

произвольного элемента α из K. В самом деле, взяв след от произведения $\alpha\omega_i^*$, мы получим формулы

$$a_i = \mathrm{Sp}(\alpha\omega_i^*), \qquad i = 1, \ldots, n.$$

Предположим, что минимальный многочлен $\varphi(t)$ некоторого элемента α из сепарабельного расширения K/k раскладывается целиком на линейные множители в расширении Ω/k:

$$\varphi(t) = (t - \alpha_1)\ldots(t - \alpha_m).$$

Из формулы (9) очевидным образом следует, что вместе с K/k расширение $k(\alpha)/k$ также сепарабельно. Так как минимальный многочлен φ является также и характеристическим многочленом для α относительно $k(\alpha)/k$, то ввиду теорем 7 и 8

$$\mathrm{Sp}_{k(\alpha)/k}\alpha^r = \sum_{s=1}^{m} \alpha_s^r,$$

а поэтому для дискриминанта $D(1, \alpha, \ldots, \alpha^{m-1}) = D$ базиса $1, \alpha, \ldots, \alpha^{m-1}$ расширения $k(\alpha)/k$ имеет место выражение

$$D = \det\left(\sum_{s=1}^{m} \alpha_s^{i+j}\right)_{0 \leqslant i,j \leqslant m-1} = \det(\alpha_s^i)\cdot\det(\alpha_s^j) = \prod_{1 \leqslant i < j \leqslant m} (\alpha_i - \alpha_j)^2.$$

Но $D \neq 0$, поэтому $\alpha_i \neq \alpha_j$, и мы доказали следующий факт.

Теорема 9. *Минимальный многочлен любого элемента из сепарабельного расширения не имеет кратных корней (в том поле, где он раскладывается на линейные множители).*

Элемент α из алгебраического расширения поля k называется *сепарабельным* над k, если его минимальный многочлен $\varphi_\alpha(t) \in k[t]$ не имеет кратных корней, и называется *несепарабельным* в противном случае. Согласно теореме 9 все элементы из конечного сепарабельного расширения K/k сепарабельны над k. Обратно, если элемент α сепарабелен над k, то расширение $k(\alpha)/k$ сепарабельно.

Теорема 10 (о примитивном элементе). *Всякое конечное сепарабельное расширение K/k является простым, т. е. в нем существует такой элемент θ, что $K = k(\theta)$.*

Теорема 11. *Для конечного сепарабельного расширения K/k степени n существует ровно n (и не более) изоморфизмов в надлежащее расширение Ω/k, при которых каждый элемент из k отображается на себя. Если $\sigma_1, \ldots, \sigma_n$ — все эти изоморфизмы, то для любого элемента $\alpha \in K$ его характеристический многочлен $f_\alpha(t)$ в поле Ω имеет разложение*

$$f_\alpha(t) = (t - \sigma_1(\alpha))(t - \sigma_2(\alpha)) \ldots (t - \sigma_n(\alpha)).$$

Элементы $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ (принадлежащие полю Ω) называются сопряженными с элементом $\alpha \in K$. Образы $\sigma_1(K), \ldots, \sigma_n(K)$ поля K при изоморфизмах σ_i называются полями, сопряженными с полем K. Если θ — примитивный элемент поля K над k, то очевидно, $\sigma_i(K) = k(\sigma_i(\theta))$.

Следствие 1. *В тех же обозначениях имеем*

$$N_{K/k}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) \ldots \sigma_n(\alpha),$$

$$\mathrm{Sp}_{K/k}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \ldots + \sigma_n(\alpha).$$

Следствие 2. *Для произвольного конечного расширения поля рациональных чисел степени n существует ровно n изоморфизмов в поле комплексных чисел.*

Пусть $\omega_1, \ldots, \omega_n$ — базис K/k. Так как $\mathrm{Sp}(\omega_i\omega_j) = \sum_{s=1}^{n} \sigma_s(\omega_i)\sigma_s(\omega_j)$, то матрица $(\mathrm{Sp}(\omega_i\omega_j))$ представляется в виде произведения $(\sigma_i(\omega_j))'(\sigma_i(\omega_j))$ (штрих обозначает транспонирование), а поэтому для дискриминанта базиса ω_i имеем также следующую формулу:

$$D(\omega_1, \ldots, \omega_n) = (\det(\sigma_i(\omega_j)))^2. \qquad (15)$$

4. Нормальные расширения. Алгебраическое расширение Ω/k называется *нормальным*, если для любого элемента $\alpha \in \Omega$ его минимальный многочлен $\varphi_\alpha(t) \in k[t]$ в кольце $\Omega[t]$ целиком раскладывается на линейные множители.

Теорема 12. *Всякое конечное расширение K/k можно погрузить в конечное нормальное расширение L/k ($k \subset K \subset L$).*

Если $K = k(\alpha_1, \ldots, \alpha_s)$ и $\varphi_1(t), \ldots, \varphi_s(t)$ — минимальные многочлены элементов $\alpha_1, \ldots, \alpha_s$ относительно k, то в качестве L можно взять расширение над K, в котором многочлен $f(t) = \varphi_1(t) \ldots \varphi_s(t)$ раскладывается на линейные множители (следствие теоремы 5) и которое порождается всеми корнями $f(t)$.

Пусть характеристика поля k равна p. Элемент α из алгебраического расширения поля k называется *чисто несепарабельным*, если α^{p^m} содержится в k при некотором целом $m \geqslant 0$. Алгебраическое расширение Ω/k называется *чисто несепарабельным*, если все элементы из Ω чисто несепарабельны над k. Чисто несепарабельное расширение нормально.

Автоморфизм σ поля K (изоморфное отображение K на себя) называется *автоморфизмом расширения* K/k, если $\sigma(a) = a$ при всех $a \in k$. Совокупность всех автоморфизмов расширения K/k образует группу (произведение автоморфизмов σ и τ определяется как произведение отображений: $(\sigma\tau)(x) = \sigma(\tau(x))$, $x \in K$). Если расширение K/k конечно, то его группа автоморфизмов G также конечна и ее порядок не превосходит степени расширения $(K : k)$.

Определение. *Конечное расширение K/k называется расширением Галуа, если порядок его группы автоморфизмов G равен степени $(K : k)$.* Сама группа G называется в этом случае *группой Галуа* расширения Галуа K/k.

Теорема 13. *Для того чтобы конечное расширение K/k было расширением Галуа, необходимо и достаточно, чтобы оно было нормальным и сепарабельным.*

Если G — произвольная конечная группа автоморфизмов поля K, то через K^G обозначают подполе неподвижных элементов, т. е. тех элементов $a \in K$, для которых $\sigma(a) = a$ при всех $\sigma \in G$. Если G — группа автоморфизмов конечного расширения K/k, то это расширение будет расширением Галуа тогда и только тогда, когда $K^G = k$.

Если характеристика поля k равна 0, то понятие конечного расширения Галуа над k совпадает с понятием конечного нормального расширения.

Теорема 14. *Пусть k — поле характеристики p, K/k — конечное нормальное расширение, G — его группа автоморфизмов и $K_0 = K^G$ — подполе неподвижных элементов. Тогда K/K_0 — расширение Галуа с группой Галуа G, а K_0/k — чисто несепарабельное расширение.*

Задачи

1. Пусть $\Omega = k(x)$ есть поле рациональных функций от x с коэффициентами из поля k. Доказать, что всякий элемент из Ω, не принадлежащий k, трансцендентен над k.

2. Пусть $k \subset K \subset L$ — цепочка конечных расширений. Доказать, что для любого $\theta \in L$ справедлива формула

$$N_{K/k}(N_{L/K}(\theta)) = N_{L/k}(\theta).$$

(Предположить сначала, что $L = K(\theta)$, и рассмотреть для расширения L/k базис $\omega_i\theta^j$, где ω_i — базис K/k.)

3. Найти в расширении $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ поля рациональных чисел $\mathbb{Q}$ примитивный элемент и выразить через него числа $\sqrt{2}$ и $\sqrt{3}$.

4. Доказать, что конечное расширение K/k является простым тогда и только тогда, когда для этого расширения существует только конечное число промежуточных полей.

5. Пусть k — произвольное поле характеристики $p \neq 0$. Доказать, что многочлен $f(t) = t^p - t - a$ $(a \in k)$ либо целиком раскладывается в поле k на линейные множители, либо неприводим. Показать, далее, что во втором случае расширение $k(\theta)/k$, где $f(\theta) = 0$, сепарабельно.

6. Пусть k_0 — поле характеристики $p \neq 0$ и $k = k_0(x)$ — поле рациональных функций от x с коэффициентами из k_0. Показать, что многочлен $f(t) = t^p - x$ неприводим в кольце $k[t]$. Доказать, далее, что расширение $k(\theta)/k$, где $f(\theta) = 0$, несепарабельно.

7. Доказать, что если для конечного расширения K/k степени n существует n различных изоморфизмов в некоторое расширение Ω/k, оставляющих элементы из k на месте, то это расширение K/k сепарабельно.

8. Пусть k — произвольное поле характеристики $\neq p$, содержащее первообразный корень степени p из 1. Доказать, что если элемент $\alpha \in k$ не является p-й степенью элемента из k, то $\left(k\left(\sqrt[p]{\alpha}\right) : k\right) = p$.

9. Пусть K/k — конечное сепарабельное расширение и φ — линейная функция на линейном пространстве K над полем k со значениями в k. Доказать, что в поле K существует, и притом единственный, элемент α такой, что

$$\varphi(\xi) = \mathrm{Sp}_{K/k}(\alpha\xi), \qquad \xi \in K.$$

§ 3. Конечные поля

Поле Σ называется *конечным*, если оно состоит из конечного числа элементов. Примером конечного поля является поле вычетов $\mathbb{F}_p$ в кольце целых рациональных чисел $\mathbb{Z}$ по простому модулю p. Все конечные поля имеют простую характеристику, и если характеристика некоторого конечного поля Σ равна p, то это поле содержит простое подполе (не имеющее собственных подполей), которое изоморфно полю $\mathbb{F}_p$. Можно поэтому считать, что $\mathbb{F}_p \subset \Sigma$. Расширение $\Sigma/\mathbb{F}_p$, очевидно, конечно. Если его степень равна m и если $\omega_1, \ldots, \omega_m$ — базис Σ над $\mathbb{F}_p$, то каждый элемент $\xi \in \Sigma$ однозначно представляется в виде $\xi = c_1\omega_1 + \ldots + c_m\omega_m$, где c_i независимо друг от друга пробегают все p элементов из $\mathbb{F}_p$. Так как число всех таких линейных комбинаций равно p^m, то этим мы доказали, что *число элементов любого конечного поля равно степени его характеристики.*

Мультипликативная группа Σ^* конечного поля Σ является, разумеется, конечной абелевой группой. Выясним ее строение.

Лемма. *Конечная подгруппа G мультипликативной группы K^* произвольного поля K всегда циклична.*

Доказательство. Покажем сначала, что если в абелевой группе G существуют элементы порядков m и n, то в G существует также элемент, порядок которого равен общему наименьшему кратному k чисел m и n. Пусть элементы x и y из G имеют

порядки m и n соответственно. Если $(m, n) = 1$, то произведение xy имеет, как легко видеть, порядок $k = mn$. В общем случае, используя канонические разложения чисел m и n в произведения степеней простых чисел, мы можем найти для них представления в виде произведений

$$m = m_0 m_1, \qquad n = n_0 n_1$$

таких, что $(m_0, n_0) = 1$ и $k = m_0 n_0$. Элементы x^{m_1} и y^{n_1} имеют порядки m_0 и n_0 соответственно, а их произведение $x^{m_1} y^{n_1}$ имеет порядок $k = m_0 n_0$.

Пусть теперь G — конечная подгруппа порядка g мультипликативной группы поля K. Если m есть наибольший из порядков элементов группы G, то, очевидно, $m \leqslant g$. С другой стороны, из только что доказанного легко следует, что порядок любого элемента из G является делителем m, т. е. все элементы группы G являются корнями многочлена $t^m - 1$. Но в любом поле многочлен степени m не может иметь более m корней, поэтому $g \leqslant m$. Таким образом, $g = m$, а это и означает, что группа G циклична.

Применяя доказанную лемму к интересующему нас случаю конечного поля, получаем следующий факт.

Теорема 1. *Мультипликативная группа конечного поля, состоящего из p^m элементов, есть циклическая группа порядка $p^m - 1$.*

Следствие. *Всякое конечное расширение конечного поля является простым.*

Действительно, если θ — образующий элемент группы Σ^*, то, очевидно, $\mathbb{F}_p(\theta) = \Sigma$. Для промежуточного поля Σ_0 тем более $\Sigma_0(\theta) = \Sigma$.

Из теоремы 1 вытекает также, что все элементы из Σ являются корнями многочлена $t^{p^m} - t$, а так как степень этого многочлена равна числу элементов в Σ, то в кольце $\Sigma[t]$ имеем разложение

$$t^{p^m} - t = \prod_{\xi \in \Sigma} (t - \xi)$$

(ξ пробегает все элементы поля Σ).

Теорема 2. *Для простого числа p и любого натурального m существует, и с точностью до изоморфизма только одно, конечное поле, состоящее из p^m элементов.*

Доказательство. По следствию теоремы 5 § 2 над полем $\mathbb{F}_p$ существует расширение $\Omega/\mathbb{F}_p$, в котором многочлен $t^{p^m} - t$ раскладывается на линейные множители. Обозначим через Σ совокупность всех его корней (содержащихся в Ω). Так как в любом поле характеристики p справедлива формула

$$(x \pm y)^{p^m} = x^{p^m} \pm y^{p^m},$$

то сумма и разность любых двух элементов из Σ также принад-

лежат Σ. Совокупность Σ замкнута, очевидно, и относительно действий умножения и деления (если делитель не нуль). Следовательно, Σ является подполем поля Ω. Многочлен $t^{p^m} - t$ не имеет кратных корней (так как его производная $p^m t^{p^m-1} - 1 = -1$ не обращается в нуль ни при каких значениях переменной t), поэтому Σ состоит *из* p^m *элементов. Существование конечного поля* из p^m элементов доказано.

Пусть теперь Σ и Σ' — два расширения степени m над $\mathbb{F}_p$. Выберем в Σ примитивный элемент θ (следствие теоремы 1) и обозначим через $\varphi(t)$ его минимальный многочлен. Так как $\varphi(t)$ является делителем многочлена $t^{p^m} - t$, а последний многочлен раскладывается на линейные множители и в Σ', то $\varphi(t)$ имеет корень $\theta' \in \Sigma'$. Расширение $\mathbb{F}_p(\theta')/\mathbb{F}_p$ имеет степень, равную степени многочлена $\varphi(t)$, т. е. m, а потому $\mathbb{F}_p(\theta') = \Sigma'$. Существование изоморфизма поля Σ на Σ' следует теперь из теоремы 4 § 2.

Конечное поле из p^m элементов обозначают обычно через $GF(p^m)$ (и называют также полем Галуа — Galois field).

Следствие. *Над конечным полем* $\Sigma_0 = GF(p^r)$ *существуют неприводимые многочлены произвольной степени* n.

Действительно, $p^r - 1$ является делителем $p^{rn} - 1$, поэтому все корни многочлена $t^{p^{rn}} - t$ в поле $\Sigma = GF(p^{rn})$ образуют подполе, изоморфное полю Σ_0. Мы можем, следовательно, считать, что $\Sigma_0 \subset \Sigma$. Минимальный многочлен какого-нибудь примитивного элемента $\theta \in \Sigma$ относительно Σ_0 будет неприводимым многочленом из кольца $\Sigma_0[t]$ степени n, так как

$$(\Sigma : \Sigma_0) = (\Sigma : \mathbb{F}_p)/(\Sigma_0 : \mathbb{F}_p) = rn/r = n.$$

Заметим в заключение, что для выяснения того, является ли данное конечное коммутативное кольцо полем, достаточно лишь проверить, что оно не имеет делителей нуля. В самом деле, пусть $\mathfrak{O}$ есть конечное кольцо без делителей нуля и пусть a — отличный от нуля элемент из $\mathfrak{O}$. Если $ax_1 = ax_2$, то $a(x_1 - x_2) = 0$, откуда $x_1 = x_2$. Таким образом, при различных x_1 и x_2 произведения ax_1 и ax_2 также различны, и, значит, вместе с x произведение ax пробегает все элементы кольца $\mathfrak{O}$. Но в таком случае при любом $b \neq 0$ уравнение $ax = b$ разрешимо в $\mathfrak{O}$, т. е. все отличные от нуля элементы кольца $\mathfrak{O}$ образуют группу по умножению.

Задачи

1. Показать, что число $r(m)$ различных неприводимых многочленов степени m в кольце $\mathbb{F}_p[t]$, старшие коэффициенты которых равны 1, выражается формулой

$$r(m) = \frac{1}{m} \sum_{d|m} \mu\left(\frac{m}{d}\right) p^d$$

(d пробегает все делители m, а $\mu(k)$ обозначает функцию Мёбиуса).

2. Найти все неприводимые многочлены второй степени над полем $\mathbb{F}_5 = GF(5)$.

3. Показать, что поле $GF(p^m)$ содержится в поле $GF(p^n)$ (в смысле изоморфного вложения) тогда и только тогда, когда $m \mid n$.

4. Какую степень над $\mathbb{F}_p$ имеет поле разложения многочлена $t^n - 1$?

5. Пусть $\Sigma = GF(p^m)$. Показать, что отображения σ_i: $\xi \to \xi^{p^i}$, $\xi \in \Sigma$ ($i = 0, 1, \ldots, m-1$) являются попарно различными автоморфизмами поля Σ и что каждый автоморфизм Σ совпадает с одним из σ_i.

6. Пусть $p^r = q$, $\Sigma_0 = GF(q)$ и Σ — конечное расширение поля Σ_0 степени n. Доказать, что отображения $\xi \to \xi^{q^i}$, $\xi \in \Sigma$, $i = 0, 1, \ldots, n-1$, составляют полную систему n попарно различных автоморфизмов поля Σ, не меняющих элементов из Σ_0. Показать, далее, что характеристический многочлен $f_\xi(t)$ элемента $\xi \in \Sigma$ относительно Σ/Σ_0 в поле Σ имеет разложение

$$f_\xi(t) = (t-\xi)(t-\xi^q)\ldots\left(t-\xi^{q^{n-1}}\right)$$

(использовать теорему 8 § 2). Вывести отсюда, что

$$\mathrm{Sp}_{\Sigma/\Sigma_0}(\xi) = \xi + \xi^q + \ldots + \xi^{q^{n-1}}, \quad N_{\Sigma/\Sigma_0}(\xi) = \xi^{1+q+\ldots+q^{n-1}}.$$

7. Доказать, что конечное расширение конечного поля всегда сепарабельно.

8. В обозначениях задачи 6 показать, что всякий элемент поля Σ_0 является нормой некоторого элемента из Σ.

9. Пусть $\Sigma = GF(p^{mr})$, $p^m = q$, $\alpha \in \Sigma$. Доказать, что в поле Σ уравнение $\xi^q - \xi = \alpha$ разрешимо тогда и только тогда, когда $\alpha + \alpha^q + \ldots + \alpha^{q^{r-1}} = 0$.

10. Пусть ε — первообразный корень простой степени p из 1. Так как элементы простого подполя $\Sigma_0 = GF(p)$ поля $\Sigma = GF(p^m)$ являются классами вычетов в кольце целых рациональных чисел по модулю p, то имеет смысл степень $\varepsilon^{\mathrm{Sp}\gamma}$ при любом $\gamma \in \Sigma$ (след берется относительно расширения Σ/Σ_0). Доказать, что

$$\sum_{\xi\in\Sigma} \varepsilon^{\mathrm{Sp}\xi\alpha} = \begin{cases} 0 & \text{при } \alpha \neq 0, \\ p^m & \text{при } \alpha = 0. \end{cases}$$

11. Пусть χ — характер мультипликативной группы поля $\Sigma = GF(p^m)$, $p^m = q$ (относительно определения характеров см. § 5). Продолжим χ на все поле Σ, положив $\chi(0) = 0$. Выражение

$$\tau_\alpha(\chi) = \sum_{\xi\in\Sigma} \chi(\xi)\,\varepsilon^{\mathrm{Sp}\alpha\xi}, \qquad \alpha \in \Sigma,$$

являющееся комплексным числом, называется *гауссовой суммой в конечном поле* Σ. Предполагая, что характер χ отличен от единичного характера χ_0, доказать формулы

$$\tau_\alpha(\chi) = \chi(\alpha)^{-1}\tau_1(\chi), \qquad \alpha \neq 0, \qquad |\tau_\alpha(\chi)| = \sqrt{q}, \qquad \alpha \neq 0,$$

$$\sum_{\alpha\neq 0} \tau_\alpha(\chi) = 0.$$

12. Пусть $p \neq 2$. Так как все квадраты в мультипликативной группе Σ^* поля $\Sigma = GF(p^m)$ образуют подгруппу индекса 2, то, полагая $\psi(\alpha) = +1$, если $\alpha \neq 0$ является квадратом, и $\psi(\alpha) = -1$ в противном случае, мы

получаем характер ψ группы Σ^*. Доказать, что при $\alpha\beta \neq 0$

$$\tau_\alpha(\psi)\tau_\beta(\psi) = \psi(-\alpha\beta)p^m.$$

13. Доказать, что при $\alpha \neq 0$ $\sum_{\xi\in\Sigma} \psi(\xi^2 - \alpha) = -1$.

14. Пусть $f(x_1, \ldots, x_n)$ — неособенная квадратичная форма определителя δ с коэффициентами из $\Sigma = GF(p^m)$, $p^m = q$, $p \neq 2$, и пусть α — произвольный элемент из Σ. Доказать, что в поле Σ число решений N уравнения $f(x_1, \ldots, x_n) = \alpha$ выражается формулами

$$N = q^{2r} + q^r\psi((-1)^r\alpha\delta), \qquad \text{если} \quad n = 2r+1,$$
$$N = q^{2r-1} + \omega q^{r-1}\psi((-1)^r\delta), \qquad \text{если} \quad n = 2r.$$

где $\omega = -1$ при $\alpha \neq 0$ и $\omega = q-1$ при $\alpha = 0$.

15. Пусть p и q — различные нечетные простые рациональные числа. Для целого x соответствующие классы вычетов из полей $GF(p)$ и $GF(q)$ будем обозначать той же буквой x. Для поля $GF(q)$ выберем расширение Δ, в котором многочлен $t^p - 1$ раскладывается на линейные множители, и через ε обозначим какой-нибудь первообразный корень степени p из 1, содержащийся в Δ. Символ Лежандра $\left(\frac{x}{p}\right)$ совпадает, очевидно, с характером $\psi(x)$ для поля $GF(p)$, указанным в задаче 12. Так как его значениями являются ± 1, то можно считать, что $\left(\frac{x}{p}\right) \in \Delta$. Доказать, что для «гауссовой суммы»

$$\tau = \sum_{x\in GF(p)} \left(\frac{x}{p}\right)\varepsilon^x \in \Delta$$

имеют место равенства

$$\tau^2 = (-1)^{\frac{p-1}{2}}p, \tag{1}$$

$$\tau^q = \left(\frac{q}{p}\right)\tau. \tag{2}$$

16. Используя представление $\left(\frac{p}{q}\right) = p^{(q-1)/2}$ символа Лежандра в поле $GF(q)$, вывести из формул (1) и (2) закон взаимности Гаусса

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

§ 4. Некоторые сведения о коммутативных кольцах

В этом параграфе под кольцом везде понимается коммутативное кольцо с единичным элементом 1 и без делителей нуля.

1. Делимость в кольцах. Пусть $\mathfrak{O}$ — кольцо. Если для элементов α и $\beta \neq 0$ из $\mathfrak{O}$ существует такой элемент $\xi \in \mathfrak{O}$, что $\beta\xi = \alpha$, то говорят, что α делится на β (β делит α), и пишут $\beta|\alpha$. Так как $\mathfrak{O}$ не имеет делителей нуля, то равенством $\beta\xi = \alpha$ элемент ξ определен однозначно. Понятие делимости в произвольных

кольцах обладает, очевидно, всеми свойствами делимости для целых рациональных чисел. Например, если $\gamma|\beta$ и $\beta|\alpha$, то $\gamma|\alpha$.

Элемент $\varepsilon \in \mathfrak{O}$, являющийся делителем единичного элемента 1, называется единицей кольца $\mathfrak{O}$ (или обратимым элементом).

Теорема 1. *Все единицы кольца $\mathfrak{O}$ образуют группу по умножению.*

Доказательство. Пусть E есть совокупность всех единиц кольца $\mathfrak{O}$. Если $\varepsilon \in E$ и $\eta \in E$, то $\varepsilon\varepsilon' = 1$ и $\eta\eta' = 1$ при некоторых ε' и η' из $\mathfrak{O}$. Но тогда $\varepsilon\eta(\varepsilon'\eta') = 1$, а значит, $\varepsilon\eta \in E$. Так как $1 \in E$ и для каждой единицы ε элемент ε', определяемый равенством $\varepsilon\varepsilon' = 1$, также является единицей, то E — группа, а это и утверждается теоремой.

Элементы $\alpha \neq 0$ и $\beta \neq 0$ кольца $\mathfrak{O}$ называются ассоциированными, если они делятся друг на друга. Из равенств $\alpha = \beta\xi$ и $\beta = \alpha\eta$ ($\xi \in \mathfrak{O}$, $\eta \in \mathfrak{O}$) следует, что $\alpha = \alpha\xi\eta$, откуда $1 = \xi\eta$ (так как $\alpha \neq 0$ и в кольце нет делителей нуля). Таким образом, ассоциированность двух элементов $\neq 0$ из $\mathfrak{O}$ означает, что они отличаются друг от друга на множитель, являющийся единицей в $\mathfrak{O}$.

Пусть $\mu \neq 0$ — элемент кольца $\mathfrak{O}$, не являющийся единицей. Говорят, что элементы α и β из $\mathfrak{O}$ сравнимы между собой по модулю μ, и пишут $\alpha \equiv \beta \pmod{\mu}$, если их разность $\alpha - \beta$ делится на μ. Для сравнений по модулю μ также справедливы обычные свойства сравнений в кольце целых чисел. Для любого $\alpha \in \mathfrak{O}$ через $\bar{\alpha}$ обозначим совокупность всех элементов из $\mathfrak{O}$, сравнимых с α по модулю μ. Совокупность $\bar{\alpha}$ называется классом вычетов по модулю μ. Равенство $\bar{\alpha} = \bar{\beta}$, очевидно, имеет место тогда и только тогда, когда $\alpha \equiv \beta \pmod{\mu}$. В множестве классов вычетов по модулю μ можно определить сумму и произведение классов, полагая

$$\bar{\alpha} + \bar{\beta} = \overline{\alpha + \beta}, \quad \bar{\alpha}\bar{\beta} = \overline{\alpha\beta}.$$

Поскольку в кольце $\mathfrak{O}$ сравнения по модулю μ можно почленно складывать и перемножать, то так определенные сумма и произведение классов не зависят от выбора представителей (вычетов) α и β. Простая проверка показывает, что относительно введенных действий все классы вычетов по модулю μ образуют коммутативное кольцо с единичным элементом $\bar{1}$ (возможно, с делителями нуля). Оно называется кольцом классов вычетов по модулю μ.

Если в каждом классе вычетов по модулю μ выбрать по представителю, то совокупность S всех таких представителей называется полной системой вычетов по модулю μ. Полная система вычетов S характеризуется, следовательно, тем, что всякий элемент кольца $\mathfrak{O}$ сравним по модулю μ с одним и только с одним элементом из S.

2. Идеалы. Подмножество A кольца $\mathfrak{O}$ называется идеалом, если оно является подгруппой аддитивной группы кольца $\mathfrak{O}$ и если для любого $\alpha \in A$ и любого $\xi \in \mathfrak{O}$ произведение $\xi\alpha$ принадлежит A. Подмножество, состоящее из одного нуля, а также все кольцо $\mathfrak{O}$ являются тривиальными примерами идеалов. Первый из этих идеалов называется нулевым, а второй — единичным.

Пусть $\alpha_1, \ldots, \alpha_m$ — произвольные элементы кольца $\mathfrak{O}$. Очевидно, что совокупность A всех линейных комбинаций $\xi_1\alpha_1 + \ldots + \xi_m\alpha_m$ этих элементов с коэффициентами ξ_i из $\mathfrak{O}$ является идеалом кольца $\mathfrak{O}$. Он называется идеалом, порожденным элементами $\alpha_1, \ldots, \alpha_m$, и обозначается через $A = (\alpha_1, \ldots, \alpha_m)$. Элементы $\alpha_1, \ldots, \alpha_m$ называются при этом образующими идеала A. В общем случае не для всякого идеала существуют конечные системы образующих. Идеал A называется главным, если для него существует система образующих, состоящая из одного элемента, т. е. если он имеет вид $A = (\alpha)$. Ненулевой главный идеал (α) состоит, очевидно, из тех элементов кольца $\mathfrak{O}$, которые делятся на α. Нулевой и единичный идеалы главные: нулевой идеал порождается нулем, а единичный — произвольной единицей ε кольца $\mathfrak{O}$. Два главных идеала (α) и (β) совпадают тогда и только тогда, когда α и β ассоциированы между собой.

Пусть A и B — два идеала кольца $\mathfrak{O}$. Совокупность всех элементов $\xi \in \mathfrak{O}$, представимых в виде

$$\xi = \alpha_1\beta_1 + \ldots + \alpha_s\beta_s,$$

где $\alpha_i \in A$ и $\beta_i \in B$ $(s \geqslant 1)$, является также идеалом в $\mathfrak{O}$. Этот идеал называется произведением идеалов A и B и обозначается через AB. Так как умножение идеалов коммутативно и ассоциативно, то все идеалы (коммутативного) кольца $\mathfrak{O}$ образуют относительно действия умножения коммутативную полугруппу.

Два элемента α и β из $\mathfrak{O}$ называются сравнимыми по модулю идеала A, в обозначении $\alpha \equiv \beta \pmod{A}$, если их разность $\alpha - \beta$ принадлежит A, т. е. если α и β принадлежат одному и тому же классу смежности по аддитивной подгруппе A. Ясно, что сравнение $\alpha \equiv \beta \pmod{A}$ имеет место тогда и только тогда, когда $\bar{\alpha} = \bar{\beta}$, где под $\bar{\gamma}$ понимается класс смежности по подгруппе A с представителем $\gamma \in \mathfrak{O}$. Отношение сравнимости по модулю идеала в случае главного идеала (μ) совпадает со сравнимостью по модулю элемента μ (см. п. 1). Рассмотрим фактор-группу $\mathfrak{O}/A$ аддитивной группы кольца $\mathfrak{O}$ по подгруппе A. В случае, когда подгруппа A есть идеал, в фактор-группе $\mathfrak{O}/A$ можно определить умножение. Именно, для $\bar{\alpha}$ и $\bar{\beta}$, из $\mathfrak{O}/A$ положим

$$\bar{\alpha}\bar{\beta} = \overline{\alpha\beta}.$$

Если $\bar{\alpha} = \bar{\alpha}_1$ и $\bar{\beta} = \bar{\beta}_1$, то ввиду равенства $\alpha_1\beta_1 - \alpha\beta = \alpha_1(\beta_1 - \beta) + \beta(\alpha_1 - \alpha)$ и ввиду того, что $\alpha_1 - \alpha$ и $\beta_1 - \beta$ принадлежат A,

имеем $\alpha_1\beta_1 \equiv \alpha\beta \pmod{A}$ (здесь существенно, что A — идеал), а значит, произведение $\overline{\alpha\beta}$ не зависит от выбора представителей α и β. Легко проверяется, что относительно этого действия умножения, а также действия сложения $\overline{\alpha} + \overline{\beta} = \overline{\alpha + \beta}$ фактор-группа $\mathfrak{O}/A$ является кольцом. Кольцо $\mathfrak{O}/A$ называется фактор-кольцом кольца $\mathfrak{O}$ по идеалу A. В случае главного идеала (μ) фактор-кольцо $\mathfrak{O}/(\mu)$ совпадает с кольцом классов вычетов по модулю μ.

3. Целые элементы. Всякое кольцо $\mathfrak{o}$ (коммутативное и без делителей нуля) можно вложить в поле. Чтобы показать это, рассмотрим совокупность всех формальных дробей a/b, где a и b — элементы из $\mathfrak{o}$, причем $b \neq 0$. Две дроби a/b и c/d называются равными тогда и только тогда, когда $ad = bc$. Сложение и умножение определяем формулами

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Легко проверяется, что эти действия согласованы с условием равенства, а также что относительно них все рассматриваемые дроби a/b образуют поле. Обозначим это поле через k_0. Если дроби вида $a/1 = ac/c$ $(c \neq 0)$ мы отождествим с элементами $a \in \mathfrak{o}$, то $\mathfrak{o}$ будет подкольцом поля k_0. Каждый элемент из k_0 является, очевидно, отношением двух элементов из $\mathfrak{o}$.

Пусть теперь Ω — произвольное поле, содержащее $\mathfrak{o}$ в качестве подкольца. Совокупность k всех отношений a/b, где a и b принадлежат $\mathfrak{o}$ $(b \neq 0)$, является подполем поля Ω. Это подполе называется полем отношений кольца $\mathfrak{o}$. Легко видеть, что поле k изоморфно построенному выше полю k_0, а значит, оно определено кольцом $\mathfrak{o}$ однозначно (с точностью до изоморфизма).

Определение. *Пусть кольцо $\mathfrak{o}$ содержится в поле Ω. Элемент $\alpha \in \Omega$ называется целым относительно $\mathfrak{o}$, если он является корнем многочлена с коэффициентами из $\mathfrak{o}$, старший коэффициент которого равен* 1.

Так как всякий элемент $a \in \mathfrak{o}$ является корнем многочлена $t - a$, то все элементы из $\mathfrak{o}$ являются целыми относительно $\mathfrak{o}$.

Пусть $\omega_1, \ldots, \omega_m$ — произвольные элементы из Ω. Совокупность M всех линейных комбинаций $a_1\omega_1 + \ldots + a_m\omega_m$ с коэффициентами $a_i \in \mathfrak{o}$ назовем $\mathfrak{o}$-модулем в Ω с конечным числом образующих, а сами элементы $\omega_1, \ldots, \omega_m$ — образующими $\mathfrak{o}$-модуля M. Так как $1 \in \mathfrak{o}$, то все ω_i содержатся в M.

Лемма 1. *Если $\mathfrak{o}$-модуль M с конечным числом образующих является кольцом, то все его элементы целые относительно $\mathfrak{o}$.*

Доказательство. Мы можем, конечно, считать, что не все ω_i равны нулю. Пусть α — произвольный элемент из M. Так как при любом i произведение $\alpha\omega_i$ принадлежит M, то

$$\alpha\omega_i = \sum_{j=1}^{m} a_{ij}\omega_j, \qquad a_{ij} \in \mathfrak{o}, \qquad i = 1, \ldots, m.$$

Отсюда следует, что $\det(\alpha E - (a_{ij})) = 0$ (E — единичная матрица порядка m). Таким образом, элемент α является корнем многочлена $f(t) = \det(tE - (a_{ij}))$ с коэффициентами из $\mathfrak{o}$ и со старшим коэффициентом 1, а это и доказывает лемму.

Теорема 2. *Совокупность $\mathfrak{O}$ всех целых относительно $\mathfrak{o}$ элементов из Ω является кольцом.*

Доказательство. Нам надо проверить, что сумма, разность и произведение двух целых элементов α и β из Ω являются также целыми элементами поля Ω. Если α и β являются соответственно корнями многочленов

$$t^m - a_m t^{m-1} - \ldots - a_1, \qquad t^n - b_n t^{n-1} - \ldots - b_1,$$

где a_i и b_j — элементы из $\mathfrak{o}$, то

$$\alpha^m = a_1 + a_2\alpha + \ldots + a_m\alpha^{m-1}, \ \beta^n = b_1 + b_2\beta + \ldots + b_n\beta^{n-1}.$$

Отсюда легко следует, что $\mathfrak{o}$-модуль, состоящий из всех линейных комбинаций произведений

$$\alpha^i\beta^j, \qquad 0 \leqslant i < m, \quad 0 \leqslant j < n, \tag{1}$$

с коэффициентами из $\mathfrak{o}$, является кольцом (так как произведение $\alpha^k\beta^l$ при любых $k \geqslant 0$ и $l \geqslant 0$ может быть представлено в виде линейной комбинации элементов (1) с коэффициентами из $\mathfrak{o}$). По лемме 1 все элементы этого кольца целые относительно $\mathfrak{o}$; в частности, целыми будут $\alpha \pm \beta$ и $\alpha\beta$. Теорема 2 доказана.

Определение. *Пусть $\mathfrak{o}$ — подкольцо поля Ω. Совокупность $\mathfrak{O}$ всех элементов Ω, целых относительно $\mathfrak{o}$, называется целым замыканием кольца $\mathfrak{o}$ в поле Ω.*

Определение. *Подкольцо $\mathfrak{O}_0$ поля K называется целозамкнутым в K, если его целое замыкание в K совпадает с $\mathfrak{O}_0$.*

Кольцо $\mathfrak{o}$ называют просто *целозамкнутым*, если оно целозамкнуто в своем поле отношений k.

Теорема 3. *Пусть $\mathfrak{o}$ — подкольцо поля Ω. Целое замыкание $\mathfrak{O}$ кольца $\mathfrak{o}$ в поле Ω целозамкнуто в Ω.*

Доказательство. Пусть θ — произвольный элемент из Ω, целый относительно $\mathfrak{O}$, так что

$$\theta^n = \alpha_1 + \alpha_2\theta + \ldots + \alpha_n\theta^{n-1}, \tag{2}$$

где все α_i принадлежат $\mathfrak{O}$. Нам надо доказать, что $\theta \in \mathfrak{O}$. Для каждого $i = 1, \ldots, n$ при некотором m_i имеет место равенство

$$\alpha_i^{m_i} = \sum_{j=1}^{m_i} a_{ij}\alpha_i^{j-1}, \qquad a_{ij} \in \mathfrak{o} \tag{3}$$

(так как α_i целый относительно $\mathfrak{o}$). Рассмотрим $\mathfrak{o}$-модуль M, порожденный произведениями

$$\alpha_1^{k_1} \ldots \alpha_n^{k_n}\theta^k, \qquad 0 \leqslant k_i < m_i, \quad 0 \leqslant k < n. \tag{4}$$

Из (2) и (3) легко следует, что всякое произведение $\alpha_1^{l_1} \ldots \alpha_n^{l_n}\theta^l$

с неотрицательными показателями может быть выражено в виде линейной комбинации элементов (4) с коэффициентами из $\mathfrak{o}$, а значит, модуль M является кольцом. По лемме 1 все элементы из M целые относительно $\mathfrak{o}$. Целым, в частности, является и θ, а это и требовалось доказать.

Лемма 2. *Пусть кольцо $\mathfrak{o}$ целозамкнуто в своем поле отношений k, и пусть старший коэффициент многочлена $f(t) \in \mathfrak{o}[t]$ равен 1. Тогда, если старший коэффициент делителя $\varphi(t) \in k[t]$ многочлена $f(t)$ равен 1, то $\varphi(t) \in \mathfrak{o}[t]$.*

Доказательство. Рассмотрим над полем k расширение Ω/k, в котором $f(t)$ раскладывается на линейные множители (следствие теоремы 5 § 2). Все корни $f(t)$ принадлежат, очевидно, целому замыканию $\mathfrak{O}$ кольца $\mathfrak{o}$ в поле Ω. В частности, кольцу $\mathfrak{O}$ принадлежат и все корни $\varphi(t)$. Но из разложения $\varphi(t) = (t-\gamma_1)\dots(t-\gamma_s)$ следует тогда, что все коэффициенты $\varphi(t)$ принадлежат $\mathfrak{O}$, а так как $\mathfrak{O} \cap k = \mathfrak{o}$ (ввиду целозамкнутости $\mathfrak{o}$), то эти коэффициенты принадлежат $\mathfrak{o}$, что и требовалось доказать.

Из леммы 2 очевидным образом вытекает следующий факт.

Теорема 4. *Пусть кольцо $\mathfrak{o}$ целозамкнуто в своем поле отношений, и пусть Ω/k — алгебраическое расширение поля k. Для того чтобы элемент $\alpha \in \Omega$ был целым относительно $\mathfrak{o}$, необходимо и достаточно, чтобы все коэффициенты его минимального многочлена принадлежали $\mathfrak{o}$.*

4. Дробные идеалы.

Определение. *Пусть $\mathfrak{O}$ — произвольное кольцо и K — его поле отношений. Подмножество $A \subset K$, содержащее отличные от нуля элементы, называется идеалом поля K (относительно кольца $\mathfrak{O}$), если оно обладает свойствами:*

1) *A является группой относительно действия сложения;*

2) *для любого $\alpha \in A$ и любого $\xi \in \mathfrak{O}$ произведение $\xi\alpha$ принадлежит A;*

3) *в поле K существует такой элемент $\gamma \neq 0$, что $\gamma A \subset \mathfrak{O}$.*

Идеал A называется целым, если он содержится в $\mathfrak{O}$, и дробным в противном случае.

Понятие целого идеала в K совпадает, таким образом, с понятием ненулевого идеала кольца $\mathfrak{O}$.

Если A и B — два идеала поля K, то под их произведением AB понимается совокупность всех элементов $\gamma \in K$, представимых в виде

$$\gamma = \alpha_1\beta_1 + \dots + \alpha_m\beta_m,\ m \geqslant 1,\ \alpha_i \in A,\ \beta_i \in B,\quad 1 \leqslant i \leqslant m.$$

Очевидно, что произведение двух идеалов поля K является также идеалом поля K. (В применении к целым идеалам введенное умножение совпадает с обычным умножением идеалов в кольцах.)

Если A и B — два идеала поля K (относительно $\mathfrak{O}$), то через $A:B$ обозначается идеал поля K, состоящий из всех тех $\xi \in K$,

для которых $\xi B \subset A$. Легко видеть, что

$$A : B = \bigcap_{\beta \in B, \beta \neq 0} A\beta^{-1},$$

где β пробегает все отличные от нуля элементы идеала B.

Идеал $\gamma\mathfrak{O}$ ($\gamma \in K^*$), состоящий из произведений $\gamma\xi$, где ξ пробегает все элементы из $\mathfrak{O}$, называется главным идеалом поля K.

Задачи

1. Идеал A кольца $\mathfrak{O}$ называется максимальным, если $A \neq \mathfrak{O}$ и если всякий промежуточный идеал B (для которого $A \subset B \subset \mathfrak{O}$) совпадает либо с A, либо с $\mathfrak{O}$. Доказать, что идеал A максимален тогда и только тогда, когда фактор-кольцо $\mathfrak{O}/A$ есть поле.

2. Пусть в поле Ω имеем подкольца $o \subset \mathfrak{O}_0 \subset \mathfrak{O}$. Доказать, что если каждый элемент из $\mathfrak{O}_0$ целый над o и каждый элемент из $\mathfrak{O}$ целый над $\mathfrak{O}_0$, то все элементы из $\mathfrak{O}$ целые над o.

3. Доказать, что если кольцо o целозамкнуто, то кольцо многочленов $o[t]$ с коэффициентами из o также целозамкнуто.

4. Пусть $\mathfrak{O}$ — подкольцо поля K, обладающее свойством: если элемент $\xi \neq 0$ из K не содержится в $\mathfrak{O}$, то $\xi^{-1} \in \mathfrak{O}$. Доказать, что кольцо $\mathfrak{O}$ целозамкнуто.

5. Пусть в кольце $\mathfrak{O}$ с полем отношений K выполнено следующее условие: если для элемента $\xi \neq 0$ из K все его степени ξ^n ($n \geqslant 0$) содержатся в некотором главном (дробном) идеале $\gamma\mathfrak{O}$ ($\gamma \in K^*$), то $\xi \in \mathfrak{O}$. Доказать, что тогда кольцо $\mathfrak{O}$ целозамкнуто. Кольцо $\mathfrak{O}$, удовлетворяющее условию задачи, называется *вполне целозамкнутым*.

6. Доказать, что если целозамкнутое кольцо нётерово (всякий идеал кольца порождается конечной системой элементов), то оно и вполне целозамкнуто.

7. Пусть $K = \mathbb{Q}(x)$ — поле рациональных функций от одной переменной x над полем рациональных чисел $\mathbb{Q}$. Каждый элемент $u \neq 0$ из K однозначно представляется в виде

$$u = x^m \frac{f(x)}{g(x)}, \tag{5}$$

где многочлены f и g из $\mathbb{Q}[x]$ таковы, что $g(0) = 1$ и $f(0) = a \neq 0$. Зафиксируем простое рациональное число p и обозначим через $\mathfrak{O}$ подмножество в K, состоящее, помимо нуля, из тех элементов $u \in K^*$, для которых в представлении (5) либо $m > 0$, либо $m = 0$ и рациональное число $a = f(0)$ не содержит p в знаменателе (в несократимой записи). Нетрудно проверить, что $\mathfrak{O}$ — подкольцо поля K. Доказать, что кольцо $\mathfrak{O}$ целозамкнуто, но не является вполне целозамкнутым (все степени $\left(\frac{1}{p}\right)^n$, $n \geqslant 0$, содержатся в главном идеале $x^{-1}\mathfrak{O}$).

8. Пусть $\mathfrak{O}$ — кольцо с полем отношений K. Идеал поля K (относительно $\mathfrak{O}$) называется d-идеалом, если он является пересечением некоторого семейства главных идеалов поля K (вообще говоря, дробных). Доказать следующие утверждения:

1) если пересечение системы d-идеалов ненулевое, то оно является d-идеалом;

2) вместе с A идеал γA ($\gamma \in K^*$) также является d-идеалом;

3) для d-идеала A и любого идеала B поля K идеал $A : B$ является d-идеалом;

4) если для идеалов A и B имеем $AB = \mathfrak{O}$, то A и B являются d-идеалами.

§ 5. Характеры

В этом параграфе мы изложим некоторые сведения о характерах конечных абелевых групп и числовых характерах.

1. Строение конечных абелевых групп. Строение произвольных конечных абелевых групп определяется следующей теоремой.

Теорема 1. *Всякая конечная абелева группа может быть представлена в виде прямого произведения циклических подгрупп.*

Согласно задачам 1 и 2 конечная циклическая группа неразложима в прямое произведение собственных подгрупп тогда и только тогда, когда ее порядок есть степень простого числа. Если поэтому в некотором разложении конечной абелевой группы G в прямое произведение $G=A_1\times\ldots\times A_s$ циклические сомножители A_i не допускают дальнейшего разложения, то их порядки являются степенями простых чисел. Разложение группы G в прямое произведение неразложимых сомножителей определено, вообще говоря, неоднозначно. Однако набор порядков неразложимых циклических сомножителей A_i определен для данной группы G единственным образом. Эти порядки (являющиеся степенями простых чисел) называются *инвариантами* конечной абелевой группы. Произведение всех инвариантов данной группы равно, очевидно, ее порядку.

2. Характеры конечных абелевых групп.

Определение. *Характером конечной абелевой группы G называется гомоморфное отображение G в мультипликативную группу поля всех комплексных чисел.*

Другими словами, характер группы G — это такая не обращающаяся в нуль комплекснозначная функция χ на G, для которой

$$\chi(xy)=\chi(x)\chi(y) \tag{1}$$

при любых x и y из G.

Так как при всяком гомоморфизме групп единичный элемент отображается на единичный, то $\chi(1)=1$, т. е. значение всякого характера χ на единичном элементе группы всегда равно единице. Если элемент $x\in G$ имеет порядок k, то

$$(\chi(x))^k=\chi(x^k)=\chi(1)=1, \tag{2}$$

т. е. $\chi(x)$ является корнем степени k из 1. Если m есть наибольший из порядков элементов группы G, то согласно задаче 3 порядок всякого элемента из G будет делителем m. Любое значение $\chi(x)$ является, следовательно, корнем степени m из 1, а значит, характеры можно определить также как гомоморфизмы G в группу корней m-й степени из 1.

Представим группу G в виде прямого произведения циклических подгрупп: $G=\{a_1\}\times\ldots\times\{a_s\}$. Так как каждый элемент

$x \in G$ может быть записан в виде

$$x = a_1^{k_1} \dots a_s^{k_s}, \tag{3}$$

а в силу (1) $\chi(x) = \chi(a_1)^{k_1} \dots \chi(a_s)^{k_s}$, то получаем, что характер χ вполне определен значениями $\chi(a_1), \dots, \chi(a_s)$. Если a_i имеет порядок m_i, то ввиду (2) $\chi(a_i)$ есть корень степени m_i из 1. Обратно, выберем произвольно для каждого $i = 1, \dots, s$ какой-нибудь корень ε_i степени m_i из 1 и для элемента $x \in G$, представленного в виде (3), положим

$$\chi(x) = \varepsilon_1^{k_1} \dots \varepsilon_s^{k_s}. \tag{4}$$

Легко видеть, что значение (4) не зависит от выбора показателей k_i в представлении (3) (каждый показатель k_i определен по модулю m_i), а также что так определенная однозначная функция χ на G удовлетворяет условию (1) и является, следовательно, характером группы G. Корень ε_i можно выбрать m_i способами, поэтому мы имеем всего $m_1 \dots m_s$ различных функций χ вида (4). Мы получили, таким образом, следующую теорему.

Теорема 2. *Число всех характеров конечной абелевой группы равно ее порядку.*

Определим умножение характеров. Для характеров χ и χ' группы G положим

$$(\chi\chi')(x) = \chi(x)\chi'(x), \qquad x \in G.$$

Очевидно, что функция $\chi\chi'$ также является характером группы G. Характер χ_0, для которого $\chi_0(x) = 1$ при всех $x \in G$, называется *единичным*. Ясно, что $\chi\chi_0 = \chi$ для любого характера χ. Если для произвольного характера χ группы G мы положим

$$\overline{\chi}(x) = \overline{\chi(x)}, \qquad x \in G,$$

где $\overline{\chi(x)}$ — комплексно сопряженное число для $\chi(x)$, то функция $\overline{\chi}$ также будет характером группы G, при этом $\chi\overline{\chi} = \chi_0$. Так как умножение характеров, очевидно, ассоциативно, то мы получаем, что все характеры конечной абелевой группы относительно введенного действия умножения образуют группу.

Пусть $G = \{a\}$ — циклическая группа порядка m и ε — фиксированный первообразный корень степени m из 1. Обозначим через χ тот характер группы G, для которого $\chi(a) = \varepsilon$ (и, значит, $\chi(a^k) = \varepsilon^k$). Так как $\chi^r(a) = \varepsilon^r$, то характеры $\chi_0 = \chi^m$, χ, χ^2, $\dots$ $\dots$, χ^{m-1} попарно различны и, следовательно, исчерпывают собой всю группу характеров группы G. Мы видим, таким образом, что группа характеров для конечной циклической группы также циклична. В общем случае легко может быть доказана теорема: *всякая конечная абелева группа изоморфна своей группе характеров.*

В произвольной абелевой группе G порядка n рассмотрим подгруппу H порядка m. Если характер χ группы G рассматривать лишь на элементах подгруппы H, то полученная функция будет, очевидно, характером группы H. Обозначим этот характер через $\widehat{\chi}$. Ясно, что отображение $\chi \to \widehat{\chi}$ является гомоморфизмом группы характеров X группы G в группу характеров Y подгруппы H. Обозначим через A его ядро. Характеры χ из A характеризуются тем, что $\chi(z) = 1$ при всех $z \in H$. Если $\chi \in A$, а x и x' принадлежат одному и тому же классу смежности G по H, то, очевидно, $\chi(x) = \chi(x')$. Полагая $\overline{\chi}(\overline{x}) = \chi(x)$, где $\chi \in A$, а $\overline{x}$ — класс смежности G по H с представителем $x \in G$, мы получаем однозначную функцию $\overline{\chi}$ на фактор-группе G/H, и эта функция является характером группы G/H. Обратно, если ψ — произвольный характер фактор-группы G/H, то, положив

$$\chi(x) = \psi(\overline{x}), \qquad x \in G,$$

мы получим характер $\chi \in A$, для которого $\overline{\chi} = \psi$. Так как при отображении $\chi \to \overline{\chi}$ ($\chi \in A$) различным характерам из A отвечают различные характеры фактор-группы G/H, то нами доказано, что число характеров χ, принадлежащих A, равно числу характеров группы G/H, т. е. равно n/m (теорема 2). Но в таком случае образ группы X при гомоморфизме $\chi \to \widehat{\chi}$ (группы X в группу Y) будет иметь порядок $n : \frac{n}{m} = m$, а так как по теореме 2 группа Y также имеет порядок m, то этот образ совпадает с Y. Это значит, что всякий характер группы H имеет вид $\widehat{\chi}$ при некотором характере χ группы G. Ясно, что число характеров $\chi \in X$, индуцирующих один и тот же характер на H, равно $n/m = (G : H)$.

Нами доказана следующая теорема.

Теорема 3. *Если G — конечная абелева группа и H — ее подгруппа, то любой характер группы H может быть продолжен до характера группы G и число таких продолжений равно индексу $(G : H)$.*

Следствие 1. *Если x — отличный от единицы элемент из G, то существует такой характер χ группы G, что $\chi(x) \neq 1$.*

Действительно, рассмотрим циклическую группу $\{x\} = H$. Так как ее порядок больше 1, то на H существует неединичный характер χ', для которого, следовательно, $\chi'(x) \neq 1$. Продолжив χ' до характера группы G, мы и получим требуемый характер χ.

Следствие 2. *Если элемент x из G не содержится в подгруппе H, то существует характер χ группы G, для которого $\chi(x) \neq 1$ и $\chi(z) = 1$ для всех $z \in H$.*

Действительно, единичный характер группы H можно продолжить до неединичного характера подгруппы $\{x, H\}$, который в свою очередь может быть продолжен до характера группы G.

Установим теперь некоторые соотношения между значениями характеров. Если χ_0 — единичный характер, то $\chi_0(x) = 1$ при всех $x \in G$, а потому $\sum_{x \in G} \chi_0(x) = n$, где n — порядок группы G. Предположим, что характер χ отличен от χ_0, так что $\chi(z) \neq 1$ для некоторого $z \in G$. Если x пробегает все элементы группы G, то zx также будет пробегать все элементы из G. Полагая $S = \sum_{x \in G} \chi(x)$, имеем, следовательно,

$$S = \sum_{x \in G} \chi(zx) = \chi(z) S.$$

Ввиду условия $\chi(z) \neq 1$ полученное равенство возможно лишь при $S = 0$. Таким образом, мы имеем формулу:

$$\sum_{x \in G} \chi(x) = \begin{cases} n, & \text{если } \chi = \chi_0, \\ 0, & \text{если } \chi \neq \chi_0. \end{cases} \tag{5}$$

Значение любого характера χ на единичном элементе группы равно единице, поэтому $\sum_{\chi} \chi(1) = n$ (здесь и далее χ пробегает все характеры группы G). Положим $T = \sum_{\chi} \chi(x)$. По следствию 1 теоремы 3 существует характер χ', для которого $\chi'(x) \neq 1$ (если $x \neq 1$). Вместе с χ произведение $\chi\chi'$ также пробегает все характеры группы G. Поэтому

$$T = \sum_{\chi} (\chi'\chi)(x) = \sum_{\chi} \chi'(x) \chi(x) = \chi'(x) T,$$

а так как $\chi'(x) \neq 1$, то $T = 0$. Этим доказана формула:

$$\sum_{\chi} \chi(x) = \begin{cases} n, & \text{если } x = 1, \\ 0, & \text{если } x \neq 1. \end{cases} \tag{6}$$

3. Числовые характеры. Для натурального числа m через G_m обозначим группу относительно действия умножения классов вычетов по модулю m целых рациональных чисел, взаимно простых с m. Класс чисел по модулю m, содержащий a в качестве представителя, будем обозначать через $\bar{a}$.

Каждому характеру χ группы G_m мы можем естественным образом сопоставить функцию χ^* на всех целых рациональных числах a, взаимно простых с m, полагая $\chi^*(a) = \chi(\bar{a})$. Распространим эту функцию χ^* на все целые рациональные числа, считая, что $\chi^*(a) = 0$, если только a и m не взаимно просты. Так полученная функция χ^* (определенная на всех целых рациональных числах) называется *числовым характером* по модулю m. В дальнейшем χ^* будет обозначаться той же буквой χ, что и исходный характер на группе G_m. Ясно, что различные характеры

группы G_m порождают различные числовые характеры, так что число числовых характеров по модулю m равно $\varphi(m)$.

Из определения легко вытекают следующие свойства числовых характеров:

1° Для любого целого рационального a значение $\chi(a)$ есть комплексное число, причем $\chi(a) \neq 0$ тогда и только тогда, когда a взаимно просто с m.

2° Если $a \equiv a' \pmod m$, то $\chi(a) = \chi(a')$.

3° Для любых целых рациональных a и b имеем $\chi(ab) = \chi(a)\chi(b)$.

Оказывается, что числовые характеры этими тремя свойствами вполне характеризуются. Действительно, пусть функция η удовлетворяет условиям 1°—3°. Для класса $\bar{a} \in G_m$, $(a, m) = 1$, положим $\chi(\bar{a}) = \eta(a)$. В силу 2° значение $\chi(\bar{a})$ не зависит от выбора представителя a, в силу 1° оно отлично от нуля. Кроме того, если $(a, m) = 1$ и $(b, m) = 1$, то по условию 3°

$$\chi(\bar{a}\bar{b}) = \chi(\overline{ab}) = \eta(ab) = \eta(a)\eta(b) = \chi(\bar{a})\chi(\bar{b}).$$

Таким образом, χ есть характер группы G_m, причем соответствующий ему числовой характер χ^* совпадает с функцией η.

Пусть m' — натуральное число, делящееся на m. Каждому характеру χ по модулю m мы можем сопоставить естественным образом некоторый характер χ' по модулю m'. Именно, если a взаимно просто с m' (а значит, и с m), то полагаем $\chi'(a) = \chi(a)$; если же $(a, m') > 1$, то $\chi'(a) = 0$. Числовая функция χ' удовлетворяет всем трем условиям 1°—3°, а потому является числовым характером по модулю m'. Будем говорить, что χ' индуцирован характером χ.

Определение. *Если для некоторого характера χ по модулю m существует такой собственный делитель d числа m и такой характер χ_1 по модулю d, что χ_1 индуцирует χ, то этот характер χ называется непримитивным; в противном случае он называется примитивным.*

Теорема 4. *Для того чтобы характер χ по модулю m был примитивным, необходимо и достаточно, чтобы для любого собственного делителя d числа m среди чисел x, сравнимых с единицей по модулю d и взаимно простых с m, существовало такое, для которого $\chi(x) \neq 1$.*

Доказательство. Если характер χ непримитивный, то он индуцируется некоторым характером χ_1 по модулю d, где d — собственный делитель m. Это значит, что для любого x, взаимно простого с m, имеет место равенство $\chi(x) = \chi_1(x)$. Если при этом $x \equiv 1 \pmod d$, то $\chi(x) = \chi_1(x) = 1$. Обратно, предположим, что для некоторого собственного делителя d числа m имеем $\chi(x) = 1$, если только $(x, m) = 1$ и $x \equiv 1 \pmod d$. Для всякого a, взаимно простого с d, мы можем найти такое a', что $(a', m) = 1$ и $a' \equiv a \pmod d$. Положим $\chi_1(a) = \chi(a')$. Значение $\chi_1(a)$ не зависит

от выбора a'. В самом деле, если $a' \equiv a'' \pmod{d}$, где a'' также взаимно просто с m, то $a'' \equiv xa' \pmod{m}$ при некотором x, взаимно простом с m. Поскольку $x \equiv 1 \pmod{d}$, то, в силу условия теоремы, $\chi(x) = 1$, а тогда $\chi(a'') = \chi(x)\chi(a') = \chi(a')$. Полагая, далее, $\chi_1(a) = 0$, если $(a, d) \neq 1$, мы получаем числовую функцию χ_1, которая, как легко видеть, является числовым характером по модулю d. Так как $\chi_1(a) = \chi(a)$ при $(a, m) = 1$, то χ индуцируется характером χ_1. Этим доказательство теоремы 4 закончено.

Рассмотренные в настоящем пункте числовые характеры часто называют также *характерами Дирихле*.

Задачи

1. Показать, что конечная циклическая группа, порядок которой есть степень простого числа, неразложима в прямое произведение собственных подгрупп.

2. Пусть порядок конечной циклической группы G равен произведению взаимно простых чисел k и l. Доказать, что G можно представить в виде прямого произведения двух подгрупп порядков k и l.

3. Пусть a — элемент максимального порядка конечной абелевой группы G. Доказать, что циклическая подгруппа $\{a\}$ выделяется в G прямым сомножителем.

4. Пусть k — натуральное число. Доказать, что элемент x конечной абелевой группы G является k-й степенью в G тогда и только тогда, когда $\chi(x) = 1$ для всех тех характеров χ группы G, для которых $\chi^k = \chi_0$ (χ_0 — единичный характер).

5. Пусть G — конечная абелева группа порядка n. Выпишем в какомнибудь порядке ее элементы $x_1, \ldots, x_n$ и ее характеры $\chi_1, \ldots, \chi_n$. Доказать, что матрица $\left(\frac{1}{\sqrt{n}}\chi_i(x_j)\right)_{i,j}$ унитарна.

6. Пусть $m_1, \ldots, m_k$ — попарно взаимно простые натуральные числа и $m = m_1 \ldots m_k$. Доказать, что для всякого характера χ по модулю m существуют однозначно определенные характеры χ_i по модулю m_i ($i = 1, \ldots, k$) такие, что для любого целого рационального a справедливо равенство $\chi(a) = \chi_1(a) \ldots \chi_k(a)$. (Для каждого i характер χ_i определяется равенством $\chi_i(a) = \chi(a')$, где a' определено сравнениями $a' \equiv a \pmod{m_i}$, $a' \equiv 1 \left(\mathrm{mod}\ \frac{m}{m_i}\right)$.)

7. Доказать, что если в условиях задачи 6 характер χ по модулю m примитивен, то для каждого $i = 1, \ldots, k$ характер χ_i по модулю m_i также примитивен.

8. Пусть d_1 и d_2 — делители натурального числа m и $d = (d_1, d_2)$. Доказать, что если характер χ по модулю m индуцируется некоторым характером по модулю d_1 и индуцируется некоторым характером по модулю d_2, то он индуцируется также и некоторым характером по модулю d.

9. Доказать, что каждый характер χ по модулю m индуцируется примитивным характером по некоторому однозначно определенному модулю f (являющемуся делителем m). Число f называется *ведущим модулем характера* χ.

10. Доказать, что число примитивных характеров по модулю m равно $\sum_{d \mid m} \mu(d)\, \varphi\left(\frac{m}{d}\right)$ (d пробегает все делители числа m, μ — функция Мёбиуса, φ — функция Эйлера).

11. Доказать, что по модулю m примитивные характеры существуют тогда и только тогда, когда m либо нечетно, либо делится на 4.

12. Пусть $\mathfrak{F}$ есть линейное пространство над полем комплексных чисел, состоящее из функций f на элементах конечной абелевой группы G с комплексными значениями $f(\sigma)$, $\sigma \in G$. Для каждого элемента $\omega \in G$ через T_ω обозначим оператор сдвига, действующий по формуле $(T_\omega f)(\sigma) = f(\omega\sigma)$. Доказать, что все характеры χ группы G являются собственными векторами операторов T_ω. Чему равны соответствующие собственные числа?

13. Сохраним обозначения предшествующей задачи и рассмотрим для фиксированной функции $f \in \mathfrak{F}$ квадратную матрицу $A = (f(\sigma\tau^{-1}))_{\sigma,\,\tau}$, где σ и τ пробегают все элементы группы G, расположенные в некотором порядке. Доказать, что определитель этой матрицы равен $\prod_\chi \left(\sum_\sigma f(\sigma)\chi(\sigma)\right)$ (σ пробегает все элементы, а χ — все характеры группы G).

Указание. Матрица A является матрицей оператора $T = \sum_\omega f(\omega) T_\omega$ в базисе, состоящем из функций l_σ, для которых

$$l_\sigma(\tau) = \begin{cases} 1 & \text{при } \sigma = \tau, \\ 0 & \text{при } \sigma \neq \tau. \end{cases}$$

Найти собственные числа оператора T.

14. Доказать утверждение задачи 13, рассматривая определитель произведения матрицы $(\chi(\sigma))_{\chi,\,\sigma}$ на матрицу A.

15. Пусть χ_1 и χ_2 — два примитивных числовых характера с ведущими модулями f_1 и f_2. Обозначим через m общее наименьшее кратное чисел f_1 и f_2 и через χ — характер по модулю m, для которого $\chi(a) = \chi_1(a)\chi_2(a)$ для всех a, взаимно простых с m. Однозначно определенный примитивный характер, который индуцирует характер χ, называется произведением $\chi_1 \cdot \chi_2$ примитивных характеров χ_1 и χ_2. Доказать, что все примитивные числовые характеры (для всевозможных ведущих модулей) относительно введенного действия умножения образуют группу.

16. Пусть G — конечная абелева группа и X — ее группа характеров. Каждой подгруппе H группы G сопоставим подгруппу $\alpha(H)$ в группе характеров X, состоящую из тех $\chi \in X$, которые аннулируют H (т. е. для которых $\chi(z) = 1$ при всех $z \in H$). Показать, что α является взаимно однозначным соответствием между всеми подгруппами группы G и всеми подгруппами ее группы характеров X. При этом соответствии включения $H_1 \subset H_2$ и $\alpha(H_1) \supset \alpha(H_2)$ равносильны.

17. Пусть Σ — конечное поле характеристики p и пусть

$$\psi(\bar{a}) = e^{2\pi i(a/p)} = \cos\frac{2\pi a}{p} + i\sin\frac{2\pi a}{p}, \qquad \bar{a} \in \mathbb{F}_p = \Sigma_0,\ a \in \mathbb{Z}.$$

Для фиксированного $\alpha \in \Sigma$ положим

$$\chi_\alpha(\xi) = \psi\left(\mathrm{Sp}_{\Sigma/\Sigma_0}\alpha\xi\right), \quad \xi \in \Sigma.$$

Показать, что соответствие $\alpha \to \chi_\alpha$, $\alpha \in \Sigma$, является изоморфизмом аддитивной группы поля Σ на группу ее характеров.

18. Пусть W_p — группа корней из 1 всех степеней p^m при всех $m \geqslant 1$ (группа типа p^∞). Показать, что группа характеров группы W_p изоморфна аддитивной группе всех целых p-адических чисел.

ТАБЛИЦА 1

Число h классов дивизоров и основная единица $\varepsilon > 1$ вещественных *квадратичных полей* $\mathbb{Q}(\sqrt{d})$. $2 \leqslant d \leqslant 101$, d свободно от квадратов, $\omega = \frac{1+\sqrt{d}}{2}$ при $d \equiv 1 \pmod 4$ и $\omega = \sqrt{d}$ при $d \equiv 2, 4 \pmod 4$.

d	h	ε	$N(\varepsilon)$	d	h	ε	$N(\varepsilon)$
2	1	$1+\omega$	-1	53	1	$3+\omega$	-1
3	1	$2+\omega$	$+1$	55	2	$89+12\omega$	$+1$
5	1	ω	-1	57	1	$131+40\omega$	$+1$
6	1	$5+2\omega$	$+1$	58	2	$99+13\omega$	-1
7	1	$8+3\omega$	$+1$	59	1	$530+69\omega$	$+1$
10	2	$3+\omega$	-1	61	1	$17+5\omega$	-1
11	1	$10+3\omega$	$+1$	62	1	$63+8\omega$	$+1$
13	1	$1+\omega$	-1	65	2	$7+2\omega$	-1
14	1	$15+4\omega$	$+1$	66	2	$65+8\omega$	$+1$
15	2	$4+\omega$	$+1$	67	1	$48\,842+5967\omega$	$+1$
17	1	$3+2\omega$	-1	69	1	$11+3\omega$	$+1$
19	1	$170+39\omega$	$+1$	70	2	$251+30\omega$	$+1$
21	1	$2+\omega$	$+1$	71	1	$3480+413\omega$	$+1$
22	1	$197+42\omega$	$+1$	73	1	$943+250\omega$	-1
23	1	$24+5\omega$	$+1$	74	2	$43+5\omega$	-1
26	2	$5+\omega$	-1	77	1	$4+\omega$	$+1$
29	1	$2+\omega$	-1	78	2	$53+6\omega$	$+1$
30	2	$11+2\omega$	$+1$	79	3	$80+9\omega$	$+1$
31	1	$1520+273\omega$	$+1$	82	4	$9+\omega$	-1
33	1	$19+8\omega$	$+1$	83	1	$82+9\omega$	$+1$
34	2	$35+6\omega$	$+1$	85	2	$4+\omega$	-1
35	2	$6+\omega$	$+1$	86	1	$10\,405+1122\omega$	$+1$
37	1	$5+2\omega$	-1	87	2	$28+3\omega$	$+1$
38	1	$37+6\omega$	$+1$	89	1	$447+106\omega$	-1
39	2	$25+4\omega$	$+1$	91	2	$1574+165\omega$	$+1$
41	1	$27+10\omega$	-1	93	1	$13+3\omega$	$+1$
42	2	$13+2\omega$	$+1$	94	1	$2\,143\,295+221\,064\omega$	$+1$
43	1	$3482+531\omega$	$+1$	95	2	$39+4\omega$	$+1$
46	1	$24335+3\,588\omega$	$+1$	97	1	$5035+1138\omega$	-1
47	1	$48+7\omega$	$+1$	101	1	$9+2\omega$	-1
51	2	$50+7\omega$	$+1$				

Замечание. Таблица 1 извлечена из работы [83], в которой h и ε вычислены для всех $d < 2025$. Вычисление числа h основано на утверждении задачи 15 § 7 гл. II.

ТАБЛИЦА 2

Число h классов дивизоров и норма $N(\varepsilon)$ основной единицы ε вещественных квадратичных полей $\mathbb{Q}(\sqrt{d})$, d свободно от квадратов, $101 \leqslant d < 500$.

d	h	$N(\varepsilon)$	d	h	$N(\varepsilon)$	d	h	$N(\varepsilon)$	d	h	$N(\varepsilon)$	d	h	$N(\varepsilon)$
101	1	−1	182	2	+1	259	2	+1	341	1	+1	422	1	+1
102	2	+1	183	2	+1	262	1	+1	345	2	+1	426	2	+1
103	1	+1	185	2	−1	263	1	+1	346	6	−1	427	6	+1
105	2	+1	186	2	+1	265	2	−1	347	1	+1	429	2	+1
106	2	−1	187	2	+1	266	2	+1	349	1	−1	430	2	+1
107	1	+1	190	2	+1	267	2	+1	353	1	−1	431	1	+1
109	1	−1	191	1	+1	269	1	−1	354	2	+1	433	1	−1
110	2	+1	193	1	−1	271	1	+1	355	2	+1	434	4	+1
111	2	+1	194	2	+1	273	2	+1	357	2	+1	435	4	+1
113	1	−1	195	4	+1	274	4	−1	358	1	+1	437	1	+1
114	2	+1	197	1	−1	277	1	−1	359	3	+1	438	4	+1
115	2	+1	199	1	+1	278	1	+1	362	2	−1	439	5	+1
118	1	+1	201	1	+1	281	1	−1	365	2	−1	442	8	−1
119	2	+1	202	2	−1	282	2	+1	366	2	+1	443	3	+1
122	2	−1	203	2	+1	283	1	+1	367	1	+1	445	4	−1
123	2	+1	205	2	+1	285	2	+1	370	4	−1	446	1	+1
127	1	+1	206	1	+1	286	2	+1	371	2	+1	447	2	+1
129	1	+1	209	1	+1	287	2	+1	373	1	−1	449	1	−1
130	4	−1	210	4	+1	290	4	−1	374	2	+1	451	2	+1
131	1	+1	211	1	+1	291	4	+1	377	2	+1	453	1	+1
133	1	+1	213	1	+1	293	1	−1	379	1	+1	454	1	+1
134	1	+1	214	1	+1	295	2	+1	381	1	+1	455	4	+1
137	1	−1	215	2	+1	298	2	−1	382	1	+1	457	1	−1
138	2	+1	217	1	+1	299	2	+1	383	1	+1	458	2	−1
139	1	+1	218	2	−1	301	1	+1	385	2	+1	461	1	−1
141	1	+1	219	4	+1	302	1	+1	386	2	+1	462	4	+1
142	3	+1	221	2	+1	303	2	+1	389	1	−1	463	1	+1
143	2	+1	222	2	+1	305	2	+1	390	4	+1	465	2	+1
145	4	−1	223	3	+1	307	1	+1	391	2	+1	466	2	+1
146	2	+1	226	8	−1	309	1	+1	393	1	+1	467	1	+1
149	1	−1	227	1	+1	310	2	+1	394	2	−1	469	3	+1
151	1	+1	229	3	−1	311	1	+1	395	2	+1	470	2	+1
154	2	+1	230	2	+1	313	1	−1	397	1	−1	471	2	+1
155	2	+1	231	4	+1	314	2	−1	398	1	+1	473	3	+1
157	1	−1	233	1	−1	317	1	−1	399	8	+1	474	2	+1
158	1	+1	235	6	+1	318	2	+1	401	5	−1	478	1	+1
159	2	+1	237	1	+1	319	2	+1	402	2	+1	479	1	+1
161	1	+1	238	2	+1	321	3	+1	403	2	+1	481	2	−1
163	1	+1	239	1	+1	322	4	+1	406	2	+1	482	2	+1
165	2	+1	241	1	−1	323	4	+1	407	2	+1	483	4	+1
166	1	+1	246	2	+1	326	3	+1	409	1	−1	485	2	−1
167	1	+1	247	2	+1	327	2	+1	410	4	+1	487	1	+1
170	4	−1	249	1	+1	329	1	+1	411	2	+1	489	1	+1
173	1	−1	251	1	+1	330	4	+1	413	1	+1	491	1	+1
174	2	+1	253	1	+1	331	1	+1	415	2	+1	493	2	−1
177	1	+1	254	3	+1	334	1	+1	417	1	+1	494	2	+1
178	2	+1	255	4	+1	335	2	+1	418	2	+1	497	1	+1
179	1	+1	257	3	−1	337	1	−1	419	1	+1	498	2	+1
181	1	−1	258	2	+1	339	2	+1	421	1	−1	499	5	+1

ТАБЛИЦА 3

Число h классов дивизоров вещественных квадратичных полей $\mathbb{Q}(\sqrt{d})$, d свободно от квадратов, $2 \leqslant d < 150\,000$.

В таблице приведены все встречающиеся значения h для всех 91 189 вещественных квадратичных полей $\mathbb{Q}(\sqrt{d})$ с d в указанных пределах ($d = 2, 3, \ldots, 149\,999$) [147]. В колонке справа ($f(h)$) указано, сколько раз данное h встречается для всех $d < 150\,000$. Наконец, в третьей колонке приведено наименьшее значение d для данного h.

h	$f(h)$	d	h	$f(h)$	d	h	$f(h)$	d
1	20 574	2	28	324	5 626	55	1	106 537
2	26 427	10	29	16	49 281	56	38	39 999
3	2 677	79	30	113	11 665	57	2	41 617
4	18 573	82	31	4	97 753	58	7	27 226
5	943	401	32	397	15 130	60	18	78 745
6	3 453	235	33	11	55 339	61	1	126 499
7	462	577	34	47	19 882	62	3	68 179
8	6 898	226	35	8	25 601	63	1	57 601
9	311	1 129	36	165	18 226	64	23	71 290
10	1 237	1 111	37	7	24 337	66	3	87 271
11	176	1 297	38	33	19 834	68	12	53 362
12	2 434	730	39	6	41 614	70	5	56 011
13	124	4 759	40	179	16 899	72	11	45 511
14	563	1 534	41	1	55 966	74	1	38 026
15	115	9 871	42	30	47 959	76	7	93 619
16	1 970	2 305	43	3	14 401	78	1	136 159
17	62	7 054	44	82	11 026	80	3	94 546
18	385	4 954	45	7	32 401	84	3	77 779
19	48	15 409	46	14	49 321	86	2	110 926
20	788	3 601	47	1	78 401	87	2	90 001
21	43	7 057	48	92	21 610	88	3	56 170
22	163	4 762	49	1	70 969	94	2	99 226
23	20	23 593	50	8	54 769	96	4	50 626
24	838	9 634	51	1	69 697	100	2	131 770
25	30	24 859	52	28	23 410	108	1	140 626
26	110	13 321	53	1	69 694	110	1	125 434
27	20	8 761	54	8	49 834	116	1	116 554

Замечание 1. Всего имеется 303 простых числа p, меньших 2000 (включая $p = 2$). Из них для двадцати шести простых чисел:

$p =$ 79, 223, 229, 257, 359, 443, 659, 733, 761, 839,
1091, 1171, 1223, 1229, 1367, 1373, 1489, 1523, 1567,
1627, 1787, 1811, 1847, 1901, 1907, 1987

— число h поля $\mathbb{Q}(\sqrt{p})$ равно 3. Для семи значений:

$p =$ 401, 439, 499, 727, 1093, 1327, 1429

— число h равно 5 и для четырех значений:

$p =$ 577, 1009, 1087, 1601

— оно равно 7. Одно поле при $p = 1129$ имеет $h = 9$ (с циклической группой классов дивизоров), и одно поле при $p = 1297$ имеет $h = 11$. Для всех

остальных 264 простых чисел $p < 2000$ число классов дивизоров поля $\mathbb{Q}(\sqrt{p})$ равно 1 (см. [83]).

Замечание 2. Из десяти тысяч квадратичных полей $\mathbb{Q}(\sqrt{p})$, p — простое, $p \equiv 1 \pmod 4$, $p \leqslant 225\,217$, только семь полей имеют нециклическую группу классов дивизоров [92]. Для этих семи полей p равно

32 009, 62 501, 114 889, 142 097, 151 141, 153 949, 220 217

и для всех них группа классов (порядка 9) имеет инварианты (3, 3).

Замечание 3. Имеются примеры полей $\mathbb{Q}(\sqrt{p})$ с простым p, $p \equiv 1 \pmod 4$, когда группа G классов дивизоров имеет инварианты другого типа [92], [125]:

p	1 129 841	1 510 889	1 777 441	2 068 117	24 137 573
G	(5,5)	(5,5)	(15,5)	(7,7)	(39,3)

Группа классов дивизоров поля $\mathbb{Q}(\sqrt{3 \cdot 14\,935\,391})$ имеет инварианты (3, 3, 3), см. [126].

Замечание 4. С. Курода [93] вычислил таблицы значений числа $h = h(p)$ классов дивизоров полей $\mathbb{Q}(\sqrt{p})$, $p \equiv 1 \pmod 4$, для всех простых $p \leqslant 2\,776\,817$. Всего имеется 100 811 таких полей. Из них только 22 528 полей имеют $h(p) > 1$ [93]. Таким образом, доля одноклассных полей на указанном промежутке среди полей $\mathbb{Q}(\sqrt{p})$, $p \equiv 1 \pmod 4$, составляет 77,65%. (Отметим, что для первых десяти тысяч простых $p \equiv 1 \pmod 4$, т. е. для $p \leqslant 225\,217$, число одноклассных полей $\mathbb{Q}(\sqrt{p})$ равно 7954, так что доля одноклассных полей с увеличением промежутка несколько уменьшилась.)

Замечание 5. Данные таблицы 3 и предшествующего замечания показывают, что среди вещественных квадратичных полей имеется довольно много одноклассных. Однако мы не знаем, будет ли их число бесконечным. В п. 2 § 7 гл. III мы отмечали, что вообще до сих пор неизвестно, конечно или бесконечно число одноклассных полей алгебраических чисел. Одноклассные поля часто встречаются и среди кубических полей (см. таблицы 8 и 9). Для более высоких степеней ввиду трудностей, связанных с большим объемом вычислений, у нас весьма мало сведений о полях с $h = 1$. В связи с этим интересен пример мнимого одноклассного поля степени 480, приведенный в работе [155]. Стоит отметить также, что согласно работе [158] для любого простого числа p существует бесконечно много полей алгебраических чисел, группа классов дивизоров которых имеет p-примарную компоненту, изоморфную наперед заданной конечной абелевой p-группе. В частности, имеется бесконечно много полей, для которых число классов h не делится на произвольное фиксированное простое число p.

Замечание 6. В отличие от работы [83], вычисление h в [147] основано на формуле $h = \sqrt{D}L(1, \chi)/(2 \ln \varepsilon)$, полученной нами в п. 1 § 4 гл. V.

ТАБЛИЦА 4

Число h классов дивизоров мнимых квадратичных полей $\mathbb{Q}(\sqrt{-a})$, a свободно от квадратов, $1 \leqslant a < 500$.

a	h	a	h	a	h	a	h	a	h	a	h	a	h
1	1	71	7	143	10	215	14	287	14	365	20	434	24
2	1	73	4	145	8	217	8	290	20	366	12	435	4
3	1	74	10	146	16	218	10	291	4	367	9	437	20
5	2	77	8	149	14	219	4	293	18	370	12	438	8
6	2	78	4	151	7	221	16	295	8	371	8	439	15
7	1	79	5	154	8	222	12	298	6	373	10	442	8
10	2	82	4	155	4	223	7	299	8	374	28	443	5
11	1	83	3	157	6	226	8	301	8	377	16	445	8
13	2	85	4	158	8	227	5	302	12	379	3	446	32
14	4	86	10	159	10	229	10	303	10	381	20	447	14
15	2	87	6	161	16	230	20	305	16	382	8	449	20
17	4	89	12	163	1	231	12	307	3	383	17	451	6
19	1	91	2	165	8	233	12	309	12	385	8	453	12
21	4	93	4	166	10	235	2	310	8	386	20	454	14
22	2	94	8	167	11	237	12	311	19	389	22	455	20
23	3	95	8	170	12	238	8	313	8	390	16	457	8
26	6	97	4	173	14	239	15	314	26	391	14	458	26
29	6	101	14	174	12	241	12	317	10	393	12	461	30
30	4	102	4	177	4	246	12	318	12	394	10	462	8
31	3	103	5	178	8	247	6	319	10	395	8	463	7
33	4	105	8	179	5	249	12	321	20	397	6	465	16
34	4	106	6	181	10	251	7	322	8	398	20	466	8
35	2	107	3	182	12	253	4	323	4	399	16	467	7
37	2	109	6	183	8	254	16	326	22	401	20	469	16
38	6	110	12	185	16	255	12	327	12	402	16	470	20
39	4	111	8	186	12	257	16	329	24	403	2	471	16
41	8	113	8	187	2	258	8	330	8	406	16	473	12
42	4	114	8	190	4	259	4	331	3	407	16	474	20
43	1	115	2	191	13	262	6	334	12	409	16	478	8
46	4	118	6	193	4	263	13	335	18	410	16	479	25
47	5	119	10	194	20	265	8	337	8	411	6	481	16
51	2	122	10	195	4	266	20	339	6	413	20	482	20
53	6	123	2	197	10	267	2	341	28	415	10	483	4
55	4	127	5	199	9	269	22	345	8	417	12	485	20
57	4	129	12	201	12	271	11	346	10	418	8	487	7
58	2	130	4	202	6	273	8	347	5	419	9	489	20
59	3	131	5	203	4	274	12	349	14	421	10	491	9
61	6	133	4	205	8	277	6	353	16	422	10	493	12
62	8	134	14	206	20	278	14	354	16	426	24	494	28
65	8	137	8	209	20	281	20	355	4	427	2	497	24
66	8	138	8	210	8	282	8	357	8	429	16	498	8
67	1	139	3	211	3	283	3	358	6	430	12	499	3
69	8	141	8	213	8	285	16	359	19	431	21		
70	4	142	4	214	6	286	12	362	18	433	12		

ТАБЛИЦА 5

Число h классов дивизоров мнимых квадратичных полей $\mathbb{Q}(\sqrt{-p})$ для простых p, $500 < p < 2000$.

p	h	p	h	p	h	p	h	p	h	p	h
503	21	739	5	983	27	1229	38	1487	37	1741	26
509	30	743	21	991	17	1231	27	1489	20	1747	5
521	32	751	15	997	14	1237	14	1493	22	1753	20
523	5	757	10	1009	20	1249	32	1499	13	1759	27
541	10	761	40	1013	26	1259	15	1511	49	1777	24
547	3	769	20	1019	13	1277	34	1523	7	1783	17
557	18	773	26	1021	22	1279	23	1531	11	1787	7
563	9	787	5	1031	35	1283	11	1543	19	1789	26
569	32	797	30	1033	12	1289	36	1549	18	1801	28
571	5	809	32	1039	23	1291	9	1553	40	1811	23
577	8	811	7	1049	44	1297	12	1559	51	1823	45
587	7	821	30	1051	5	1301	50	1567	15	1831	19
593	24	823	9	1061	26	1303	11	1571	17	1847	43
599	25	827	7	1063	19	1307	11	1579	9	1861	38
601	20	829	22	1069	30	1319	45	1583	33	1867	5
607	13	839	33	1087	9	1321	24	1597	14	1871	45
613	10	853	10	1091	17	1327	15	1601	56	1873	12
617	12	857	32	1093	10	1361	60	1607	27	1877	34
619	5	859	7	1097	36	1367	25	1609	28	1879	27
631	13	863	21	1103	23	1373	18	1613	42	1889	72
641	28	877	10	1109	50	1381	26	1619	15	1901	42
643	3	881	40	1117	14	1399	27	1621	18	1907	13
647	23	883	3	1123	5	1409	36	1627	7	1913	36
653	14	887	29	1129	16	1423	9	1637	38	1931	21
659	11	907	3	1151	41	1427	15	1657	16	1933	18
661	18	911	31	1153	16	1429	22	1663	17	1949	70
673	12	919	19	1163	7	1433	36	1667	13	1951	33
677	30	929	36	1171	7	1439	39	1669	26	1973	42
683	5	937	20	1181	46	1447	23	1693	22	1979	23
691	5	941	46	1187	9	1451	13	1697	28	1987	7
701	34	947	5	1193	36	1453	14	1699	11	1993	24
709	10	953	32	1201	16	1459	11	1709	42	1997	42
719	31	967	11	1213	10	1471	23	1721	52	1999	27
727	13	971	15	1217	32	1481	52	1723	5		
733	14	977	20	1223	35	1483	7	1733	34		

ТАБЛИЦА 6

«Нетривиальные» группы классов дивизоров мнимых квадратичных полей $\mathbb{Q}(\sqrt{-m})$ для $0 < m < 24\,000$ (см. [141]).

Группа G классов дивизоров поля $\mathbb{Q}(\sqrt{-m})$ называется «тривиальной», если ее инварианты (среди которых каждый следующий является делителем предыдущего) имеют вид $a, 2, \ldots, 2$. В противном случае G называется «нетривиальной». «Тривиальная» группа однозначно определяется своим порядком и числом простых делителей дискриминанта поля $\mathbb{Q}(\sqrt{-m})$. В таблице для поля $\mathbb{Q}(\sqrt{-m})$ с «нетривиальной» группой G в колонке справа указаны инварианты группы G. Все поля $\mathbb{Q}(\sqrt{-m})$ с $0 < m < 24\,000$, не приведенные в таблице, имеют «тривиальные» группы классов дивизоров.

m	G	m	G	m	G	m	G
974	12, 3	5 614	8, 4	8 366	28, 4	10 295	32, 4
1 513	4, 4	5 703	18, 3	8 446	12, 4	10 366	16, 4
1 582	4, 4	5 795	8, 4	8 522	30, 3	10 414	20, 4
1 590	4, 4, 2	5 857	12, 3	8 555	8, 4	10 549	8, 4, 2
1 598	8, 4	5 910	4, 4, 2	8 633	16, 4	10 605	4, 4, 2, 2
1 886	16, 4	5 986	8, 4	8 638	8, 4	10 718	16, 4
1 918	4, 4	6 001	8, 4	8 671	16, 4	10 759	12, 4
2 329	8, 4	6 014	24, 4	8 701	8, 4, 2	10 790	12, 4, 2
2 379	4, 4	6 085	6, 6	8 710	4, 4, 2	10 798	12, 3
2 437	6, 3	6 123	4, 4	8 738	16, 4	10 803	4, 4
2 542	4, 4	6 221	42, 3	8 751	24, 3	10 961	32, 4
2 702	12, 4	6 226	12, 6	8 790	8, 4, 2	11 001	6, 6, 2
2 993	12, 4	6 286	12, 4	8 878	8, 4	11 199	20, 5
3 026	12, 4	6 355	4, 4	8 942	24, 4	11 326	24, 4
3 262	8, 4	6 398	16, 4	8 974	16, 4	11 534	44, 4
3 299	9, 3	6 402	4, 4, 2	9 069	12, 6	11 651	18, 3
3 358	8, 4	6 494	24, 4	9 118	8, 4	11 713	4, 4, 2
3 502	4, 4	6 497	8, 8	9 214	16, 4	11 822	20, 4
3 886	6, 6	6 583	12, 3	9 266	36, 4	11 966	32, 4
3 934	8, 4	6 690	6, 6, 2	9 385	12, 6	12 002	20, 4
4 027	3, 3	6 789	6, 6, 2	9 422	24, 4	12 013	6, 6
4 318	8, 4	6 910	6, 6	9 497	24, 3	12 067	6, 3
4 369	12, 4	6 914	36, 3	9 503	20, 4	12 095	32, 4
4 486	10, 5	6 953	16, 4	9 510	8, 4, 2	12 118	6, 6
4 633	8, 4	7 006	20, 4	9 554	40, 4	12 131	12, 3
4 658	16, 4	7 059	8, 4	9 574	18, 3	12 206	48, 4
4 718	16, 4	7 081	16, 4	9 595	4, 4	12 207	20, 4
4 777	8, 4	7 361	28, 4	9 673	12, 4	12 282	6, 6, 2
4 810	4, 4, 2	7 582	8, 4	9 809	32, 4	12 394	18, 3
4 895	16, 4	7 585	4, 4, 2	9 881	28, 4	12 451	5, 5
5 037	4, 4, 2	7 769	24, 4	9 934	12, 3	12 453	6, 6, 2
5 069	12, 6	7 966	8, 8	9 955	4, 4	12 481	12, 6
5 134	16, 4	7 977	6, 6	10 001	40, 4	12 505	8, 4, 2
5 142	6, 6	8 103	12, 4	10 015	18, 3	12 595	4, 4
5 190	8, 4, 2	8 126	40, 4	10 074	8, 4, 2	12 638	32, 4
5 306	12, 6	8 242	6, 6	10 081	12, 4	12 710	16, 4, 2
5 417	24, 3	8 322	8, 4, 2	10 173	6, 6	12 837	6, 6, 2

Продолжение табл. 6

m	G	m	G	m	G	m	G
12 937	8, 4	15 929	32, 4	18 555	6, 6	21 418	18, 3
12 994	12, 4	15 934	16, 4	18 649	16, 4	21 449	24, 6
13 022	16, 4	16 049	30, 6	18 721	32, 4	21 454	24, 4
13 073	16, 4	16 201	20, 4	18 761	32, 4	21 571	8, 4
13 143	16, 4	16 238	12, 12	18 814	20, 4	21 605	24, 4, 2
13 317	8, 4, 2	16 301	78, 3	18 922	10, 5	21 755	16, 4
13 342	12, 4	16 441	28, 4	19 187	12, 3	21 895	24, 4
13 359	24, 4	16 446	10, 10	19 286	42, 3	21 922	20, 4
13 398	4, 4, 2, 2	16 582	10, 5	19 346	44, 4	21 930	6, 6, 2, 2
13 677	8, 4, 2	16 609	24, 4	19 427	9, 3	21 998	20, 4
13 678	8, 4	16 627	6, 3	19 545	6, 6, 2	22 055	40, 4
13 727	28, 4	16 710	8, 4, 2	19 590	12, 4, 2	22 127	16, 8
13 817	28, 4	16 769	28, 4	19 618	12, 4	22 222	12, 4
13 829	54, 3	16 782	10, 10	19 651	6, 3	22 321	8, 8, 2
13 906	16, 4	16 814	48, 4	19 677	6, 6, 2	22 395	6, 6
14 033	36, 3	16 870	6, 6, 2	19 679	54, 3	22 443	6, 3
14 062	12, 4	16 887	24, 4	19 726	20, 4	22 481	60, 3
14 126	36, 4	16 895	24, 4	19 762	8, 8	22 654	16, 4
14 155	4, 4	17 131	6, 3	19 919	45, 3	22 711	42, 3
14 162	20, 4	17 146	42, 3	19 947	4, 4	22 717	10, 5
14 334	18, 6	17 266	16, 4	19 981	12, 4, 2	22 763	8, 4
14 446	20, 4	17 282	36, 3	19 982	28, 4	22 862	12, 4, 2
14 462	24, 4	17 399	54, 3	20 002	12, 4	22 873	12, 4
14 473	12, 4	17 402	12, 4, 2	20 091	8, 4	22 965	12, 6, 2
14 547	4, 4	17 422	12, 4	20 129	60, 3	23 095	16, 4
14 606	10, 10	17 427	4, 4	20 155	4, 4	23 137	16, 4
14 637	4, 4, 2, 2	17 561	12, 12	20 162	36, 4	23 142	4, 4, 2, 2
14 722	8, 4	17 574	12, 4, 2	20 310	12, 4, 2	23 155	8, 4
14 730	6, 6, 2	17 723	18, 3	20 366	44, 4	23 165	12, 6, 2
14 795	8, 4	17 751	28, 4	20 398	8, 4, 2	23 178	12, 6
15 049	12, 6	17 753	24, 4	20 445	8, 4, 2, 2	23 190	16, 4, 2
15 326	48, 4	18 021	10, 10	20 654	44, 4	23 329	24, 4
15 389	20, 10	18 046	24, 4	20 658	8, 4, 2	23 377	16, 4
15 538	16, 4	18 158	40, 4	20 734	24, 4	23 439	36, 4
15 549	12, 4, 2	18 278	12, 4, 2	20 737	16, 4	23 585	16, 4, 2
15 655	24, 4	18 285	4, 4, 2, 2	21 018	6, 6, 2	23 605	12, 6
15 658	10, 5	18 286	16, 4	21 098	16, 4, 2	23 683	6, 3
15 742	16, 4	18 362	30, 3	21 190	8, 4, 2	23 862	6, 6, 2
15 805	8, 4, 2	18 409	28, 4	21 233	28, 4	23 871	24, 4
15 806	44, 4	18 458	18, 6	21 243	8, 4	23 910	8, 8, 2
15 910	8, 4, 2	18 542	28, 4	21 395	16, 4	23 953	24, 4

Замечание. К настоящему времени известны многочисленные примеры мнимых квадратичных полей, для которых группа классов дивизоров G имеет более двух инвариантов, делящихся на одно и то же нечетное простое число. Некоторые из них можно найти в работах [74], [111], [120], [126], [127], [151].

Приведем отдельные примеры. Для не простых m даны их разложения на простые сомножители. Справа указаны (примарные) инварианты группы классов G поля $\mathbb{Q}(\sqrt{-m})$.

m	G
4724490703	(3, 3, 3, 3, 5, 53)
1571310110659	(3, 3, 3, 3, 5, 11, 43)
699234050083	(9, 3, 3, 3, 19, 25)
282910884511	(27, 3, 3, 3, 631)
41·1827827279	(2, 9, 9, 3, 3, 103)
2·5·7·17·19·1034639	(2, 2, 2, 2, 2, 3, 3, 3, 3, 25)
2·23·31·43·131·18131	(8, 4, 2, 2, 2, 3, 3, 3, 3, 7)
29·59·32 413	(8, 4, 3, 3, 3)
613·88 799	(2, 3, 3, 3, 5, 5)
11·17·23·31·73	(8, 2, 2, 2, 2, 3, 3, 3)
14 935 391	(81, 3, 3, 5)
2·3·47·3943	(8, 2, 2, 3, 3, 3)
131·61 699 320 931	(2, 2, 3, 3, 3, 19, 499)
167·12 409·42 169	(8, 2, 3, 3, 3, 3, 181)
83 309 629 817	(4, 9, 3, 3, 3, 181)
222 637 549 223	(3, 5, 5, 5, 19, 61)
1171·1439·153 441 403	(4, 2, 5, 5, 5, 5, 2957)

ТАБЛИЦА 7

Дискриминанты известных порядков мнимых квадратичных полей, для которых каждый род принадлежащих им модулей состоит из одного класса

I. Дискриминанты максимальных порядков (шестьдесят пять значений):

— 3	— 43	—148	—340	— 595	—1320
— 4	— 51	—163	—372	— 627	—1380
— 7	— 52	—168	—403	— 660	—1428
— 8	— 67	—187	—408	— 708	—1435
—11	— 84	—195	—420	— 715	—1540
—15	— 88	—228	—427	— 760	—1848
—19	— 91	—232	—435	— 795	—1995
—20	—115	—235	—483	— 840	—3003
—24	—120	—267	—520	—1012	—3315
—35	—123	—280	—532	—1092	—5460
—40	—132	—312	—555	—1155	

II. Дискриминанты немаксимальных порядков (тридцать шесть значений):

$-3\cdot2^2$	$-4\cdot2^2$	$-7\cdot8^2$	$-15\cdot4^2$	$-88\cdot2^2$	$-408\cdot2^2$
$-3\cdot3^2$	$-4\cdot3^2$	$-8\cdot2^2$	$-15\cdot8^2$	$-120\cdot2^2$	$-520\cdot2^2$
$-3\cdot4^2$	$-4\cdot4^2$	$-8\cdot3^2$	$-20\cdot3^2$	$-168\cdot2^2$	$-760\cdot2^2$
$-3\cdot5^2$	$-4\cdot5^2$	$-8\cdot6^2$	$-24\cdot2^2$	$-232\cdot2^2$	$-840\cdot2^2$
$-3\cdot7^2$	$-7\cdot2^2$	$-11\cdot3^2$	$-35\cdot3^2$	$-280\cdot2^2$	$-1320\cdot2^2$
$-3\cdot8^2$	$-7\cdot4^2$	$-15\cdot2^2$	$-40\cdot2^2$	$-312\cdot2^2$	$-1848\cdot2^2$

Удобные числа Эйлера:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848.

ТАБЛИЦА 8

Число h классов дивизоров вполне вещественных кубических полей дискриминанта $< 100\,000$ (см. [103]).

Кубическое поле $\mathbb{Q}(\theta)$ называется вполне вещественным, если для него $s = 3$, $t = 0$, т. е. если все его изоморфизмы в поле комплексных чисел вещественны. Если минимальный многочлен числа 0 раскладывается в $\mathbb{Q}(\theta)$ целиком на линейные множители, то $\mathbb{Q}(\theta)$ называется циклическим. Если же это не так, то мы имеем тройку сопряженных кубических полей, и такая тройка засчитывается в таблице только один раз. Всего имеется 4804 вполне вещественных кубических поля с дискриминантами $< 100\,000$. Среди них 51 поле — циклическое. В таблице для каждого из приведенных в ней интервалов указано число всех вполне вещественных кубических полей с дискриминантами из этого интервала и число полей с данным h (в пределах таблицы $h \leqslant 9$).

Границы для дискриминанта	Общее число полей	Число полей с данным h								
		1	2	3	4	5	6	7	8	9
1—10 000	382	358	9	14	1	—	—	—	—	—
10 001—20 000	450	408	20	20	2	—	—	—	—	—
20 001—30 000	467	415	26	21	2	2	—	1	—	—
30 001—40 000	479	425	24	24	2	4	—	—	—	—
40 001—50 000	485	418	29	33	3	1	1	—	—	—
50 001—60 000	500	442	27	23	1	1	2	3	1	—
60 001—70 000	490	417	32	33	3	4	—	—	—	1
70 001—80 000	509	436	35	30	3	3	2	—	—	—
80 001—90 000	514	432	44	33	2	2	—	1	—	—
90 001—100 000	528	442	42	37	1	2	2	2	—	—

Замечание 1. Некоторые из дискриминантов $< 100\,000$ имеют по два, три и четыре вполне вещественных кубических поля (не сопряженных между собой). В каждом из десяти интервалов таблицы содержится

16, 8, 5, 3, 4, 2, 4, 4, 1, 4

циклических кубических поля соответственно.

Замечание 2. В статье [125] указано одно семейство циклических кубических полей, среди которых для дискриминантов 313^2, $15\,013^2$, $88\,513^2$, $110\,563^2$ число классов дивизоров h равно 7, 127, 511, 553 соответственно.

ТАБЛИЦА 9

Число классов h для чисто кубических полей $\mathbb{Q}\left(\sqrt[3]{m}\right)$, $1 < m < 10^4$ ($m = ab^2$, $a > b$, a и b свободны от квадратов).

В таблице приведены все значения h, встречающиеся для 8122 чисто кубических полей $\mathbb{Q}\left(\sqrt[3]{m}\right)$ с m в указанных пределах. В колонке справа ($f(h)$) указано, сколько раз это h встречается для всех $m < 10\,000$. Наконец, в третьей колонке приведено наименьшее значение m для данного h [60].

h	$f(h)$	m	h	$f(h)$	m	h	$f(h)$	m
1	596	2	6	952	39	11	7	2348
2	285	11	7	26	235	12	359	43
3	1847	7	8	32	141	13	5	1049
4	87	113	9	1258	70	14	7	514
5	37	263	10	9	303	15	97	267

Продолжение табл. 9

h	$f(h)$	m	h	$f(h)$	m	h	$f(h)$	m
16	9	681						
17	1	8511	80	1	4799	243	6	3913
18	674	65	81	77	1298	252	3	2786
19	2	667	84	9	1737	254	1	8002
20	6	761	87	2	4103	255	1	2751
21	51	213	90	27	970	264	1	7297
22	4	281	93	1	2748	270	4	4593
24	96	229	96	5	4307	276	1	4093
26	1	3403	99	8	995	279	1	5149
27	385	182	102	4	2374	288	1	5826
28	6	509	105	4	2737	297	3	6487
30	38	524	108	87	511	300	1	9931
32	3	2399	111	2	5737	306	2	4694
33	19	1618	117	4	5215	312	1	9938
34	1	1719	120	10	1727	315	2	5359
36	262	322	126	23	1141	324	10	2198
37	2	5545	127	1	2741	336	1	8005
39	7	2597	128	1	5987	342	1	3907
40	2	2733	129	1	2946	351	3	3605
41	1	6659	132	3	3045	360	1	7985
42	21	515	135	11	1015	369	1	5829
44	2	4817	136	1	3209	372	1	7133
45	68	763	141	1	6991	378	3	3155
48	30	561	144	17	1730	390	1	9591
49	1	8171	150	1	8431	396	2	7997
51	4	1037	153	2	3661	405	6	7970
52	1	4793	154	1	9041	432	4	6878
54	172	614	156	2	7461	435	1	8006
56	2	857	162	36	813	459	1	9254
57	5	1541	168	2	2747	480	1	7415
58	1	6814	171	1	9198	486	4	6162
60	14	997	175	1	5711	576	1	4291
63	29	1005	180	12	2702	585	1	9262
64	1	9749	186	1	4099	612	1	7995
66	5	3482	189	7	6430	630	1	9933
68	1	9521	192	2	7925	648	1	4097
69	4	3590	198	7	3374	696	1	5503
70	1	3467	201	2	2723	747	1	2743
71	1	3539	216	17	2765	756	1	8030
72	90	741	222	1	5823	972	1	9709
74	1	3581	225	3	5362	1017	1	8615
75	3	1657	230	1	4451	1170	1	7999
78	9	1801	240	2	5835	1296	1	8827

Замечание 1. В пределах таблицы для 7409 полей h равно $2^{\alpha}3^{\beta}$ и для остальных 713 полей h делится на простое число $\geqslant 5$. Для значений m в пределах каждой тысячи число полей $\mathbb{Q}\left(\sqrt[3]{m}\right)$ с $h = 1$ равно соответственно

98, 64, 56, 61, 65, 55, 49, 54, 44, 50.

Число полей $\mathbb{Q}\left(\sqrt[3]{m}\right)$, $m < 10\,000$, для которых h делится на

2, 3, 5, 7, 11, 13, 17, 19,

равно соответственно

$$3510,\quad 6954,\quad 369,\quad 202,\quad 62,\quad 36,\quad 19,\quad 9.$$

Замечание 2. Число классов дивизоров поля $\mathbb{Q}\left(\sqrt[3]{m}\right)$ при малых значениях m можно найти в [9], [124]. Число h для чисто кубических полей рассматривается также в [125], [146], [148], [149], [150].

Замечание 3. Если q — простое число и $q \equiv 2 \pmod 3$, то число классов дивизоров поля $\mathbb{Q}\left(\sqrt[3]{-q}\right)$ не делится на 3. Обозначим через $n(x)$ число простых чисел q, которые сравнимы с 2 по модулю 3 и которые не превосходят x, и через $g(x)$ — число тех $q \leqslant x$, для которых число классов поля $\mathbb{Q}\left(\sqrt[3]{-q}\right)$ равно 1. Отношение $\dfrac{g(x)}{n(x)}$ имеет поразительную тенденцию к «постоянству» (см. [146] и [148]). В пределах проведенных вычислений это отношение вплоть до $x = 101\,000$ колеблется в небольших пределах, принимая значения вблизи 0,47 и 0,48. Аналогичный феномен проявляется еще ярче (см. [150]), если ограничиться полями $\mathbb{Q}\left(\sqrt[3]{-r}\right)$ для простых $r \equiv 17 \pmod{18}$ (в этом классе полей значительно реже встречаются четные h). Пусть $n(x)$ и $g(x)$ имеют тот же смысл, что и выше, но применительно к простым r, которые $\equiv 17 \pmod{18}$. В этом случае в промежутке $2000 < x < 200\,000$ отношение $\dfrac{g(x)}{n(x)}$ принимает значения около 0,61, достигая локального минимума 0,603 вблизи $x = 38\,000$ и локального максимума 0,627 вблизи $x = 70\,000$. К сожалению, в обоих случаях у нас нет никаких аргументов, которые подкрепили бы предположение, что отмеченная стабильность отношения $\dfrac{g(x)}{n(x)}$ сохранится для сколь угодно больших q или r.

Отметим попутно, что поле $\mathbb{Q}\left(\sqrt[3]{2\,000\,145\,629}\right)$ одноклассно [149].

ТАБЛИЦА 10

Множитель $h^* = h^*(l)$ числа классов дивизоров l-кругового поля для простых $l < 300$.

В таблице для h^* указано разложение на простые множители, кроме двух случаев $l = 233$ и $l = 269$; числа, отмеченные звездочкой, составные, однако их разложение на простые сомножители неизвестно (см. [112], [97]).

l	h^*	l	h^*	l	h^*
3	1	29	2·2·2	61	41·1861
5	1	31	3·3	67	67·12739
7	1	37	37	71	7·7·79241
11	1	41	11·11	73	89·134353
13	1	43	211	79	5·53·377911
17	1	47	5·139	83	3·279405653
19	1	53	4889	89	113·118401449
23	3	59	3·59·233	97	577·3457·206209

Продолжение табл. 10

l	h^*
101	5·5·5·5·5·101·601·18701
103	5·103·1021·17247691
107	3·743·9859·2886593
109	17·1009·9431866153
113	2·2·2·17·11853470598257
127	5·13·43·547·883·3079·626599
131	3·3·3·5·5·53·131·1301·4673706701
137	17·17·47737·46890540621121
139	3·3·47·47·277·277·967·1188961909
149	3·3·149·5129663383200408054 61
151	7·11·11·281·25951·1207501·312885301
157	5·13·13·157·157·1093·1873·418861·3148601
163	2·2·181·23167·365473·441845817162679
167	11·499·5123189985848229035947419
173	5·20297·231169·72571729362851870621
179	5·1069·1445866739233494828676463512 1
181	5·5·5·37·41·61·1321·2521·548843578258927770 1
191	11·13·51263·612771091·36733950669733713761
193	6529·15361·29761·91969·10369729·19026280449
197	2·2·2·5·1877·7841·939830268487086665622561 1549
199	3·3·3·3·19·727·25645039·207293548177·3168190412839
211	3·3·7·7·41·71·181·281·281·421·1051·12251·113981701· ·4343510221
223	7·43·17909933575379·11757537731851·3424804483726447
227	5·2939·2939·2939·1692824021974901·13444015915122722869
229	13·17·457·7753·705053·47824141·414153903321692666991589
233	233·1433·10428188106847239128192009224591072712660 41 *
239	2·2·2·2·2·2·3·5·511123·14136487·123373184789· ·2249739998789113695307 9
241	47·47·13921·15601·2359873·126767281·518123008737871423891201
251	7·11·348270001·9631365977251· ·3696311145677554372436636265 01
257	257·20738946049·10229977445639119615612986981834190371496 97
263	13·263·787·385927· ·4187591009556788673281894446299480742601862 83
269	13·40170973189· ·7157703949875286788563837229656316512687317037*
271	11·31·37·271·811·1201·1621·15391·21961·7288651·20238391· ·751928131·666587726641
277	2·2·2·2·17·47·47·829·89977·1371353·4873333·30697273· ·1776834909244716811072486129
281	11·11·17·41·41·401·3235961·64523056921· ·9773431399762339685694610754114060 81
283	3·3·283·2064523·39341481709417· ·5484646647490654799157896194266098076673
293	3·3·293·38901409·52561753·354041533·19844792749· ·7024055669982494626097540798 33

Замечание 1. Первые семь нечетных простых чисел исчерпывают собой все l с $h^*(l) = 1$ (см. [138], [106]). Существует гипотеза [100], что функция $h^*(l)$ строго возрастает для всех простых $l \geqslant 19$. В свое время Куммером было высказано предположение, что $h^*(l)$ при $l \to \infty$

асимптотически выражается формулой

$$h^*(l) \sim 2l\left(\frac{l}{4\pi^2}\right)^{(l-1)/4}.$$

Однако до настоящего времени вопрос о справедливости этого утверждения остается открытым. Доказана лишь следующая более слабая формула

$$\lim_{l\to\infty}\frac{\ln h^*(l)}{l\ln l}=\frac{1}{4},$$

получающаяся из формулы Куммера логарифмированием [54], [129]. Рост функции $h^*(l)$ мажорируется сверху оценкой [100]:

$$h^*(l)<2l\left(\frac{l}{24}\right)^{(l-1)/4}.$$

Замечание 2. В настоящее время известны все m-круговые поля, для которых $h(m)<10^4$. Всего таких полей пятьдесят семь (при перечислениях круговых полей следует исключать значения $m=4k+2$, так как они определяют те же самые круговые поля, что и значения $m=2k+1$). Если $h(m)=1$ (т. е. в максимальном порядке поля деления круга на m частей имеет место однозначность разложения на простые множители), то m равно одному из следующих двадцати девяти значений [106]:

3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21,
24, 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84.

Все m, для которых $2\leqslant h(m)\leqslant 10$, исчерпываются значениями из следующей таблицы [104] (число круговых полей с $h\leqslant 10$ равно $29+15=44$).

$h(m)$	2	3	4	5	6	7	8	9	10
m	39,56	23, 52, 72	120	51.80	Нет	63	29,68	31, 57, 96	55

ТАБЛИЦА 11

Иррегулярные простые числа <8000.

Всего имеется 1006 нечетных простых чисел, меньших 8000. Из них 609 регулярных и 397 иррегулярных. Рядом с иррегулярным простым числом l в соседней колонке справа указаны все номера $2a$ чисел Бернулли B_{2a} ($2\leqslant 2a\leqslant l-3$), числители которых делятся на l. Нумерация чисел Бернулли четная: $B_2=1/6$, $B_4=-1/30$ и т. д. В случае нескольких значений $2a$ (для данного l) они выписаны друг под другом в порядке возрастания. Общее число иррегулярных пар $(l, 2a)$, приведенных в таблице, равно 502 (см. [47] и [86]).

l	$2a$	l	$2a$	l	$2a$	l	$2a$
37	32	233	84	353	186	461	196
59	44	257	164		300	463	130
67	58	263	100	379	100	467	94
101	68	271	84		174		194
103	24	283	20	389	200	491	292
131	22	293	156	401	382		336
149	130	307	88	409	126		338
157	62	311	292	421	240	523	400
	110	347	280	433	366	541	86

Продолжение табл. 11

l	$2a$	l	$2a$	l	$2a$	l	$2a$
547	270	1153	802	1847	954	2557	1464
	486	1193	262		1016	2579	1730
557	222	1201	676		1558	2591	854
577	52	1217	784	1871	1794		2574
587	90		866	1877	1026	2621	1172
	92		1118	1879	1260	2633	1416
593	22	1229	784	1889	242	2647	1172
607	592	1237	874	1901	1722	2657	710
613	522	1279	518	1933	1058	2663	1244
617	20	1283	510		1320	2671	404
	174	1291	206	1951	1656		2394
	338		824	1979	148	2689	926
619	428	1297	202	1987	510	2753	482
631	80		220	1993	912	2767	2528
	226	1301	176	1997	772	2777	1600
647	236	1307	382		1888	2789	1984
	242		852	2003	60		2154
	554	1319	304		600	2791	2554
653	48	1327	466	2017	1204	2833	1832
659	224	1367	234	2039	1300	2857	98
673	408	1381	266	2053	1932	2861	352
	502	1409	358	2087	376	2909	400
677	628	1429	996		1298		950
683	32	1439	574	2099	1230	2927	242
691	12	1483	224	2111	1038	2939	332
	200	1499	94	2137	1624		1102
727	378	1523	1310	2143	1916		2748
751	290	1559	862	2153	1832	2957	138
757	514	1597	842	2213	154		788
761	260	1609	1356	2239	1826	2999	776
773	732	1613	172	2267	2234	3011	1496
797	220	1619	560	2273	876	3023	2020
809	330	1621	980		2166	3049	700
	628	1637	718	2293	2040	3061	2522
811	544	1663	270	2309	1660	3083	1450
821	744		1508		1772	3089	1706
827	102	1669	388	2357	2204	3119	1704
839	66		1086	2371	242	3181	3142
877	868	1721	30		2274	3203	2368
881	162	1733	810	2377	1226	3221	98
887	418		942	2381	2060	3229	1634
929	520	1753	712	2383	842	3257	922
	820	1759	1520		2278	3313	2222
953	156	1777	1192	2389	776	3323	3292
971	166	1787	1606	2411	2126	3329	1378
1061	474	1789	848	2423	290	3391	2232
1091	888		1442		884		2534
1117	794	1811	550	2441	366	3407	2076
1129	348		698		1750		2558
1151	534		1520	2503	1044	3433	1300
	784	1831	1274	2543	2374	3469	1174
	968						

Продолжение табл. 11

l	$2a$	l	$2a$	l	$2a$	l	$2a$
3491	2544	4219	4190	5119	4086	6173	5008
3511	1416	4243	2712	5167	4112		5894
	1724		4146	5179	4732	6217	4186
3517	1836	4259	3580	5189	1102	6247	1492
	2586		3726	5209	644		3474
3529	3490	4261	2068		2928	6257	4272
3533	2314	4339	214	5227	308	6263	3286
	3136	4349	2052	5231	3466		4226
3539	2082	4409	636	5297	4810	6287	4452
	2130		672	5303	4156		5034
3559	344	4421	3768	5309	158	6317	2354
	1592	4451	2896	5351	1948	6329	5102
3581	1466		2978	5399	1482	6337	1956
3583	1922	4457	444	5413	1702	6343	750
3593	360	4493	746	5441	4726		5820
	642	4519	848	5443	1710	6367	1190
3607	1976	4523	456	5477	1150	6373	2838
3613	2082	4561	436	5479	1826		4226
3617	16	4591	2292		4802	6379	218
	2856		3596	5501	666	6421	438
3631	1104	4637	3618	5527	5206	6449	4884
3637	2526	4639	3226	5531	3438		5830
	3202	4657	1578	5557	3196	6451	3236
3671	1580		2416	5569	938	6491	346
3677	2238		4110	5573	2032	6521	236
3697	1884	4663	216	5639	2672	6529	1564
3779	2362		4278	5641	4580	6547	734
3797	1256	4679	3592		5258	6569	1692
3821	3296	4691	3450	5669	2218		1776
3833	1840	4751	3768		2680	6571	1744
	1998	4783	252	5689	348	6577	1312
	3286	4793	2636	5701	2450	6619	1952
3851	216	4813	2620	5783	2200		3170
	404	4861	4678	5791	1258	6659	2950
3853	748	4889	2924	5813	4284		4014
3881	1686	4903	3106	5821	1150	6689	5252
	2138	4909	1462	5839	2308	6701	5484
3917	1490	4943	492	5861	3554	6733	1690
3967	106	4951	1914	5897	2996	6763	4144
3989	1936		2468	5903	3970		6218
4001	534		3890		5000		6230
4003	82	4957	3812	5923	4240	6779	3994
	142	4969	1940	5927	3642	6793	2686
	2610	4973	4208	5939	342	6823	4952
4021	3228	5009	1544		5014	6827	4108
4027	2332		4956	5953	3274	6833	2254
4049	1854	5039	594	6007	912		5144
4051	3548	5077	3092	6011	5870	6857	6676
4073	3620	5081	3016	6037	3396	6863	6406
4129	1784	5099	1378	6043	1226	6949	2432
4157	658	5101	190	6091	702	6971	2010
	2322	5107	4872	6101	2008	6997	1746

Продолжение табл. 11

l	$2a$	l	$2a$	l	$2a$	l	$2a$
7001	4842	7211	898	7537	2264	7817	7346
7039	1454	7213	1436	7547	5644	7823	3298
7057	4154		6930	7559	116	7829	1392
	4972	7229	6236	7591	2620	7853	3494
7069	1478	7309	324	7607	3594	7901	2472
	2570	7321	348	7643	5026		4286
7109	290	7351	1466	7681	368	7907	584
7121	1502	7411	4712	7687	1246	7919	3888
7127	6798	7459	5286		3216	7927	6448
7177	962	7487	2500		6516	7937	3980
7187	3906	7489	4250	7691	2218	7949	2506
7207	1670	7499	3642	7727	950		3436
	5774	7507	6924		3756	7951	4328
						7963	4748

ТАБЛИЦА 12

Иррегулярные простые числа $< 125\,000$, имеющие индекс иррегулярности 4 и 5.

В колонке справа указаны номера $2a$ чисел Бернулли B_{2a} ($2a \leqslant l-3$), числители которых делятся на l. Таблицы 12 и 13 (а также приведенные ниже замечания) извлечены из статьи [142].

l	$2a$				
12 613	308	502	9 400	10 536	
15 737	6 352	7 454	12 486	13 078	
43 189	9 454	14 464	26 380	35 578	
56 263	10 770	21 958	52 530	55 200	
72 337	2 346	15 858	44 354	68 030	
76 289	11 860	25 284	26 406	72 266	
77 783	5 590	52 114	52 246	73 092	
78 233	10 400	32 084	46 620	47 364	64 628
84 067	16 322	43 722	44 246	44 79.	
94 693	11 636	54 754	76 326	80 650	84 726
102 559	6 076	50 092	54 402	66 162	
108 179	9 344	15 048	56 432	78 964	
109 789	10 734	44 536	44 836	105 520	
109 843	16 464	25 396	27 844	84 202	
109 891	36 552	56 682	69 590	103 212	
115 727	36 360	71 962	101 956	112 830	
115 901	33 582	68 462	90 922	95 722	
120 557	42 760	93 110	95 380	101 758	

Напомним (п. 3 § 7 гл. III), что если для данного l среди чисел Бернулли $B_2, \ldots, B_{l-3}$ имеется ровно r чисел, делящихся на l, то r называется *индексом иррегулярности* простого нечетного l. Число l регулярно, если его индекс иррегулярности равен нулю. Обозначим через $\pi_r(x)$ число простых нечетных чисел $\leqslant x$, индекс иррегулярности которых равен r. Если $\pi(x)$ обозначает число всех нечетных простых чисел, не превосходящих x, то

$$\pi(x) = \sum_{r \geqslant 0} \pi_r(x).$$

При $x = 125\,000$ имеем следующую таблицу:

r	0	1	2	3	4	5	$\geqslant 6$
$\pi_r(x)$	7128	3559	875	153	16	2	0

Таким образом, среди 11 733 нечетных простых чисел $< 125\,000$ имеется 7128 регулярных и 4605 иррегулярных.

Основываясь на допущении, что числители чисел Бернулли равномерно распределены в классах вычетов по любому простому модулю, и привлекая вероятностные соображения, Зигель в работе [129] выдвинул гипотезу, что среди всех нечетных простых чисел доля регулярных простых чисел составляет

$$\frac{1}{\sqrt{e}} \cong 0{,}6065,$$

т. е. около 61% (об этом мы упоминали в п. 3 § 7 гл. III). Те же эвристические аргументы Зигеля позволяют также предположить, что

$$\lim_{x \to \infty} \frac{\pi_r(x)}{\pi(x)} = \frac{1}{\sqrt{e}\, r!\, 2^r} \qquad (r \geqslant 0).$$

Приведенная формула довольно хорошо согласуется с табличными данными, однако мы не имеем никаких подходов к ее доказательству. Если она верна, то, в частности, получаем, что для любого натурального r существует бесконечно много иррегулярных простых чисел с индексом иррегулярности r (в то же время их плотность очень быстро убывает с увеличением r).

Иррегулярная пара (см. п. 1 § 7 гл. V) вида $(l, l-3)$ впервые появляется при $l = 16\,843$. Иррегулярные пары вида $(l, l-5)$ и $(l, l-9)$ мы имеем при $l = 37$ и $l = 67$ соответственно. В то же время для всех $l < 125\,000$ мы не встречаем ни одной иррегулярной пары вида $(l, l-7)$.

Согласно одному сравнению Вороного при $l \equiv 3 \pmod 4$ пара $(l, (l+1)/2)$ всегда регулярна. Если же $l \equiv 1 \pmod 4$ и $l < 125\,000$, то $(l, (l-1)/2)$ — также регулярная пара. Однако, верно ли это для всех $l \equiv 1 \pmod 4$, неизвестно. Последний вопрос особенно интересен в связи с утверждением задачи 2 § 6 гл. V ([46], [55]).

В пределах $l < 125\,000$ не встречается ни одной иррегулярной пары $(l, 2a)$, для которой B_{2a} делилось бы на l^2. Однако более вероятным является предположение, что существуют l, для которых $l^2 | B_{2a}$, $2 \leqslant 2a \leqslant l-3$.

Известен отрезок из 27 последовательных простых чисел, состоящий сплошь из регулярных чисел; он начинается с $l = 17\,881$. Наибольший известный отрезок последовательных иррегулярных простых чисел содержит 11 простых чисел и начинается с $l = 8597$.

В связи с замечанием в конце п. 3 § 7 гл. III (с. 252) интересен вопрос, как часто встречаются последовательные иррегулярные пары, т. е. пары вида $(l, 2a)$ и $(l, 2a+2)$. В пределах таблицы 11 мы встречаем две таких пары при $l = 491$ и $l = 587$. В статье [87] отмечается, что для всех $l < 30\,000$ других последовательных иррегулярных пар нет.

Согласно теореме Дирихле (п. 3 § 3 гл. V) при любом модуле m все простые числа равномерно распределены по классам приведенных вычетов,

Данные работы [142] позволяют предположить, что иррегулярные простые числа также равномерно распределяются по всем $\varphi(m)$ классам приведенных вычетов. Для $m = 3, 4, 5$ распределение иррегулярных простых чисел $< 125\,000$ по классам вычетов выглядит следующим образом:

m	r	ω	m	r	ω
3	1	2282	5	1	1114
	2	2323		2	1193
4	1	2283		3	1149
	3	2322		4	1149

Здесь в колонке ω указано число иррегулярных простых чисел $< 125\,000$, которые $\equiv r \pmod m$.

ТАБЛИЦА 13

Разложение на простые множители числителей N_{2a} чисел Бернулли B_{2a} (в несократимой записи) для $2a \leqslant 60$.

$2a$	N_{2a}
2	1
4	1
6	1
8	1
10	5
12	691
14	7
16	3617
18	43867
20	283·617
22	11·131·593
24	103·2294797
26	13·657931
28	7·9349·362903
30	5·1721·1001259881
32	37·683·305065927
34	17·151628697551
36	2631527155305347737 3
38	19·154210205991661
40	137616929·1897170067619
42	1520097643918070802691
44	11·59·8089·2947939·1798482437
46	23·383799511·67568238839737
48	653·56039·153289748932447906241
50	5·5·417202699·47464429777438199
52	13·577·58741·401029177·4534045619429
54	39409·660183281·1120412849144121779
56	7·113161·163979·190880827068405505503 13
58	29·67·186707·6235242049·3734958336910 4129
60	2003·5549927·109317926249509865773025015237911

Замечание: В книге [144] содержатся значения чисел Бернулли B_{2a} для $2a \leqslant 124$. Более обширная таблица чисел Бернулли (для $2a \leqslant 250$) приведена в статье [153]. В этой работе указаны целые числа C_{2a} такие, что $B_{2a} = C_{2a} - \Sigma(1/p)$, где p пробегает простые числа, для которых $(p-1) \mid 2a$. В [153] отмечается также, что авторами вычислены числа Бернулли для $2a \leqslant 836$ и соответствующая таблица передана на хранение в редакцию журнала (архив UMT — Unpublished Mathematical Tables).

СПИСОК ЛИТЕРАТУРЫ

Помимо работ, цитируемых в тексте, в список литературы включены несколько книг, сыгравших особенно важную роль в развитии вопросов, излагаемых в настоящей книге. Конечно, наш перечень весьма далек от полного. Обширная библиография, охватывающая работы до 1970 г., приведена в книге [33].

I. МОНОГРАФИИ И ОБЗОРЫ

1. Алгебраическая теория чисел/Под ред. Касселса Дж., Фрёлиха А.— М.: Мир, 1969.
2. Боревич З. И., Шафаревич И. Р. Теория чисел.— М.: Наука, 1964; 2-е изд., 1972.
3. Бохнер С., Мартин У. Т. Функции многих комплексных переменных.— М.: ИЛ, 1951.
4. Бурбаки Н. Коммутативная алгебра.— М.: Мир, 1971.
5. Ван дер Варден Б. Л. Алгебра.— М.: Наука, 1976; 2-е изд. 1979.
6. Вейль А. Основы теории чисел.— М.: Мир, 1972.
7. Вороной Г. Ф. Собрание сочинений.— Киев: Изд-во АН УССР, т. 1 и т. 2, 1952; т. 3, 1953.
8. Гаусс К. Ф. Арифметические исследования (Disquisitiones arithmeticae).— В кн.: Гаусс К. Ф. Труды по теории чисел.— М.: Изд-во АН СССР, 1959, с. 7—583.
9. Делоне Б. Н., Фаддеев Д. К. Теория иррациональностей третьей степени.— Тр. Мат. ин-та АН СССР, 1940, т. 11, с. 1—340.
10. Дирихле П. Г. Л. Лекции по теории чисел.— М.— Л.: ОНТИ, 1936.
11. Зигель К. Автоморфные функции нескольких комплексных переменных.— М.: ИЛ, 1954.
12. Касселс Дж. Диофантовы уравнения со специальным рассмотрением эллиптических кривых.— Математика. Сб. пер., 1968, т. 12, № 1, с. 113—160; № 2, с. 5—48.
13. Касселс Дж. Рациональные квадратичные формы.— М.: Мир, 1982.
14. Кох Х. Теория Галуа p-расширений.— М.: Мир, 1973.
15. Ленг С. Алгебраические числа.— М.: Мир, 1966.
16. Ленг С. Алгебра.— М.: Мир, 1968.
17. Маркушевич А. И. Краткий курс теории аналитических функций. 4-е изд.,— М.: Наука, 1978.
18. Матиясевич Ю. В. Диофантовы множества.— Успехи мат. наук, 1972, т. 27, № 5(167), с. 185—222.
19. Семинар по комплексному умножению.— Математика. Сб. пер., 1968, т. 12, № 1, с. 55—95.
20. Хассе Х. Лекции по теории чисел.— М.: ИЛ, 1953.
21. Шевалле К. Введение в теорию алгебраических функций от одной переменной.— М.: Физматгиз, 1959.
22. Эдвардс Г. М. Последняя теорема Ферма. Генетическое введение в алгебраическую теорию чисел.— М.: Мир, 1980.
23. Eichler M. Quadratische Formen und orthogonale Gruppen.— Berlin: Springer-Verlag, 1952.

24. Hasse H. Über die Klassenzahl abelscher Zahlkörper.— Berlin: Akademie-Verlag, 1952.
25. Hasse H. Zahlentheorie.— Berlin: Akademie-Verlag, 1968.
26. Hilbert D. Die Theorie der algebraischen Zahlkörper.— Jahresbericht Deutsch. Math.— Vereinigung, 1897, Bd. 4, S. 175—546. [In.: Hilbert D. Gesammelte Abhandlungen.— New York: Chelsea, 1965, S. 63—363.]
27. Ireland K., Rosen M. A classical introduction to modern number theory.— New York — Heidelberg — Berlin: Springer-Verlag, 1982.
28. Iwasawa K. Lectures on p-adic L-functions.— Ann. Math. Studies, № 74.— Princeton — New Jersey: Princeton Univ. Press, 1972.
29. Lang S. Abelian varieties.— New York — London: Interscience Publishers, 1959.
30. Lang S. Diophantine geometry.— New York — London: Interscience Publishers, 1962.
31. Lang S. Cyclotomic fields.— New York — Heidelberg — Berlin: Springer-Verlag, 1978; v. 2, 1980.
32. Lang S. Units and class groups in number theory and algebraic geometry.— Bull. Amer. Math. Soc (N. S.), 1982, v. 6, № 3, p. 253—316.
33. Narkiewicz W. Elementary and analytic theory of algebraic numbers.— Warszawa: Polish Scientific Publishers, 1974.
34. O'Meara O. T. Introduction to quadratic forms.— Berlin: Springer-Verlag, 1963.
35. Ribenboim P. 13 lectures on Fermat's last theorem.— New York — Heidelberg — Berlin: Springer-Verlag, 1979.
36. Serre J.— P. Formes modulaires et Fonctions zêta p-adiques.— Lect. Notes Math., 1973, № 350, p. 191—268.
37. Tate J. The arithmetic of elliptic curves.— Inventiones math., 1974, v. 23, № 3—4, p. 179—206.
38. Washington L. C. Introduction to cyclotomic fields.— New York — Heidelberg — Berlin: Springer-Verlag, 1982.
39. Weil A. Sur les courbes algébriques et les variétés qui s'en déduisent.— Act. Sci. Ind., № 1041.— Paris: Hermann, 1948.

II. СТАТЬИ

40. Абрашкин В. А. Нахождение двухклассных мнимых квадратичных полей с четным дискриминантом методом Хегнера.— Мат. заметки, 1974, т. 15, № 2, с. 241—246.
41. Архипов Г. И., Карацуба А. А. О локальном представлении нуля формой.— Изв. АН СССР. Сер. мат., 1981, т. 45, № 5, с. 948—961.
42. Венков Б. А. О числе классов бинарных квадратичных форм отрицательных определителей. I и II.— Изв. АН СССР. Сер. 7, отд. физ.-мат. наук, 1928, № 4—5, с. 375—392; № 6—7, с. 455—480. [См. также в кн.: Венков Б. А. Исследования по теории чисел. Избранные труды.— Л.: Наука, 1981, с. 91—125.]
43. Голод Е. С., Шафаревич И. Р. О башне полей классов.— Изв. АН СССР. Сер. мат., 1964, т. 28, № 2, с. 261—272.
44. Делоне Б. Н. Решение неопределенного уравнения $x^3q + y^3 = 1$.— Изв. Российской АН. Сер. 6, 1922, т. 16, с. 273—280.
45. Демьянов В. Б. О кубических формах в дискретно нормированных полях.— Докл. АН СССР, 1950, т. 74, № 5, с. 889—891.
46. Киселев А. А. Выражение числа классов идеалов вещественных квадратичных полей через числа Бернулли.— Докл. АН СССР, 1948, т. 61, № 5, с. 777—779.
47. Кобелев В. В. Доказательство великой теоремы Ферма для всех простых показателей, меньших 5500.— Докл. АН СССР, 1970, т. 190, № 4, с. 767—768.

48. Нисневич Л. Б. О числе точек алгебраического многообразия в простом конечном поле.— Докл. АН СССР, 1954, т. 99, № 1, с. 17—20.
49. Новиков А. П. О числе классов полей комплексного умножения.— Изв. АН СССР. Сер. мат., 1962, т. 26, № 5, с. 677—686.
50. Новиков А. П. О числе классов полей, абелевых над квадратично-мнимым полем.— Изв. АН СССР. Сер. мат., 1967, т. 31, № 3, с. 717—726.
51. Степанов С. А. Сравнения с двумя неизвестными.— Изв. АН СССР. Сер. мат., 1972, т. 36, № 4, с. 683—711.
52. Чеботарев Н. Г. Определение плотности совокупности простых чисел, принадлежащих к заданному классу подстановок.— Изв. Российской АН. Сер. 6, 1923, т. 17, с. 205—250. [См. также в кн.: Чеботарев Н. Г. Собрание сочинений, т. 1.— М.— Л.: Изд-во АН СССР, 1949, с. 27—65.]
53. Шафаревич И. Р. Новое доказательство теоремы Кронекера — Вебера.— Тр. Мат. ин-та АН СССР, 1951, т. 38, с. 382—387.
54. Ankeny N. C., Chowla S. The class number of the cyclotomic field.— Canadian J. Math., 1951, v. 3, № 4, p. 486—494.
55. Ankeny N. C., Chowla S. A further note on the class number of real quadratic fields.— Acta arithm., 1962, v. 7, № 3, p. 271—272.
56. Ax J. Zeroes of polynomials over finite fields.— Amer. J. Math., 1964, v. 86, № 2, p. 255—261.
57. Ax J., Kochen S. Diofantine problems over local fields. I.— Amer. J. Math., 1965, v. 57, № 3, p. 605—630.
58. Baker A. Contributions to the theory of diophantine equations.— Philos. Trans. Roy. Soc. London, 1968, v. A263, № 1139, p. 173—208.
59. Baker A. Imaginary quadratic fields with class number 2.— Ann. Math., 1971, v. 94, № 1, p. 139—152. [Русский перевод: Математика. Сб. пер., 1972, т. 16, № 5, с. 3—14.]
60. Barrucand P., Williams H. C., Baniuk L. A computational technique for determining the class number of a pure cubic field.— Math. Comput., 1976, v. 30, № 134, p. 312—323.
61. Birch B. J. Homogeneous forms of odd degree in a large number of variables.— Mathematika, 1957, v. 4, № 8, p. 102—105.
62. Birch B. J. Diophantine analysis and modular functions.— Algebr. Geom., London, 1969, p. 35—42. [Русский перевод: Математика. Сб. пер., 1971, т. 15, № 3, с. 173—176.]
63. Birch B. J., Lewis D. J., Murphy T. G. Simultaneous quadratic forms.— Amer. J. Math., 1962, v. 84, № 1, p. 110—115.
64. Birch B. J., Mc Cann K. A criterion for the p-adic sulubility of diophantine equations.— Quart. J. Math., 1967, v. 18, № 69, p. 59—63.
65. Bombieri E. Counting points on curves over finite fields (d'après S. A. Stepanov).— Lect. Notes Math., 1974, № 383, p. 234—241.
66. Brauer R. A note on systems of homogeneous algebraic equations.— Bull. Amer. Math. Soc., 1945, v. 51, p. 749—755.
67. Brückner H. Zum ersten Fall der Fermat'schen Vermutung.— J. reine und angew. Math., 1975, Bd. 274/275, S. 21—26.
68. Carlitz L. Note on irregular primes.— Proc. Amer. Math. Soc., 1954, v. 5, № 2, p. 329—331.
69. Coates J. The work of Mazur and Wiles on cyclotomic fields.— Lect. Notes. Math., 1981, № 901, p. 220—242.
70. Davenport H. Cubic forms in sixteen variables.— Proc. Roy. Soc., London, 1963, v. A272, № 1350, p. 285—303.
71. Davenport H., Lewis D. J. Homogeneous additive equations.— Proc. Roy. Soc., London, 1963, v. A274, № 1359, p. 443—460.
72. Denef J. The rationality of the Poincaré series associated to the p-adic points on a variety.— Inventiones math., 1984, v. 77, № 1, p. 1—23.
73. Deuring M. Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins.— Inventiones math., 1968, v. 5, № 3, p. 169—179.
74. Diaz y Diaz F. On some families of imaginary quadratic fields.— Math. Comput., 1978, v. 32, № 142, p. 637—650.

75. Eichler M. Eine Bemerkung zur Fermat'schen Vermutung.— Acta arithm., 1965, v. 11, № 1, p. 129—131.

76. Faltings G. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.— Inventiones math., 1983, v. 73, № 3, p. 349—366.

77. Gross B., Zagier D. Points de Heegner et dérivées de fonctions.— C. r. Acad. Sci., Paris, 1983, t. 297, sér. 1, № 2, p. 85—88.

78. Hasse H. Zur Geschlechtertheorie in quadratischen Zahlkörpern.— J. Math. Soc. Japan, 1951, v. 3, № 1, p. 45—51.

79. Heath-Brown D. R. Cubic forms in ten variables.— Proc. London Math. Soc., 1983. v. 47, № 2, p. 225—257.

80. Hecke E. Bestimmung der Klassenzahl einer neuen Reihe von algebraischen Zahlkörpern — Nachr. Akad. Wiss. Göttingen. Math.— phys. Kl., 1921, № 1, S. 1—23. [Hecke E. Mathematische Werke.— Göttingen: Vandenhoeck — Ruprecht, 1970, S. 290—312.]

81. Heegner K. Diophantische Analysis und Modulfunktionen.— Math. Z., 1952, Bd. 56, № 3, S. 227—253.

82. Igusa J. Some observations on higher degree characters.— Amer. J. Math., 1977, v. 99, № 2. p. 393—417.

83. Ince E. L. Cycles of reduced ideals in quadratic fields. Mathematical tables, v. 4.— London: British association for the advancement of science, 1934.

84. Iwasawa K. A class number formula for cyclotomic fields.— Ann. Math., 1962, v. 76, № 1, p. 171—179.

85. Jensen K. L. Om talteoretiske Egenskaber ved de Bernoulliske tal.— Nyt Tidsskrift f. Math., 1915, v. 26, p. 73—83.

86. Johnson W. On the vanishing of the Iwasawa invariant μ_p for $p < 8000$.— Math. Comput., 1973, v. 27, № 122, p. 387—396.

87. Johnson W. Irregular primes and cyclotomic invariants.— Math. Comput., 1975, v. 29, № 129, p. 113—120.

88. Kenku M A. Determination of the even discriminants of complex quadratic fields of class-number 2.— Proc. London Math. Soc., Ser. 3, 1971, v. 22, № 4, p. 734—746.

89. Kneser M. Kleine Lösungen der diophantischen Gleichung $ax^2 + by^2 = cz^2$.— Abhandl. Math. Sem. Univ. Hamburg, 1959, Bd. 23, S. 163—173.

90. Kubota T., Leopoldt H. W. Eine p-adische Theorie der Zetawerte.— J. reine und angew. Math., 1964, Bd. 214/215, S. 328—339.

91. Kummer E. E. Algemeiner Beweis des Fermat'schen Satzes dass die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten λ, welche ungerade Primzahlen sind und in die Zählern der ersten $\frac{1}{2}(\lambda-3)$ Bernoulli'schen Zahlen als Faktoren nicht vorkommen.— J. reine und angew. Math., 1850, Bd. 40, S. 130—138.

92. Lakein R. B. Computation of the ideal class group of certain complex quartic fields. II.— Math. Comput., 1975, v. 29. № 129, p. 137—144.

93. Lakein R. B. Review of UMT file: Kuroda S. Table of class numbers, $h(p)$ greiter than 1, for fields $Q(\sqrt{p})$, $p \equiv 1 \pmod 4 \leqslant 2\,776\,817$.— Math. Comput., 1975, v. 29, № 129, p. 335—336.

94. Lang S., Weil A. Number of points of varieties in finite fields.— Amer. J. Math., 1954, v. 76, № 4, p. 819—827.

95. Lehmer D. H. On Fermat's quotient, base two.— Math. Comput., 1981, v. 36, № 153, p. 289—290.

96. Lehmer D. H., Lehmer E., Vandiver H. S. An application of high-speed computing to Fermat's last theorem.— Proc. Nat. Acad. Sci. U. S. A., 1954, v. 40, № 1, p. 25—33.

97. Lehmer D. H., Masley J. M. Table of the cyclotomic class numbers $h^*(p)$ and their factors for $200 < p < 521$.— Math. Comput., 1978, v. 32, № 142, p. 577—582.

98. Leopoldt H. W. Eine Verallgemeinerung der Bernoullischen Zahlen.— Abhandl. math. Semin. Univ. Hamburg, 1958, Bd. 22, S. 131—140.

99. Leopoldt H. W. Zur Arithmetik in abelschen Zahlkörpern.— J. reine und angew Math., 1962, Bd. 209, № 1—2, S. 54—71.

100. Lepistö T. On the growth on the first factor of the class number of the prime cyclotomic field.— Ann. Acad. Sci. Fennicae, Ser. A, I, 1974, № 577, p. 3—21.

101. Lewis D. J. Cubic homogeneous polynomials over p-adic number fields.— Ann. Math., 1952, v. 56, № 3, p. 473—478.

102. Linden F. J. van der. Class number computations of real abelian number fields.— Math. Comput., 1982, v. 39, № 160, p. 693—707.

103. Llorente P., Oneto A. V. On the real cubic fields.— Math. Comput., 1982, v. 39, № 160, p. 689—692.

104. Masley J. M. Solution of small class number problems for cyclotomic fields.— Compositio Math., 1976, v. 33, № 2, p. 179—186.

105. Masley J. M. Class numbers of real cyclic number fields with small conductor.— Compositio Math., 1978, v. 37, № 3, p. 297—319.

106. Masley J. M., Montgomery H. L. Cyclotomic fields with unique factorization.— J. reine und angew Math., 1976, Bd. 286/287, S. 248—256.

107. Mattuck A., Tate J. On the inequality of Castelnuovo — Severi.— Abhandl. Math. Sem. Univ. Hamburg, 1958, Bd. 22, № 3—4, S. 295—299. [Русский перевод: Математика. Сб. переводов, 1960, т. 4, № 2, с. 25—28.]

108. Metsänkylä T. Distribution of irregular prime numbers.— J. reine and angew. Math., 1976, Bd. 282, S. 126—130.

109. Meuser D. On the rationality of certain generating functions.— Math. Ann., 1981, Bd. 256, № 3, S. 303—310.

110. Mirimanoff D. Sur le dernier théorème de Fermat.— C. r. Acad. Sci., Paris, 1910, t. 150, № 4, p. 204—206.

111. Neild C., Shanks D. On the 3-rank of quadratic fields and the Euler product.— Math. Comput., 1974, v. 28, № 125, p. 279—291.

112. Newman M. A table of the first factor for prime cyclotomic fields.— Math. Comput., 1970, v. 24, № 109, p. 215—219.

113. Odlyzko A. M. Lower bounds for discriminants of number fields.— Acta arithm., 1976, v. 29, № 3, p. 275—297.

114. Odlyzko A. M. Lower bounds for discriminants of number fields. II.— Tôhoku Math. J., 1977, v. 29, № 2, p. 209—216.

115. Pleasonts P. A. B. Cubic polynomials over algebraic number fields.— J. Number Theory, 1975, v. 7, № 3, p. 310—344.

116. Ramachandra K. Some applications of Kronecker's limit formulas.— Ann. Math., 1964, v. 80, № 1, p. 104—148.

117. Reidemeister K. Über die Relativklassenzahl gewisser relativquadratischer Zahlkörper.— Abhandl. math. Semin. Univ, Hamburg, 1929, Bd. 1, S. 27—48.

118. Ribet K. A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$. — Inventiones Math., 1976, v. 34, № 3, p. 151—162.

119. Schmidt W. M. Linearformen mit algebraischen Koeffizienten. II.— Math. Ann., 1971, Bd. 191, № 1, S. 1—20.

120. Schoof R. J. Class groups of complex quadratic fields.— Math. Comput., 1983, v. 41, № 163, p. 295—302.

121. Seah E., Washington L. C., Williams H. C. The calculation of a large cubic class number with an application to real cyclotomic fields.— Math. Comput., 1983, v. 41, № 163, p. 303—305.

122. Selfridge J. L., Nicol C. A., Vandiver H. S. Proof of Fermat's last theorem for all prime exponents less than 4002.— Proc. Nat. Acad. Sci. U. S. A., 1955, v. 41, № 11, p. 970—973.

123. Selmer E. S. The diophantine equation $ax^3 + by^3 + cz^3 = 0$.— Acta Math., 1951, v. 85, № 3—4, p. 203—262.

124. Selmer E. S. Tables for the purely cubic field $K(\sqrt[3]{m})$. — Avhandl. utg. Norske vid. Akad. Oslo. Mat.— naturvid. Kl., 1955, № 5, p. 1—38.

125. Shanks D. The simplest cubic fields.— Math. Comput., 1974, v. 28, № 128, p. 1137—1152.

126. Shanks D. Class groups of the quadratic fields found by F. Diaz y Diaz.— Math. Comput., 1976, v. 30, № 133, p. 173—178.

127. Shanks D., Serafin R. Quadratic fields with four invariants divisible by 3.— Math. Comput., 1973, v. 27, № 121, p. 183—187.

128. Shanks D., Williams H. C. Gunderson's function in Fermat's last theorem.— Math. Comput., 1981, v. 36, № 153, p. 291—295.

129. Siegel C. L. Zu zwei Bemerkungen Kummers.— Nachr. Akad. Wiss. Göttingen. II. Math.— Phys. Kl., 1964, № 6, S. 51—57.

130. Siegel C. L. Bernoullische Polynome und quadratische Zahlkörper.— Nachr. Akad. Wiss. Göttingen. Math.— Phys. Kl., 1968, № 2, S. 7—38. [Siegel C. L. Gesammelte Abhandlungen, Bd. 4.— Berlin: Springer-Verlag, 1979, S. 9—40.]

131. Siegel C. L. Über die Fourierschen Koeffizienten von Modulformen.— Nachr. Akad. Wiss. Göttingen. Math.— Phys. Kl., 1970, № 3, S. 15—56. [Siegel C. L. Gesammelte Abhandlungen, Bd. 4.— Berlin: Springer Verlag, 1979, S. 98—139.]

132. Skula L. Divisorentheorie einer Halbgruppe.— Math. Z., 1970, Bd. 114, № 2, S. 113—120.

133. Skula L. Eine Bemerkung zu dem ersten Fall der Fermat'schen Vermutung.— J. reine und angew. Math., 1972, Bd. 253, S. 1—14.

134. Stark H. M. A complete determination of the complex quadratic fields of class-number one.— Michigan Math. J., 1967, v. 14, № 1, p. 1—27.

135. Stark H. M. A transcendence theorem for class-number problems. II.— Ann. Math., 1972. v. 96, № 1, p. 174—209.

136. Stark H. M. On complex quadratic fields with class-number two.— Math. Comput., 1975, v. 29, № 129, p. 289—302.

137. Terjanian G. Un contre-exemple à une conjecture d'Artin.— C. r. Acad. Sci., Paris, 1966, t. AB262, № 11, p. A612.

138. Uchida K. Class numbers of imaginary abelian number fields, III.— Tôhoku Math. J., 1971, v. 23, № 4, p. 573—580.

139. Vandiver H. S. Fermat's last theorem and the second factor in the cyclotomic class number.— Bull. Amer. Math. Soc., 1934, v. 40, № 2, p. 118—126.

140. Vandiver H. S. Examination of methods of attack of the second case of Fermat's last theorem.— Proc. Nat. Acad. Sci. U. S. A., 1954, v. 40, № 8, p. 732—735.

141. Wada H. A table of ideal class groups of imaginary quadratic fields.— Proc. Japan Acad., 1970, v. 46, № 5, p. 401—403.

142. Wagstaff S. S. (Jr.) The irregular primes to 125 000.— Math. Comput., 1978, v. 32, № 142, p. 583—591.

143. Warning E. Bemerkung zur vorstehenden Arbeit von Herrn Chevalley.— Abhandl. Math. Semin. Univ. Hamburg, 1935, Bd. 11, № 1—2, S. 76—83.

144. Washington L. C. On Fermat's last theorem.— J. reine und angew. Math., 1977, Bd 289, S. 115—117.

145. Wieferich A. Zum letzten Fermatschen Theorem.— J. reine und angew. Math., 1909, Bd. 136, S. 293—302.

146. Williams H. C. Certain pure cubic fields with class-number one.— Math. Comput., 1977, v. 31, № 138, p. 578—580.

147. Williams H. C., Broere J. A computational technique for evaluating $L(1, \chi)$ and the class number of a real quadratic field.— Math. Comput., 1976, v. 30, № 136, p. 887—893.

148. Williams H. C., Cormack G., Seah E. Calculation of the regulator of a pure cubic field.— Math. Comput., 1980, v. 34, № 150, p. 567—611.

149. Williams H. C., Dueck G. W., Schmid B. K. A rapid method of evaluating the regulator and class number of a pure cubic field.— Math. Comput., 1983, v. 41, № 163, p. 235—286.

150. Williams H. C., Shanks D. A note on class-number one in pure cubic fields.— Math. Comput., 1979, v. 33, № 148, p. 1317—1320.

ДОПОЛНЕНИЕ ПРИ КОРРЕКТУРЕ

151. Diaz y Diaz F., Shanks D., Williams H. C. Quadratic fields with 3-rank equal to 4.— Math. Comput., 1979, v. 33, № 146, p. 836—840.

152. Keller W., Löh G. The criteria of Kummer and Mirimanoff extended to include 22 consecutive irregular pairs.— Tokyo J. Math., 1983, v. 6, № 2, p. 397—402.

153. Knuth D. E., Buckholtz T. J. Computation of tangent, Euler, and Bernoulli numbers.— Math. Comput., 1967, v. 21, № 100, p. 663—688.

154. Krasner M. Sur le premier cas du théorème de Fermat.— C. r. Acad. Sci., Paris, 1934, t. 199, № 4, p. 256—258.

155. Martinet J. Petits discriminants.— Ann. Inst. Fourier, 1979, t. 29, № 1, p. 159—170.

156. Tateyama K. On the ideal class groups of some cyclotomic fields.— Proc. Japan Acad., 1982, v. A58, № 7, p. 333—335.

157. Wada H. Some computations of criteria of Kummer.— Tokyo J. Math., 1980, v. 3, № 1, p. 173—176.

158. Yahagi O. Construction of number fields with prescribed l-class groups.— Tokyo J. Math., 1978, v. 1, № 2, p. 275—283.

159. Adleman L. M., Heath-Brown D. R. The first case of Fermat's last theorem.— Inventiones Math., 1985, v. 79, № 2, p. 409—416.

160. Fouvry E. Theoreme de Brun — Titchmarsh; application au theoreme de Fermat.— Inventiones Math., 1985, v. 79, № 2, p. 383—407.

161. Heath-Brown D. R. Fermat's last Theorem for «almst all» exponents.— Bull. London Math. Soc., 1985, v. 17, pt. 1, № 64, p. 15—16.

ПЕРЕЧЕНЬ СТАНДАРТНЫХ ОБОЗНАЧЕНИЙ

$\mathbb{Z}$ — кольцо целых рациональных чисел

$\mathbb{Z}_p$ — кольцо целых p-адических чисел

$\mathbb{Q}$ — поле рациональных чисел

$\mathbb{Q}_p$ — поле p-адических чисел

$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ — поле вычетов по простому модулю p

$\mathbb{F}_q = GF(q)$ — конечное поле, содержащее q элементов

$\mathbb{R} = \mathbb{Q}_\infty$ — поле вещественных чисел

$\mathbb{R}^m$ — вещественное m-мерное пространство

$\mathbb{C}$ — поле всех комплексных чисел

K^* — мультипликативная группа поля K

$\mathrm{Sp}\,\alpha = \mathrm{Sp}_{K/k}(\alpha)$, $N(\alpha) = N_{K/k}(\alpha)$ — след и норма элемента α из конечного расширения K/k поля k

$\mathrm{R} = \mathrm{R}(K)$ — регулятор поля алгебраических чисел K

B_m — числа Бернулли (в четной нумерации: $B_{2r+1} = 0$ при $r \geqslant 1$)

$h = h(K)$ — число классов дивизоров поля алгебраических чисел K

$h^* = h^*(p)$ — первый множитель числа классов дивизоров поля деления круга на p частей

$h_0 = h_0(p)$ — второй множитель числа классов дивизоров поля деления круга на p частей

$\zeta(s)$ — дзета-функция Римана

$\zeta_K(s)$ — дзета-функция Дедекинда

$a \mid b$ — a делит b

$a \nmid b$ — a не делит b

$\left(\dfrac{a}{p}\right)$ — символ Лежандра

(α, β) — символ Гильберта в поле p-адических чисел

$\left(\dfrac{\alpha, b}{p}\right)$ — символ Гильберта (для рациональных a и b) в поле $\mathbb{Q}_p$, включая $p = \infty$

$[\xi]$ — целая часть вещественного числа ξ

$\mathrm{Re}\,\alpha$, $\mathrm{Im}\,\alpha$ — вещественная a и мнимая b части комплексного числа $\alpha = a + bi$

$A \subset B$ — включение, допускающее равенство

$\varphi(m)$ — теоретико-числовая функция Эйлера

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ОГЛАВЛЕНИЕ