ALGEBRAIC NUMBERS

SERGE LANG
Columbia University, New York

Addison-Wesley Publishing Company,
Reading, Mass. Palo Alto. London
1964

БИБЛИОТЕКА СБОРНИКА «МАТЕМАТИКА»

С. ЛЕНГ

АЛГЕБРАИЧЕСКИЕ ЧИСЛА

Перевод с английского
Ю. И. МАНИНА

ИЗДАТЕЛЬСТВО «МИР»
Москва 1966

УДК 511.6

Небольшая монография С. Ленга посвящена важному разделу современной теории чисел. Кроме традиционного материала, она включает ряд глубоких результатов, не освещавшихся ранее в монографической литературе. Книга может служить хорошим введением в теорию полей классов и арифметику линейных групп. Она представляет интерес для математиков различных специальностей.

Редакция литературы по математическим наукам

ПРЕДИСЛОВИЕ

Цель этой книги — изложить основные классические результаты алгебраической и аналитической теории чисел. Из-за отсутствия в литературе требуемого материала мне пришлось включить элементы алгебраической теории в одну из глав книги [7], однако в весьма отрывочном виде. Поэтому я счел полезным дать здесь более полное изложение, способное, кроме всего прочего, служить введением к записям семинара Артина — Тейта по теории полей классов [3].

С другой стороны, помимо классической теории целого замыкания, дискретно нормированных колец, дифференты и дискриминанта, я дополнил теоремы о единицах и о числе классов известной оценкой Минковского для дискриминанта, а к принадлежащей Артину и Уэйплсу оценке числа элементов в параллелотопах добавил более точную асимптотическую формулу. Оба эти результата имеют количественный характер (в отличие от качественной точки зрения, которой я придерживался в книге [7]).

Четыре главы, посвященные аналитической теории чисел, воспроизводят без существенных изменений следующие четыре опубликованные и неопубликованные работы, посвященные дзета-функции и L-функциям числовых полей.

Диссертация Тейта, все еще неопубликованная (изложена в гл. VII).

Теоремы о плотности простых идеалов в обобщенных арифметических прогрессиях в варианте, возникшем на

одном из семинаров Артина около двенадцати лет назад.

Статья Брауэра [5], в которой доказана высказанная в качестве предположения Зигелем асимптотическая формула $\log(hR) \sim \log d^{1/2}$.

Принадлежащий Вейлю вариант явной формулы в теории простых идеалов [10].

В определенном отношении план этой книги более или менее совпадает с планом работы Гильберта [6], хотя, разумеется, и алгебраический, и аналитический аспекты теории чисел изложены в их нынешнем виде (а теория полей классов опущена). Книга Гильберта содержит много примеров и вычислений, что и сейчас делает ее чтение весьма приятным. Все изложения теории алгебраических чисел испытали на себе ее влияние и влияние курса Артина [1] (а также неопубликованных записей семинаров Артина). Мы принимаем глобальную точку зрения и лишь по ходу дела занимаемся локальными полями, которые более полно изучены в книге Серра [8]. В пользу прямого глобального подхода к изучению числовых полей можно сказать многое; я даже включил основную лемму, использованную Артином в его первоначальном доказательстве закона взаимности. Я надеюсь, что благодаря этому читатель сможет приобрести некоторую интуицию иного характера, чем при других вариантах изложения.

С. Ленг

Нью-Йорк, 1963 г.

ПРЕДВАРИТЕЛЬНЫЕ ТРЕБОВАНИЯ

Главы I — V замкнуты и требуют от читателя знания лишь элементарной алгебры, скажем на уровне теории Галуа. Кроме того, нужны некоторые результаты о нормированиях. Их полные формулировки содержатся в книге, а несложные доказательства, относящиеся собственно к основному курсу алгебры, можно найти в [7]. В гл. VI используется язык теоретико-множественной топологии.

В главах, посвященных аналитической теории чисел, необходим ряд сведений из анализа. В гл. VII используется аппарат анализа Фурье на локально компактных группах. В гл. VIII — X нужны лишь стандартные аналитические факты (некоторые из них мы даже доказываем), за исключением ссылки на формулу Планшереля в гл. X.

При доказательстве теоремы Брауэра — Зигеля используется формализм теории L-рядов и характеров. Результаты, доказательства которых не приводятся, сформулированы явно и не должны смущать читателя.

Слово *кольцо*, если не оговорено обратное, всегда означает коммутативное кольцо с единицей и без делителей нуля.

Для всякого поля K символом K^* обозначается его мультипликативная группа, а символом $\overline{K}$ — его алгебраическое замыкание. Для всякого многочлена f символом f' обозначается либо его производная, либо его образ относительно некоторого гомоморфизма; точный смысл всегда будет ясен из контекста.

Мы пользуемся обозначениями o и O. Пусть f, g — две функции вещественного переменного, $g \geqslant 0$. Мы пишем $f = O(g)$, если существует такая константа $C > 0$, что $|f(x)| \leqslant Cg(x)$ при всех достаточно больших x. Мы пишем $f = o(g)$, если $\lim\limits_{x\to\infty} [f(x)/g(x)] = 0$. Наконец, мы пишем $f \sim g$, если $\lim\limits_{x\to\infty} [f(x)/g(x)] = 1$.

ОТ ПЕРЕВОДЧИКА

В тексте книги отсутствовали доказательства нескольких результатов второй главы; они были заменены ссылками на соответствующие места книги [7]. В русском переводе эти доказательства приведены полностью (они отмечены значками ◀.....▶). В связи с этим в текст внесены небольшие изменения; кроме того, исправлены замеченные неточности и опечатки, список которых любезно прислал автор.

Ю. И. Манин

Глава I

ЦЕЛЫЕ АЛГЕБРАИЧЕСКИЕ ЧИСЛА

В этой главе описаны основные свойства кольца целых алгебраических чисел в произвольном числовом поле (всегда предполагается, что это поле имеет конечную степень над полем рациональных чисел $\mathbf{Q}$). Сюда входят также общие сведения о структуре простых идеалов.

Доказательства проводятся в более общей ситуации только в том случае, когда их нельзя сократить, пользуясь специальными свойствами интересующих нас объектов. Писать курс коммутативной алгебры не входило в наши намерения.

§ 1. Локализация

Пусть A — некоторое кольцо. *Мультипликативным подмножеством* в нем называется любое подмножество, содержащее 1 и вместе с любыми двумя элементами x, y их произведение xy. Кроме того, мы постоянно будем считать, что 0 не принадлежит подмножеству.

Пусть K — поле частных кольца A, S — мультипликативное подмножество кольца A. Символом $S^{-1}A$ мы будем обозначать множество частных вида x/s, где $x \in A$, $s \in S$. Оно образует кольцо, в которое A канонически вкладывается.

Пусть M есть A-модуль, содержащийся в некотором поле L (которое содержит поле K). Тогда символом $S^{-1}M$ обозначается множество элементов вида v/s, где $v \in M$ и $s \in S$. Это множество, очевидно, является $S^{-1}A$-модулем. Иногда мы будем рассматривать случай, когда M — кольцо, содержащее A в качестве подкольца.

Пусть $\mathfrak{p}$ — простой идеал кольца A (по определению, $\mathfrak{p} \neq A$). Дополнение $A \setminus \mathfrak{p}$ к $\mathfrak{p}$ в кольце A является тогда

мультипликативным подмножеством $S = S_{\mathfrak{p}}$ этого кольца, и мы будем писать в этом случае $A_{\mathfrak{p}}$ вместо $S^{-1}A$.

Локальным кольцом называется кольцо с единственным максимальным идеалом. Пусть $\mathfrak{o}$ — такое кольцо, а $\mathfrak{m}$ — его максимальный идеал. Тогда любой элемент $x \in \mathfrak{o}$, не лежащий в $\mathfrak{m}$, является единицей (т. е. обратим), потому что иначе главный идеал $x\mathfrak{o}$ содержался бы в некотором максимальном идеале, не совпадающем с $\mathfrak{m}$. Тем самым $\mathfrak{m}$ совпадает с множеством необратимых элементов кольца $\mathfrak{o}$.

Введенное выше кольцо $A_{\mathfrak{p}}$ локально. Непосредственно проверяется, что его максимальный идеал $\mathfrak{m}_{\mathfrak{p}}$ состоит из частных вида x/s, где $x \in \mathfrak{p}$ и $s \in \mathfrak{o} \setminus \mathfrak{p}$.

Заметим, что $\mathfrak{m}_{\mathfrak{p}} \cap A = \mathfrak{p}$. Действительно, включение $\supset$ очевидно. Обратно, если $y = x/s \in \mathfrak{m}_{\mathfrak{p}} \cap A$, где $x \in \mathfrak{p}$ и $s \in S$, то $x = sy \in \mathfrak{p}$ и $s \notin \mathfrak{p}$. Следовательно, $y \in \mathfrak{p}$.

Пусть A — некоторое кольцо, S — его мультипликативное подмножество. Пусть $\mathfrak{a}'$ — идеал в кольце $S^{-1}A$. Тогда

$$\mathfrak{a}' = S^{-1}(\mathfrak{a}' \cap A).$$

Действительно, включение $\supset$ очевидно. Обратно, пусть $x \in \mathfrak{a}'$.

Пусть $x = a/s$, где $a \in A$ и $s \in S$. Тогда $sx \in \mathfrak{a}' \cap A$, откуда $x \in S^{-1}(\mathfrak{a}' \cap A)$.

Применение операции S^{-1} дает гомоморфное отображение мультипликативной системы идеалов кольца A на мультипликативную систему идеалов кольца $S^{-1}A$. Это другая формулировка только что доказанных свойств. Если для некоторого идеала $\mathfrak{a} \subset A$ идеал $S^{-1}\mathfrak{a}$ единичен, то, очевидно, множество $\mathfrak{a} \cap S$ непусто. Мы будем говорить в этом случае, что $\mathfrak{a}$ *пересекается* с S.

§ 2. Целое замыкание

Пусть A — кольцо, x — произвольный элемент некоторого поля L, содержащего A. Элемент x называется *целым* над кольцом A, если выполнено одно из следующих условий.

Ц1. *Существует такой конечно порожденный ненулевой A-модуль $M \subset L$, что $xM \subset M$.*

Ц2. *Элемент x удовлетворяет некоторому уравнению вида*

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$$

с коэффициентами $a_i \in A$, где $n \geqslant 1$ — целое число. (Такое уравнение мы будем называть *целым*.)

На самом деле оба эти условия эквивалентны. Действительно, если выполнено условие Ц2, то модуль M, порожденный элементами $1, x, \ldots, x^{n-1}$, отображается в себя при умножении на x. Обратно, пусть существует такой ненулевой модуль $M = \langle v_1, \ldots, v_n \rangle$, что $xM \subset M$. Тогда

$$\begin{aligned} xv_1 &= a_{11}v_1 + \ldots + a_{1n}v_n \\ &\ldots\ldots\ldots\ldots \\ xv_n &= a_{n1}v_1 + \ldots + a_{nn}v_n, \end{aligned}$$

где $a_{ij} \in A$. Перенося члены $xv_1, \ldots, xv_n$ вправо, получаем отсюда, что определитель

$$\begin{vmatrix} a_{11}-x & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22}-x & \ldots & a_{2n} \\ \cdot & \cdot & \ldots & \cdot \\ a_{n1} & a_{n2} & \ldots & a_{nn}-x \end{vmatrix}$$

равен нулю. Это дает целое уравнение для x над кольцом A.

Предложение 1. *Пусть A — кольцо, K — его поле частных, x — алгебраический над K элемент. Существует такой ненулевой элемент $c \in A$, что cx цел над A.*

Доказательство. Существует некоторое уравнение вида

$$a_n x^n + \ldots + a_0 = 0,$$

где $a_i \in A$ и $a_n \neq 0$. Умножим это уравнение на a_n^{n-1}. Тогда

$$(a_n x)^n + \ldots + a_0 a_n^{n-1} = 0$$

дает искомое уравнение для элемента $a_n x$ над A.

Пусть B — некоторое кольцо, содержащее A. Назовем кольцо B *целым* над A, если всякий его элемент цел над A.

Предложение 2. *Если кольцо B цело над A и конечно порождено как A-алгебра, то оно конечно порождено и как A-модуль.*

Доказательство. Можно провести индукцию по числу образующих A-алгебры B, так что достаточно рассмотреть случай, когда $B=A[x]$, где x — некоторый целый над A элемент. Но мы уже убедились, что в этом случае утверждение справедливо.

Предложение 3. *Пусть $A\subset B\subset C$ — три кольца. Если B цело над A, а C цело над B, то C цело и над A.*

Доказательство. Пусть $x\in C$. Элемент x удовлетворяет целому уравнению

$$x^n+b_{n-1}x^{n-1}+\ldots+b_0=0,$$

где $b_i\in B$. Положим $B_1=A[b_0, \ldots, b_{n-1}]$. Тогда по предложению 2 кольцо B_1 конечно порождено как A-модуль, а кольцо $B_1[x]$ также конечно порождено как B_1-модуль. Следовательно, это последнее кольцо представляет собой конечно порожденный A-модуль, а так как умножение на x отображает его в себя, то элемент x цел над A.

Предложение 4. *Пусть $A\subset B$ — два кольца, и B цело над A. Пусть σ — некоторый гомоморфизм кольца B. Тогда кольцо $\sigma(B)$ цело над $\sigma(A)$.*

Доказательство. Применим σ к целому уравнению, которому удовлетворяет элемент x кольца B. В результате получится целое уравнение для элемента $\sigma(x)$ над кольцом $\sigma(A)$.

Это предложение часто используется в случае, когда σ — изоморфизм; оно особенно полезно в теории Галуа.

Предложение 5. *Пусть A — кольцо, содержащееся в поле L. Пусть B — множество тех элементов поля L, которые целы над A. Тогда B — кольцо. (Оно называется целым замыканием кольца A в L.)*

Доказательство. Пусть x, $y\in B$, и пусть M, N — конечно порожденные A-модули, для которых $xM\subset M$ и $yN\subset N$. Тогда модуль MN конечно порожден и отображается в себя при умножении на $x\pm y$ и xy.

Следствие. *Пусть A — кольцо, K — его поле частных, L — конечное сепарабельное расширение поля K. Пусть x — любой элемент поля L, целый над A. Тогда норма и след элемента x из L в K целы над A. Целы также все коэффициенты неприводимого многочлена над полем K, корнем которого является x.*

Доказательство. Для всякого изоморфизма σ поля L над K элемент σx цел над A. Поскольку норма является произведением элементов σx для всех σ, а след — суммой таких элементов, то они целы над A. Коэффициенты же неприводимого уравнения с точностью до знака совпадают с элементарными симметрическими функциями от элементов σx и, значит, тоже целы над A.

Кольцо A называется *целозамкнутым в поле L*, если всякий элемент этого поля, целый над A, принадлежит A. Кольцо называется *целозамкнутым*, если оно целозамкнуто в своем поле частных.

Предложение 6. *Пусть A — нетерово целозамкнутое кольцо, L — конечное сепарабельное расширение его поля частных K. Тогда целое замыкание кольца A в поле L конечно порождено над A.*

Доказательство. Так как кольцо A нетерово, достаточно проверить, что его целое замыкание содержится в некотором конечно порожденном A-модуле.

Пусть $w_1, \ldots, w_n$ — линейный базис расширения L над K. Умножив каждый элемент w_i на подходящий элемент кольца A, мы, не теряя общности, можем считать, что w_i целы над A (предложение 1). Оператор следа Tr из поля L в K является K-линейным отображением L в K. Оно ненулевое: существует элемент $x \in L$, для которого $\mathrm{Tr}(x) \neq 0$. Для всякого ненулевого элемента $\alpha \in L$ функция $\mathrm{Tr}(\alpha x)$ на L принадлежит пространству, двойственному L над K. Этим определяется гомоморфизм L в двойственное пространство. Поскольку ядро такого отображения тривиально, то L изоморфно своему двойственному пространству, и этот изоморфизм определяется билинейной формой

$$(x, y) \rightsquigarrow \mathrm{Tr}(xy).$$

Пусть $w_1', \ldots, w_n'$—базис, двойственный к $w_1, \ldots, w_n$, так что

$$\mathrm{Tr}\,(w_i' w_j) = \sigma_{ij}.$$

Пусть $c \in A$—такой ненулевой элемент, что все cw_i' целы над A. Пусть элемент $z \in L$ цел над A. Тогда все элементы zcw_i' и все их следы $\mathrm{Tr}\,(czw_i')$ целы над A. Положим

$$z = b_1 w_1 + \ldots + b_n w_n,$$

где $b_i \in K$. Тогда

$$\mathrm{Tr}\,(czw_i') = cb_i$$

и $cb_i \in A$, так как кольцо A целозамкнуто. Следовательно, z содержится в A-модуле

$$Ac^{-1}w_1 + \ldots + Ac^{-1}w_n.$$

Поскольку в качестве z мы взяли произвольный элемент целого замыкания кольца A в поле L, то это целое замыкание содержится в некотором конечно порожденном A-модуле, что и завершает доказательство.

Предложение 7. *Всякое кольцо A с однозначным разложением на множители целозамкнуто.*

Доказательство. Предположим, что существуют частное a/b, $a, b \in A$, целое над A, и простой элемент $p \in A$, который делит b, но не делит a. Для некоторого целого числа $n \geqslant 1$ имеем

$$(a/b)^n + a_{n-1}(a/b)^{n-1} + \ldots + a_0 = 0,$$

откуда

$$a^n + a_{n-1}ba^{n-1} + \ldots + a_0 b^n = 0.$$

Так как p делит b, он должен делить a^n, а значит, и a, что противоречит предположению.

Теорема 1. *Пусть A—кольцо главных идеалов, L—конечное сепарабельное расширение его поля частных, имеющее степень n. Пусть B—целое замыкание кольца A в L. Тогда B является свободным A-модулем ранга n.*

Доказательство. B как модуль над A не имеет кручения. Согласно общей теории колец главных идеалов,

всякий конечно порожденный модуль без кручения над таким кольцом свободен. Совпадение его ранга со степенью $[L:K]$ очевидно.

Теорема 1 применяется к кольцу целых чисел $\mathbf{Z}$. Всякое конечное расширение поля рациональных чисел $\mathbf{Q}$ называется *числовым полем*. Целое замыкание кольца $\mathbf{Z}$ в числовом поле K называется кольцом *целых алгебраических чисел* этого поля и обозначается символом I_K, а иногда также символом $\mathfrak{o}_K$.

Предложение 8. *Пусть A — подкольцо кольца B, целого над A, S — мультипликативное подмножество кольца A. Тогда кольцо $S^{-1}B$ цело над $S^{-1}A$. Если A целозамкнуто, то и $S^{-1}A$ целозамкнуто.*

Доказательство. Пусть $x \in B$, $s \in S$ и M — конечно порожденный A-модуль, для которого $xM \subset M$. Тогда $S^{-1}M$ — конечно порожденный $S^{-1}A$-модуль, который отображается в себя при умножении на $s^{-1}x$, так что этот последний элемент цел над $S^{-1}A$. Для доказательства второго утверждения рассмотрим элемент x из поля частных кольца A, целый над кольцом $S^{-1}A$. Он удовлетворяет уравнению

$$x^n + \frac{b_{n-1}}{s_{n-1}} x^{n-1} + \ldots + \frac{b_0}{s_0} = 0,$$

где $b_i \in A$ и $s_i \in S$. Следовательно, существует такой элемент $s \in S$, для которого sx цел над A и, значит, принадлежит A. Тем самым, x принадлежит кольцу $S^{-1}A$.

Следствие. *Пусть B является целым замыканием кольца A в некотором расширении L поля частных A; тогда $S^{-1}B$ является целым замыканием кольца $S^{-1}A$ в L.*

§ 3. Простые идеалы

Пусть $\mathfrak{p}$ — простой идеал кольца A, $S = A \setminus \mathfrak{p}$. Для всякого кольца B, содержащего A, символом $B_{\mathfrak{p}}$ обозначим кольцо $S^{-1}B$.

Пусть кольцо B содержит A, $\mathfrak{p}$ — некоторый простой идеал в A и $\mathfrak{P}$ — простой идеал в B. Будем говорить,

что $\mathfrak{P}$ *лежит над* $\mathfrak{p}$, если $\mathfrak{P} \cap A = \mathfrak{p}$. В этом случае вложение

$$A \to B$$

индуцирует вложение факторколец

$$A/\mathfrak{p} \to B/\mathfrak{P}$$

и имеет место коммутативная диаграмма

$$\begin{array}{ccc} B & \to & B/\mathfrak{P} \\ \uparrow & & \uparrow \\ A & \to & A/\mathfrak{p} \end{array},$$

в которой горизонтальные стрелки означают канонические гомоморфизмы, а вертикальные — вложения.

Если кольцо B цело над A, то $B/\mathfrak{P}$ цело над $A/\mathfrak{p}$ (предложение 4).

Лемма Накаяма. *Пусть A — кольцо, $\mathfrak{a}$ — идеал, содержащийся во всех максимальных идеалах кольца A, M — конечно порожденный A-модуль. Если $\mathfrak{a}M = M$, то $M = 0$.*

Доказательство. Проведем индукцию по числу образующих модуля M. Пусть $w_1, \ldots, w_m$ — некоторая система образующих. Существует выражение вида

$$w_1 = a_1 w_1 + \ldots + a_m w_m,$$

где $a_i \in \mathfrak{a}$. Следовательно,

$$(1 - a_1) w_1 = a_2 w_2 + \ldots + a_m w_m.$$

Если бы элемент $1 - a_1$ не был обратим в A, он содержался бы в некотором максимальном идеале $\mathfrak{p}$. Так как, по предположению, $a_1 \in \mathfrak{p}$, мы имели бы противоречие. Следовательно, $1 - a_1$ обратим. Деля на него, получаем, что M порожден уже $m - 1$ элементами, что и завершает доказательство.

Предложение 9. *Пусть A — кольцо, $\mathfrak{p}$ — простой идеал, B — кольцо, содержащее A и целое над A. Тогда $\mathfrak{p}B \neq B$ и существует простой идеал $\mathfrak{P} \subset B$, лежащий над $\mathfrak{p}$.*

Доказательство. Мы знаем, что $B_\mathfrak{p}$ цело над $A_\mathfrak{p}$ и что $A_\mathfrak{p}$ представляет собой локальное кольцо с максимальным идеалом $\mathfrak{m}_\mathfrak{p}$. Очевидно, что

$$\mathfrak{p}B_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}B = \mathfrak{p}A_\mathfrak{p}B_\mathfrak{p} = \mathfrak{m}_\mathfrak{p}B_\mathfrak{p},$$

поэтому достаточно проверить наше первое утверждение в случае, когда A — локальное кольцо. Если бы идеал $\mathfrak{p}B$ совпадал с B, имело бы место представление вида

$$1 = a_1b_1 + \ldots + a_nb_n,$$

где $a_i \in \mathfrak{p}$ и $b_i \in B$. Положим $B_0 = A[b_1, \ldots, b_n]$. Тогда $\mathfrak{p}B_0 = B_0$, и кольцо B_0 в силу предложения 2 является конечно порожденным A-модулем. Следовательно, $B_0 = 0$, что невозможно.

Для доказательства второго утверждения вернемся к первоначальным обозначениям и рассмотрим следующую коммутативную диаграмму:

$$\begin{array}{ccc} B & \longrightarrow & B_\mathfrak{p} \\ \uparrow & & \uparrow \\ A & \longrightarrow & A_\mathfrak{p} \end{array},$$

в которой все стрелки означают вложения. Мы только что установили, что $\mathfrak{m}_\mathfrak{p}B_\mathfrak{p} \neq B_\mathfrak{p}$. Следовательно, идеал $\mathfrak{m}_\mathfrak{p}B_\mathfrak{p}$ содержится в некотором максимальном идеале $\mathfrak{M}$ кольца $B_\mathfrak{p}$ и, значит, пересечение $\mathfrak{M} \cap A_\mathfrak{p}$ содержит $\mathfrak{m}_\mathfrak{p}$. Поскольку $\mathfrak{m}_\mathfrak{p}$ максимален, то

$$\mathfrak{m}_\mathfrak{p} = \mathfrak{M} \cap A_\mathfrak{p}.$$

Положим $\mathfrak{P} = \mathfrak{M} \cap B$. Тогда $\mathfrak{P}$ — простой идеал кольца B. Рассматривая его пересечение с кольцом A и двигаясь двумя путями по коммутативной диаграмме, убеждаемся, что $\mathfrak{M} \cap A = \mathfrak{p}$ и, таким образом,

$$\mathfrak{P} \cap A = \mathfrak{p},$$

что и следовало доказать.

Замечание. *Пусть кольцо B цело над A, а $\mathfrak{b} \subset B$ — ненулевой идеал. Тогда и $\mathfrak{b} \cap A$ — ненулевой идеал.*

Для доказательства этого рассмотрим ненулевой элемент $b \in \mathfrak{b}$. Этот элемент удовлетворяет уравнению

$$b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0,$$

где $a_i \in A$, $a_0 \neq 0$. Но элемент a_0 принадлежит пересечению $\mathfrak{b} \cap A$.

Предложение 10. *Пусть A — подкольцо кольца B, и пусть B цело над A. Пусть $\mathfrak{P}$ — простой идеал кольца B, лежащий над простым идеалом $\mathfrak{p}$ кольца A. Он максимален в том и только том случае, когда $\mathfrak{p}$ максимален.*

Доказательство. Пусть $\mathfrak{p}$ максимален. Тогда $A/\mathfrak{p}$ — поле. Тем самым достаточно показать, что кольцо, целое над полем, является полем. Из элементарной теории полей хорошо известно, что если x цел над k, то кольцо $k[x]$ является полем и, следовательно, x обратим в этом кольце. Обратно, пусть идеал $\mathfrak{P}$ максимален в B. Тогда факторкольцо $B/\mathfrak{P}$ является полем, которое цело над кольцом $A/\mathfrak{p}$. Если бы $A/\mathfrak{p}$ не было полем, то в этом кольце имелся бы ненулевой максимальный идеал $\mathfrak{m}$. По предложению 9, существовал бы максимальный идеал $\mathfrak{M}$ кольца $B/\mathfrak{P}$, лежащий над $\mathfrak{m}$, что приводит к противоречию.

§ 4. Китайская теорема об остатках

Китайская теорема об остатках. *Пусть A — кольцо, $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ — такие идеалы, что $\mathfrak{a}_i + \mathfrak{a}_j = A$ при всех $i \neq j$. Для любого семейства $x_1, \ldots, x_n$ элементов кольца A существует такой элемент $x \in A$, что $x \equiv x_i \pmod{\mathfrak{a}_i}$ при всех i.*

Доказательство. Проведем индукцию по n. При $n = 2$ имеем

$$1 = a_1 + a_2,$$

где $a_i \in \mathfrak{a}_i$, так что достаточно положить $x = x_2a_1 + x_1a_2$.

Пусть теорема доказана для семейства из $n-1$ идеала. Для всякого i найдутся такие элементы $a_i \in \mathfrak{a}_i$ и $b_i \in \mathfrak{a}_i$, что

$$a_i + b_i = 1, \quad i \geqslant 2.$$

Произведение $\prod_{i=2}^{n}(a_i+b_i)$ равно 1 и лежит в идеале $\mathfrak{a}_1+\prod_{i=2}^{n}\mathfrak{a}_i$, так что $\mathfrak{a}_1+\prod_{i=2}^{n}\mathfrak{a}_i=A$. В силу справедливости теоремы при $n=2$, найдется такой элемент $y_1\in A$, что

$$y_1\equiv 1 \pmod{\mathfrak{a}_1},$$

$$y_1\equiv 0 \pmod{\prod_{i=2}^{n}\mathfrak{a}_i}.$$

Аналогично, найдутся такие элементы $y_2, \ldots, y_n$, что

$$y_j\equiv 1 \pmod{\mathfrak{a}_j}, \qquad y_j\equiv 0 \pmod{\mathfrak{a}_i}, \quad i\neq j.$$

Линейная комбинация $x=x_1y_1+\ldots+x_ny_n$ тогда удовлетворяет нашим требованиям.

Еще одно замечание в том же духе: для любого семейства идеалов $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ кольца A со свойством

$$\mathfrak{a}_1+\ldots+\mathfrak{a}_n=A$$

и для любого семейства положительных целых чисел $\nu_1, \ldots, \nu_n$ имеем

$$\mathfrak{a}_1^{\nu_1}+\ldots+\mathfrak{a}_n^{\nu_n}=A.$$

Доказательство тривиально; мы оставляем его в качестве упражнения.

§ 5. Расширения Галуа

Предложение 11. *Пусть A — кольцо, целозамкнутое в своем поле частных K. Пусть L — конечное расширение Галуа поля K с группой G. Пусть $\mathfrak{p}$ — максимальный идеал кольца A, а $\mathfrak{P}$, $\mathfrak{Q}$ — простые идеалы целого замыкания кольца A в поле L, лежащие над $\mathfrak{p}$. Тогда существует автоморфизм $\sigma\in G$, для которого $\sigma\mathfrak{P}=\mathfrak{Q}$.*

Доказательство. Предположим, что $\mathfrak{Q}\neq\sigma\mathfrak{P}$ при всех $\sigma\in G$. Тогда $\tau\mathfrak{Q}\neq\sigma\mathfrak{P}$ для любой пары элементов $\sigma,\tau\in G$. Следовательно, существует такой элемент $x\in B$, что

$$x\equiv 0 \pmod{\sigma\mathfrak{P}} \quad \text{при всех} \quad \sigma\in G,$$
$$x\equiv 1 \pmod{\sigma\mathfrak{Q}} \quad \text{при всех} \quad \sigma\in G$$

(воспользоваться китайской теоремой об остатках). Норма

$$N_K^L(x) = \prod_{\sigma \in G} \sigma x$$

принадлежит кольцу $B \cap K = A$, поскольку оно целозамкнуто, и, значит, лежит в идеале $\mathfrak{P} \cap A = \mathfrak{p}$. Но $x \notin \sigma\mathfrak{Q}$ при всех $\sigma \in G$, так что $\sigma x \notin \mathfrak{Q}$ при всех $\sigma \in G$. Это противоречит тому обстоятельству, что норма элемента x принадлежит пересечению $\mathfrak{p} = \mathfrak{Q} \cap A$.

Локализуя, можно избавиться от предположения, что $\mathfrak{p}$ — максимальный идеал; достаточно его простоты.

Следствие. *Пусть A — кольцо, целозамкнутое в своем поле частных K. Пусть E — конечное сепарабельное расширение поля K, а B — целое замыкание кольца A в E. Пусть $\mathfrak{p}$ — максимальный идеал в A. Тогда существует только конечное число простых идеалов кольца B, лежащих над $\mathfrak{p}$.*

Доказательство. Пусть L — наименьшее расширение Галуа поля K, содержащее E. Пусть $\mathfrak{Q}_1$, $\mathfrak{Q}_2$ — различные простые идеалы кольца B, лежащие над $\mathfrak{p}$, и $\mathfrak{P}_1$, $\mathfrak{P}_2$ — простые идеалы целого замыкания кольца A в поле L, лежащие над $\mathfrak{Q}_1$, $\mathfrak{Q}_2$ соответственно. Тогда $\mathfrak{P}_1 \neq \mathfrak{P}_2$. Тем самым наше утверждение достаточно проверить в случае, когда E — расширение Галуа поля K, а это немедленно вытекает из предложения 11.

Пусть кольцо A целозамкнуто в своем поле частных K, и пусть B — его целое замыкание в конечном расширении Галуа L с группой G. Тогда $\sigma B = B$ для всех $\sigma \in G$. Пусть $\mathfrak{p}$ — некоторый максимальный идеал кольца A, $\mathfrak{P}$ — максимальный идеал кольца B, лежащий над $\mathfrak{p}$. Обозначим символом $G_{\mathfrak{P}}$ подгруппу группы G, состоящую из тех автоморфизмов σ, для которых $\sigma\mathfrak{P} = \mathfrak{P}$. Группа $G_{\mathfrak{P}}$, естественно, действует на поле классов вычетов $B/\mathfrak{P}$ и оставляет подполе $A/\mathfrak{p}$ инвариантным. Всякому элементу $\sigma \in G_{\mathfrak{P}}$ мы можем поставить в соответствие некоторый автоморфизм σ' поля $B/\mathfrak{P}$ над $A/\mathfrak{p}$, и отображение

$$\sigma \longrightarrow \sigma'$$

индуцирует гомоморфизм группы $G_{\mathfrak{P}}$ в группу автоморфизмов поля $B/\mathfrak{P}$ над $A/\mathfrak{p}$.

Группа $G_{\mathfrak{P}}$ называется *группой разложения* идеала $\mathfrak{P}$. Ее инвариантное подполе мы будем обозначать символом L^d и называть полем *разложения* идеала $\mathfrak{P}$. Пусть B^d — целое замыкание кольца A в поле L^d, и пусть $\mathfrak{Q} = \mathfrak{P} \cap B^d$. Из предложения 11 следует, что $\mathfrak{P}$ — единственный простой идеал кольца B, лежащий над $\mathfrak{Q}$.

Пусть $G = \bigcup \sigma_j G_{\mathfrak{P}}$ — разложение группы G на смежные классы по подгруппе $G_{\mathfrak{P}}$. Тогда простые идеалы $\sigma_j\mathfrak{P}$ в точности составляют семейство различных простых идеалов кольца B, лежащих над $\mathfrak{p}$. В самом деле, для двух элементов $\sigma, \tau \in G$ имеем $\sigma\mathfrak{P} = \tau\mathfrak{P}$ в том и только том случае, когда $\tau^{-1}\sigma\mathfrak{P} = \mathfrak{P}$, т. е. когда $\tau^{-1}\sigma \in G_{\mathfrak{P}}$. Тем самым элементы τ, σ принадлежат одному и тому же классу $\bmod G_{\mathfrak{P}}$.

Очевидно, группой разложения простого идеала $\sigma\mathfrak{P}$ является группа $\sigma G_{\mathfrak{P}}\sigma^{-1}$.

Предложение 12. *L^d — наименьшее подполе E поля L, содержащее K и обладающее тем свойством, что $\mathfrak{P}$ — единственный простой идеал кольца B, лежащий над простым идеалом $\mathfrak{P} \cap E$ кольца $B \cap E$.*

Доказательство. Пусть E — поле, удовлетворяющее условию предложения, H — группа Галуа поля L над E. Положим $\mathfrak{q} = \mathfrak{P} \cap E$. По предложению 11, все простые идеалы кольца B, лежащие над $\mathfrak{q}$, сопряжены относительно H. Поскольку такой идеал единствен, именно $\mathfrak{P}$, группа H оставляет этот идеал инвариантным. Следовательно, $H \subset G_{\mathfrak{P}}$ и $E \supset L^d$. Но мы уже проверили, что само поле L^d обладает сформулированными свойствами.

Предложение 13. *В прежних обозначениях имеем $A/\mathfrak{p} = B^d/\mathfrak{Q}$ (изоморфизм определяется каноническим вложением $A/\mathfrak{p} \to B^d/\mathfrak{Q}$).*

Доказательство. Пусть σ — элемент группы G, не принадлежащий $G_{\mathfrak{P}}$. Тогда $\sigma\mathfrak{P} \neq \mathfrak{P}$ и $\sigma^{-1}\mathfrak{P} \neq \mathfrak{P}$. Положим

$$\mathfrak{Q}_\sigma = \sigma^{-1}\mathfrak{P} \cap B^d.$$

Тогда $\mathfrak{Q}_\sigma \neq \mathfrak{Q}$. Пусть x — произвольный элемент кольца B^d.

Тогда существует такой элемент y этого кольца, что

$$y \equiv x \pmod{\mathfrak{Q}},$$
$$y \equiv 1 \pmod{\mathfrak{Q}_\sigma}$$

для всех автоморфизмов σ группы G, не принадлежащих $G_{\mathfrak{P}}$. В частности,

$$y \equiv x \pmod{\mathfrak{P}},$$
$$y \equiv 1 \pmod{\sigma^{-1}\mathfrak{P}}$$

для всех σ, не принадлежащих $G_{\mathfrak{P}}$. Из второго сравнения следует, что

$$\sigma y \equiv 1 \pmod{\mathfrak{P}}$$

для всех $\sigma \notin G_{\mathfrak{P}}$. Норма элемента y из поля L^d в K является произведением y и различных множителей σy, $\sigma \notin G_{\mathfrak{P}}$. Таким образом,

$$N_K^{L^d}(y) \equiv x \pmod{\mathfrak{P}}.$$

Но эта норма принадлежит полю K и даже кольцу A, так как она является произведением элементов, целых над A. Следовательно, последнее сравнение имеет место по модулю $\mathfrak{Q}$, поскольку и x, и норма лежат в B^d. Это и есть утверждение, которое мы хотели доказать.

Для всякого элемента $x \in B$ обозначим символом x' его образ при гомоморфизме $B \to B/\mathfrak{P}$. Тогда σ' — тот автоморфизм поля $B/\mathfrak{P}$, для которого

$$\sigma' x' = (\sigma x)'.$$

Пусть $f(X)$ — многочлен с коэффициентами в кольце B. Обозначим через $f'(X)$ его естественный образ относительно описанного гомоморфизма. Именно если

$$f(X) = b_n X^n + \ldots + b_0,$$

то

$$f'(X) = b_n' X^n + \ldots + b_0'.$$

Предложение 14. *Пусть кольцо A целозамкнуто в своем поле частных K, и пусть B — его целое замыкание в конечном расширении Галуа L этого поля с группой G. Пусть $\mathfrak{p}$ — некоторый максимальный идеал кольца A, $\mathfrak{P}$ —*

максимальный идеал кольца B, лежащий над $\mathfrak{p}$. Тогда поле $B/\mathfrak{P}$ является нормальным расширением поля $A/\mathfrak{p}$, а отображение $\sigma \to \sigma'$ индуцирует некоторый гомоморфизм группы $G_{\mathfrak{P}}$ на группу Галуа поля $B/\mathfrak{P}$ над $A/\mathfrak{p}$.

Доказательство. Положим $B' = B/\mathfrak{P}$ и $A' = A/\mathfrak{p}$. Всякий элемент x' факторкольца B' является образом некоторого элемента $x \in B$. Предположим, что x' порождает некоторое сепарабельное подрасширение кольца B' над A'. Пусть f — неприводимый многочлен над полем K, корнем которого является x. Так как x цел над A, то коэффициенты f принадлежат A, и все остальные корни f целы над A. Тем самым многочлен $f(X)$ разлагается в кольце B на линейные множители

$$f(X) = \prod_{i=1}^{n} (X - x_i).$$

Но тогда

$$f'(X) = \prod_{i=1}^{n} (X - x_i'),$$

где все x_i' принадлежат кольцу B', так что многочлен f' разлагается на линейные множители в кольце B'. Так как из равенства $f(x) = 0$ следует равенство $f'(x') = 0$, кольцо B' нормально над A', и

$$[A'(x') : A'] \leqslant [K(x) : K] \leqslant [L : K].$$

Отсюда следует, что максимальное сепарабельное подрасширение кольца A' в B' имеет конечную степень над A', которая ограничена степенью $[L : K]$ (воспользоваться теоремой о примитивном элементе).

Остается проверить, что отображение $\sigma \to \sigma'$ определяет некоторый эпиморфизм группы $G_{\mathfrak{P}}$ на группу Галуа кольца B' над A'. С этой целью воспользуемся приемом, сводящим нашу задачу к случаю, когда $\mathfrak{P}$ — единственный простой идеал кольца B, лежащий над $\mathfrak{p}$. Этот прием состоит в замене кольца B кольцом B^d, что можно сделать, так как соответствующее поле классов вычетов при этом не меняется в силу предложения 13. Следовательно, для доказательства эпиморфности можно рас-

сматривать L^d в качестве основного поля. К этой ситуации мы и хотели свести задачу; будем считать, что $K = L^d$, $G = G_{\mathfrak{P}}$.

Пусть теперь $x \in B$ — такой элемент, что его образ x' порождает максимальное сепарабельное подрасширение кольца B' над A'. Пусть f — неприводимый многочлен над K, корнем которого является x. Всякий автоморфизм кольца B' переводит x' в некоторый корень многочлена f' и определяется этим корнем. Положим $x = x_1$, и пусть x_i — любой корень многочлена f. Существует такой элемент $\sigma \in G = G_{\mathfrak{P}}$, что $\sigma x = x_i$. Следовательно, $\sigma' x' = x_i'$. Тем самым автоморфизмы кольца B' над A', индуцированные элементами группы G, транзитивно действуют на множестве корней многочлена f'. Поэтому они индуцируют полную группу автоморфизмов поля классов вычетов, что и требовалось доказать.

Следствие 1. *Пусть A — кольцо, целозамкнутое в своем поле частных K. Пусть L — конечное расширение Галуа поля K, B — целое замыкание кольца A в поле L, $\mathfrak{p}$ — некоторый максимальный идеал кольца A и $\varphi : A \to A/\mathfrak{p}$ — канонический гомоморфизм. Пусть, наконец, ψ_1, ψ_2 — два гомоморфизма кольца B в алгебраическое замыкание поля $A/\mathfrak{p}$, продолжающее гомоморфизм φ. Тогда существует такой автоморфизм σ поля L над K, что*

$$\psi_1 = \psi_2 \circ \sigma.$$

Доказательство. Ядро отображений ψ_1, ψ_2 — простые идеалы кольца B, которые сопряжены в силу предложения 11. Следовательно, в группе Галуа G существует такой элемент τ, что отображения ψ_1 и $\psi_2 \circ \tau$ имеют одно и то же ядро. Поэтому, не теряя общности, можно считать, что уже ядра отображений ψ_1, ψ_2 совпадают и равны $\mathfrak{P}$. Это означает существование такого автоморфизма $\omega : \psi_1(B) \to \psi_2(B)$, что $\omega \circ \psi_1 = \psi_2$. В силу предложения 11 существует такой элемент $\sigma \in G_{\mathfrak{P}}$, что $\omega \circ \psi_1 = \psi_1 \circ \sigma$. Это доказывает требуемое.

Замечание. Во всех сформулированных утверждениях условие максимальности идеала $\mathfrak{p}$ можно заменить условием его простоты. Достаточно локализовать по $\mathfrak{p}$,

и все доказательства переносятся без изменений. Для приложений к числовым полям это несущественно, ибо все простые идеалы в этом случае максимальны.

Ядро рассмотренного выше отображения

$$G_{\mathfrak{P}} \longrightarrow G'_{\mathfrak{P}}$$

называется *группой инерции* идеала $\mathfrak{P}$. Она состоит из тех элементов группы $G_{\mathfrak{P}}$, которые индуцируют тривиальный автоморфизм поля классов вычетов. Поле инвариантных элементов для этой подгруппы называется *полем инерции* и обозначается символом L^t.

Следствие 2. *В условиях следствия* 1 *предположим еще, что* $\mathfrak{P}$ *— единственный простой идеал кольца* B, *лежащий над* $\mathfrak{p}$. *Пусть* $f(X)$ *— многочлен в кольце* $A[X]$ *со старшим коэффициентом* 1. *Предположим, что* f *неприводим в кольце* $K[X]$ *и что один из его корней лежит в кольце* B. *Тогда редуцированный многочлен* f' *является степенью некоторого неприводимого многочлена в* $A'[X]$.

Доказательство. По следствию 1, любые два корня многочлена f' сопряжены относительно некоторого автоморфизма кольца B' над A', так что f' не может разлагаться на взаимно простые множители. Поэтому f' является степенью неприводимого многочлена.

Следствие 2 известно под названием *леммы Гензеля*. Позже мы применим его к полным полям.

§ 6. Дедекиндовы кольца

Пусть $\mathfrak{o}$ — кольцо, K — его поле частных. *Дробным идеалом* кольца $\mathfrak{o}$ в поле K называется всякий $\mathfrak{o}$-модуль $\mathfrak{a}$, содержащийся в K, для которого существует такой элемент $c \in \mathfrak{o}$, $c \neq 0$, что $c\mathfrak{a} \subset \mathfrak{o}$. Если кольцо $\mathfrak{o}$ нетерово, из определения следует, что модуль $c\mathfrak{a}$, а значит, и $\mathfrak{a}$, конечно порожден.

Теорема 2. *Пусть* $\mathfrak{o}$ *— нетерово целозамкнутое кольцо, каждый ненулевой простой идеал которого максимален. Тогда всякий идеал кольца* $\mathfrak{o}$ *однозначно разлагается на простые идеалы, а ненулевые дробные идеалы образуют группу по умножению.*

Доказательство. Сначала мы докажем второе утверждение, следуя Ван дер Вардену.

(I) Пусть $\mathfrak{a} \neq 0$ — идеал в кольце $\mathfrak{o}$. Тогда существует произведение простых идеалов, которое содержится в $\mathfrak{a}$: $\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r \subset \mathfrak{a}$.

Пусть это не так; в силу нетеровости кольца $\mathfrak{o}$ существует ненулевой идеал $\mathfrak{a}$, максимальный во множестве идеалов, не содержащих произведение простых идеалов. Он не может быть простым. Следовательно, существуют такие элементы $b_1, b_2 \in \mathfrak{o}$, что $b_1, b_2 \in \mathfrak{a}$, но $b_1 \notin \mathfrak{a}$, $b_2 \notin \mathfrak{a}$. Положим $\mathfrak{a}_1 = (\mathfrak{a}, b_1)$ и $\mathfrak{a}_2 = (\mathfrak{a}, b_2)$. Тогда $\mathfrak{a}_1\mathfrak{a}_2 \subset \mathfrak{a}$ и $\mathfrak{a}_1 \neq \mathfrak{a}$, $\mathfrak{a}_2 \neq \mathfrak{a}$. Так как $\mathfrak{a}$ максимален в описанном множестве, некоторые произведения простых идеалов содержатся в $\mathfrak{a}_1$ и в $\mathfrak{a}_2$. Объединенное произведение тогда содержится в $\mathfrak{a}$, что приводит к противоречию.

(II) Всякий максимальный идеал $\mathfrak{p}$ обратим.

Пусть $\mathfrak{p}^{-1}$ — множество тех элементов $x \in K$, для которых $x\mathfrak{p} \subset \mathfrak{o}$. Тогда $\mathfrak{p}^{-1} \supset \mathfrak{o}$. Мы утверждаем, что $\mathfrak{p}^{-1} \neq \mathfrak{o}$. Действительно, пусть $a \in \mathfrak{p}$, $a \neq \mathfrak{o}$. Рассмотрим такое наименьшее число r, для которого существует произведение

$$\mathfrak{p}_1 \ldots \mathfrak{p}_r \subset (a) \subset \mathfrak{p}.$$

Тогда один из идеалов $\mathfrak{p}_i$, скажем $\mathfrak{p}_1$, содержится в $\mathfrak{p}$, а значит, и совпадает с $\mathfrak{p}$, поскольку всякий простой идеал максимален. Далее,

$$\mathfrak{p}_2 \ldots \mathfrak{p}_r \not\subset (a)$$

и, следовательно, существует такой элемент $b \in \mathfrak{p}_2 \ldots \mathfrak{p}_r$, что $b \notin (a)$. Но $b\mathfrak{p} \subset (a)$, так что $ba^{-1}\mathfrak{p} \subset \mathfrak{o}$ и, стало быть, $ba^{-1} \in \mathfrak{p}^{-1}$. А так как $b \notin a\mathfrak{o}$, то и $ba^{-1} \notin \mathfrak{o}$, что доказывает наше утверждение.

Итак, $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset \mathfrak{o}$. Так как идеал $\mathfrak{p}$ максимален, то либо $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$, либо $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}$. В первом случае всякий элемент идеала $\mathfrak{p}^{-1}$ при умножении переводит в себя конечно порожденный $\mathfrak{o}$-модуль $\mathfrak{p}$, что невозможно, так как $\mathfrak{p}^{-1} \not\subset \mathfrak{o}$, а кольцо $\mathfrak{o}$ целозамкнуто. Следовательно, $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}$.

(III) Для каждого ненулевого идеала существует обратный к нему дробный идеал.

Пусть это не так. Тогда существует максимальный необратимый идеал $\mathfrak{a}$. Мы уже убедились, что он не

может быть максимальным. Следовательно, $\mathfrak{a} \subset \mathfrak{p}$, $\mathfrak{a} \neq \mathfrak{p}$ для некоторого максимального идеала $\mathfrak{p}$. Имеем

$$\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1} \subset \mathfrak{a}\mathfrak{a}^{-1} \subset \mathfrak{o}.$$

Так как идеал $\mathfrak{a}$ конечно порожден, равенство $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$ не может иметь места, ибо идеал $\mathfrak{p}^{-1}$ не цел над $\mathfrak{o}$. Следовательно, идеал $\mathfrak{a}\mathfrak{p}^{-1}$ больше, чем $\mathfrak{a}$, и потому имеет обратный, который, будучи умножен на $\mathfrak{p}$, даст обратный идеал для $\mathfrak{a}$. Противоречие.

(IV) Пусть $\mathfrak{a}$ — некоторый ненулевой идеал, а $\mathfrak{c}$ — такой дробный идеал, что $\mathfrak{a}\mathfrak{c} = \mathfrak{o}$. Тогда $\mathfrak{c} = \mathfrak{a}^{-1}$ (множество тех элементов $x \in K$, для которых $x\mathfrak{a} \subset \mathfrak{o}$).

Очевидно, что $\mathfrak{c} \subset \mathfrak{a}^{-1}$. Обратно, если $x\mathfrak{a} \subset \mathfrak{o}$, то $x\mathfrak{a}\mathfrak{c} \subset \mathfrak{c}$ и, значит, $x \in \mathfrak{c}$, потому что $\mathfrak{a}\mathfrak{c} = \mathfrak{o}$.

Наконец, покажем, что всякий ненулевой дробный идеал обратим. В самом деле, пусть $\mathfrak{a}$ — ненулевой дробный идеал. Тогда существует такой элемент $c \in \mathfrak{o}$, что $c\mathfrak{a} \subset \mathfrak{o}$, и идеал $c\mathfrak{a}$ обратим. Пусть $c\mathfrak{a}\mathfrak{b} = \mathfrak{o}$. Тогда $c\mathfrak{b} = \mathfrak{a}^{-1}$. Это доказывает, что ненулевые дробные идеалы образуют группу.

Теперь установим однозначность разложения на простые идеалы.

Заметим сначала, что всякий ненулевой идеал $\mathfrak{a}$ равен произведению простых идеалов. Иначе существовал бы идеал $\mathfrak{a}$, максимальный во множестве идеалов, не обладающий этим свойством; он не прост, так что $\mathfrak{a} \subset \mathfrak{p}$ и $\mathfrak{a} \neq \mathfrak{p}$, где $\mathfrak{p}$ — некоторый простой идеал. Тогда $\mathfrak{a}\mathfrak{p}^{-1} \subset \mathfrak{o}$ и $\mathfrak{a}\mathfrak{p}^{-1} \supset \mathfrak{a}$, причем включение строгое. Поэтому идеал $\mathfrak{a}\mathfrak{p}^{-1}$ разлагается на простые идеалы; добавив $\mathfrak{p}$, получим некоторое разложение идеала $\mathfrak{a}$.

Пусть даны дробные идеалы $\mathfrak{a}$, $\mathfrak{b}$. Запись $\mathfrak{a} \mid \mathfrak{b}$ означает, что существует идеал $\mathfrak{c}$, для которого $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$. Это отношение равносильно включению $\mathfrak{a} \supset \mathfrak{b}$, так как можно положить $\mathfrak{c} = \mathfrak{a}^{-1}\mathfrak{b}$.

Из определения простого идеала вытекает, что если $\mathfrak{p} \mid \mathfrak{a}\mathfrak{b}$, то либо $\mathfrak{p} \mid \mathfrak{a}$, либо $\mathfrak{p} \mid \mathfrak{b}$. (В самом деле, из включения $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$ следует, что либо $\mathfrak{a} \subset \mathfrak{p}$, либо $\mathfrak{b} \subset \mathfrak{p}$.) Поэтому, рассматривая два разложения на простые идеалы

$$\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_s,$$

мы можем заключить, что $\mathfrak{p}_1$ делит правое произведение,

тем самым делит один из его сомножителей, скажем $\mathfrak{q}_i$, а значит, совпадает с $\mathfrak{q}_i$. Умножая на $\mathfrak{p}_1^{-1}$ обе стороны равенства, по индукции устанавливаем, что $r=s$ и что простые множители слева и справа совпадают с точностью до перестановки.

Пусть $\mathfrak{a}$ — ненулевой дробный идеал, $c\in\mathfrak{o}$ — такой ненулевой элемент, что $c\mathfrak{a}\subset\mathfrak{o}$. Тогда $(c)=\mathfrak{p}_1\dots\mathfrak{p}_r$ и $c\mathfrak{a}=\mathfrak{q}_1\dots\mathfrak{q}_s$. Поэтому $\mathfrak{a}$ представляется в виде

$$\mathfrak{a}=\frac{\mathfrak{q}_1\dots\mathfrak{q}_s}{\mathfrak{p}_1\dots\mathfrak{p}_r}$$

(мы пишем $1/\mathfrak{p}$ вместо $\mathfrak{p}^{-1}$). Если сократить все простые идеалы, входящие и в числитель, и в знаменатель, получившееся разложение будет определяться однозначно.

Кольцо, удовлетворяющее условиям теоремы 2, называется *дедекиндовым кольцом*. Кольцо целых алгебраических чисел в числовом поле K является дедекиндовым, потому что оно удовлетворяет всем трем условиям.

В дальнейшем все дробные идеалы мы будем считать ненулевыми, если противное не оговорено явно.

Пусть A — дедекиндово кольцо, $\mathfrak{a}$ — дробный идеал. Он представляется в виде

$$\mathfrak{a}=\coprod_{\mathfrak{p}}\mathfrak{p}^{r_\mathfrak{p}},$$

где $r_\mathfrak{p}$ — целые числа, из которых все, кроме конечного числа, равны нулю. Число $r_\mathfrak{p}$ называется *порядком* идеала $\mathfrak{a}$ относительно $\mathfrak{p}$. Если $r_\mathfrak{p}>0$, будем говорить, что $\mathfrak{p}$ является *нулем* идеала $\mathfrak{a}$; если $r_\mathfrak{p}<0$ — *полюсом*.

Пусть α — ненулевой элемент поля частных кольца A. Мы можем образовать дробный идеал $(\alpha)=A\alpha$ и применить понятия порядка, нуля и полюса к элементу α.

Пусть $\mathfrak{a}$, $\mathfrak{b}$ — дробные идеалы. Очевидно, что $\mathfrak{a}\supset\mathfrak{b}$ в том и только том случае, когда $\operatorname{ord}_\mathfrak{p}\mathfrak{a}\leqslant\operatorname{ord}_\mathfrak{p}\mathfrak{b}$ для всех простых идеалов $\mathfrak{p}$. Тем самым получается критерий для принадлежности элемента α к дробному идеалу $\mathfrak{a}$ в терминах порядков (рассмотреть идеал $\mathfrak{b}=(\alpha)$). Все это немедленно показывает, что для любых двух дробных идеалов

$\mathfrak{a}$, $\mathfrak{b}$ имеем

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}.$$

Если $\operatorname{ord}_{\mathfrak{p}}\alpha = 0$, элемент α называется *единицей* относительно $\mathfrak{p}$. В этом случае элемент α является единицей в локальном кольце $A_{\mathfrak{p}}$.

В дальнейшем все простые идеалы мы будем считать ненулевыми, если противное не оговорено явно.

Предложение 15. *Пусть $\mathfrak{o}$ — дедекиндово кольцо с конечным числом простых идеалов. Тогда $\mathfrak{o}$ — кольцо главных идеалов.*

Доказательство. Пусть $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ — все простые идеалы. Для всякого идеала

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \ldots \mathfrak{p}_s^{r_s} \neq 0$$

выберем по элементу $\pi_i \in \mathfrak{p}_i$, $\pi_i \notin \mathfrak{p}_i^2$, и найдем такой элемент $\alpha \in \mathfrak{o}$, что

$$\alpha \equiv \pi_i^{r_i} \pmod{\mathfrak{b}},$$

где $\mathfrak{b}$ — произведение всех простых идеалов в достаточно большой степени. Рассматривая разложение идеала, порожденного элементом α,

$$(\alpha) = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_s^{e_s},$$

немедленно убеждаемся, что $e_i = r_i$ для всех i и, следовательно, $\mathfrak{a} = (\alpha)$.

Предложение 16. *Пусть A — дедекиндово кольцо, S — его мультипликативное подмножество. Тогда кольцо $S^{-1}A$ тоже дедекиндово. Отображение*

$$\mathfrak{a} \rightsquigarrow S^{-1}\mathfrak{a}$$

определяет гомоморфизм группы дробных идеалов кольца A на группу дробных идеалов кольца $S^{-1}A$, а его ядро состоит из тех дробных идеалов кольца A, которые пересекаются с S.

Доказательство. Если $\mathfrak{p}$ пересекается с S, то $S_{\mathfrak{p}}^{-1} = S^{-1}A$, потому что $1 \in S_{\mathfrak{p}}^{-1}$. Для любых двух

идеалов $\mathfrak{a}$, $\mathfrak{b} \subset A$ имеем

$$S^{-1}(\mathfrak{ab}) = (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b}),$$

так что операция S^{-1} индуцирует гомоморфизм группы (дробных) идеалов.

Если $S^{-1}\mathfrak{a} = S^{-1}A$, то $1 = \alpha/s$ для некоторых элементов $\alpha \in \mathfrak{a}$ и $s \in S$. Поэтому $\alpha = s$ и $\mathfrak{a}$ пересекается с S. Это доказывает утверждение о ядре гомоморфизма.

Наше отображение эпиморфно, потому что, как было показано в § 1, всякий идеал кольца $S^{-1}A$ имеет вид $S^{-1}\mathfrak{a}$, где $\mathfrak{a}$ — некоторый идеал кольца A. Это верно, разумеется, и для дробных идеалов. Наше предложение доказано.

Главным дробным идеалом мы будем называть дробный идеал вида αA, порожденный единственным элементом α поля частных кольца A. Мы будем считать, что $\alpha \neq 0$, если противное не оговорено явно.

Пусть A — дедекиндово кольцо. Факторгруппа всех дробных идеалов по модулю подгруппы *главных идеалов* (ненулевых) называется *группой классов идеалов* кольца A.

Предложение 17. *Пусть A — дедекиндово кольцо, группа классов идеалов которого конечна. Пусть $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ — дробные идеалы, представляющие все классы, и пусть b — ненулевой элемент кольца A, лежащий в пересечении идеалов $\mathfrak{a}_i$. Пусть S — мультипликативное подмножество кольца A, порожденное степенями элемента b. Тогда $S^{-1}A$ — кольцо главных идеалов.*

Доказательство. Все идеалы $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ отображаются в единичный идеал гомоморфизмом S^{-1}, описанным в предложении 16. Так как всякий идеал кольца A равен произведению одного из идеалов $\mathfrak{a}_i$ на главный идеал, наш результат вытекает из эпиморфности гомоморфизма в предложении 16.

Если два дробных идеала $\mathfrak{a}$, $\mathfrak{b}$ принадлежат одному и тому же классу, мы пишем

$$\mathfrak{a} \sim \mathfrak{b}$$

и называем их *линейно эквивалентными*. Очевидно, что всякий дробный идеал линейно эквивалентен некоторому идеалу.

Позже мы покажем, что условие предложения 17 выполняется для кольца целых чисел поля алгебраических чисел.

7. Дискретно нормированные кольца

Дискретно нормированным кольцом $\mathfrak{o}$ называется кольцо главных идеалов, имеющее единственный (ненулевой) простой идеал $\mathfrak{m}$. Такое кольцо локально. Образующий элемент π идеала $\mathfrak{m}$ является единственным неприводимым элементом кольца $\mathfrak{o}$ (с точностью до единицы, разумеется), т. е. единственным простым элементом, так как всякий простой элемент порождает простой идеал. Поэтому в рассматриваемом случае однозначность разложения, имеющая место в любом кольце главных идеалов, принимает особенно простой вид: всякий ненулевой элемент $\alpha \in \mathfrak{o}$ представляется в форме

$$\alpha = \pi^r u,$$

где r — целое число, u — единица в $\mathfrak{o}$.

Всякое дискретно нормированное кольцо — дедекиндово, а всякое дедекиндово кольцо с единственным максимальным идеалом дискретно нормировано. Пусть A — дедекиндово кольцо, $\mathfrak{p}$ — простой идеал кольца A. Тогда $A_\mathfrak{p}$ — дискретно нормированное кольцо, ибо $A_\mathfrak{p} = S^{-1}A$, где $S = A \setminus \mathfrak{p}$ (ср. предложение 16).

Так как все идеалы дискретно нормированного кольца главные, все они являются степенями максимального идеала.

При доказательстве различных результатов о дедекиндовых кольцах часто оказывается полезным производить локализацию относительно одного простого идеала, что приводит к дискретно нормированному кольцу. Примером может служить следующее предложение.

Предложение 18. *Пусть A — дедекиндово кольцо, M, N — два A-модуля. Для всякого простого идеала $\mathfrak{p} \subset A$*

положим $S_\mathfrak{p} = A \setminus \mathfrak{p}$. *Если* $S_\mathfrak{p}^{-1}M \subset S_\mathfrak{p}^{-1}N$ *для всех* $\mathfrak{p}$, *то* $M \subset N$.

Доказательство. Пусть $a \in M$. Для всякого $\mathfrak{p}$ существуют такие элементы $x_\mathfrak{p} \in N$ и $s_\mathfrak{p} \in S_\mathfrak{p}$, что $a = x_\mathfrak{p}/s_\mathfrak{p}$. Пусть $\mathfrak{b}$ — идеал, порожденный всеми $s_\mathfrak{p}$. Это единичный идеал, так что

$$1 = \sum y_\mathfrak{p} s_\mathfrak{p},$$

где $y_\mathfrak{p} \in A$, причем только конечное число элементов $y_\mathfrak{p}$ отлично от нуля. Поэтому

$$a = \sum y_\mathfrak{p} s_\mathfrak{p} a = \sum y_\mathfrak{p} x_\mathfrak{p},$$

так что $a \in N$, что и требовалось доказать.

Всякое дискретно нормированное кольцо A является кольцом главных идеалов, так что любой конечно порожденный A-модуль без кручения M свободен. Если его ранг равен n, а $\mathfrak{p}$ — простой идеал кольца A, то $M/\mathfrak{p}M$ — свободный модуль ранга n над $A/\mathfrak{p}A$.

Предложение 19. *Пусть* A — *локальные кольцо,* M — *свободный модуль ранга* n *над* A. *Пусть* $\mathfrak{p}$ — *максимальный идеал кольца* A. *Тогда* $M/\mathfrak{p}M$ — *векторное пространство размерности* n *над* $A/\mathfrak{p}$.

Доказательство. Рассмотрим базис $x_1, \ldots, x_n$ модуля M над A. Если его элементы линейно зависимы $\bmod \mathfrak{p}$, то существует соотношение вида

$$\sum a_i x_i \in \mathfrak{p}M,$$

где $a_i \in A$ и по крайней мере один из коэффициентов a_i, скажем a_1, не принадлежит $\mathfrak{p}$. Деля на a_1, получаем, что $x_1 \in Ax_2 + \ldots + Ax_n + \mathfrak{p}M$. Положим

$$N = M/(Ax_2 + \ldots + Ax_n).$$

Тогда $\mathfrak{p}N = N$, так что $N = 0$ в силу леммы Накаяма — противоречие.

Пусть теперь A — дедекиндово кольцо, K — его поле частных, L — конечное сепарабельное расширение поля K, B — целое замыкание кольца A в L. Для всякого простого

идеала $\mathfrak{p}$ имеет место разложение

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r} \quad (e_i \geqslant 1)$$

на простые идеалы кольца B. Очевидно, что простой идеал $\mathfrak{P} \subset B$ входит в это разложение тогда и только тогда, когда он лежит над $\mathfrak{p}$.

Пусть $S = A \setminus \mathfrak{p}$; применяя к этому разложению операцию S^{-1}, получаем разложение идеала $S^{-1}\mathfrak{p}B$ в кольце $S^{-1}B$. Простые идеалы $S^{-1}\mathfrak{P}_i$ остаются различными.

Число e_i называется *индексом ветвления* простого идеала $\mathfrak{P}_i$ над $\mathfrak{p}$ и обозначается иногда символом $e(\mathfrak{P}_i/\mathfrak{p})$. Если A — локальное кольцо, то $\mathfrak{p} = (\pi)$ — главный идеал (предложение 15). Пусть S_i — дополнение к $\mathfrak{P}_i$ в кольце B, и пусть $B_i = S_i^{-1}B = B_{\mathfrak{P}_i}$. Тогда $\mathfrak{P}_i$ — главный идеал, порожденный элементом π_i, и

$$\mathfrak{p}B_i = \pi B_i = (\pi_i^{e_i}).$$

Предупреждение: кольцо B_i не обязательно цело над $A_\mathfrak{p}$. Оно цело в том и только том случае, когда в кольце B существует лишь один простой идеал, лежащий над $\mathfrak{p}$. Докажите это в качестве упражнения.

Пусть $\mathfrak{J}(A)$ — группа дробных идеалов дедекиндова кольца A; значения K, L, B те же, что и выше. Имеет место естественное вложение

$$\mathfrak{J}(A) \to \mathfrak{J}(B),$$

определенное отображением $\mathfrak{a} \rightsquigarrow \mathfrak{a}B$. Мы введем сейчас некоторый гомоморфизм в обратном направлении.

Пусть $\mathfrak{P} \subset B$ лежит над $\mathfrak{p}$; символом $f_\mathfrak{P}$ или $f(\mathfrak{P}/\mathfrak{p})$ мы будем обозначать степень расширения $B/\mathfrak{P}$ над $A/\mathfrak{p}$; назовем ее *степенью поля классов вычетов*. Назовем *нормой* $N_K^L(\mathfrak{P})$ идеала $\mathfrak{P}$ идеал $\mathfrak{p}^{f_\mathfrak{P}}$ и распространим отображение N_K^L на всю группу дробных идеалов по мультипликативности.

Предложение 20. *Пусть A — дедекиндово кольцо, K — его поле частных, $K \subset E \subset L$ — его конечные сепарабельные расширения, $A \subset B \subset C$ — башня целых замыканий кольца A в полях E и L. Пусть $\mathfrak{p}$ — простой идеал кольца A, $\mathfrak{q}$ — некоторый простой идеал кольца B,*

лежащий над $\mathfrak{p}$, *а* $\mathfrak{P}$ — *некоторый простой идеал кольца* C, *лежащий над* $\mathfrak{q}$. *Тогда*

$$e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{q})\, e(\mathfrak{q}/\mathfrak{p}),$$
$$f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{q})\, f(\mathfrak{q}/\mathfrak{p}).$$

Доказательство. Очевидно.

Из предложения 20 вытекает, что норма транзитивна, т. е. что для всякого дробного идеала $\mathfrak{c}$ кольца C

$$N_K^E N_E^L(\mathfrak{c}) = N_K^L(\mathfrak{c}).$$

Предложение 21. *Пусть* A — *дедекиндово кольцо,* K — *его поле частных,* L — *конечное сепарабельное расширение поля* K, B — *целое замыкание кольца* A *в поле* L. *Пусть* $\mathfrak{p}$ — *простой идеал кольца* A. *Тогда*

$$[L:K] = \sum_{\mathfrak{P}\mid\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}.$$

Доказательство. Локализуем относительно идеала $\mathfrak{p}$, умножая A и B на $S_{\mathfrak{p}}^{-1}$; задача сводится к случаю, когда A — дискретно нормированное кольцо. В этом случае B — свободный модуль ранга $n = [L:K]$ над A, так что $B/\mathfrak{p}B$ — векторное пространство размерности n над $A/\mathfrak{p}$.

Пусть $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r}$. Так как $\mathfrak{P}_i^{e_i} \supset \mathfrak{p}B$ для каждого i, то определен гомоморфизм

$$B \to B/\mathfrak{p}B \to B/\mathfrak{P}_i^{e_i}$$

и тем самым гомоморфизм в прямую сумму

$$B \to B/\mathfrak{p}B \to \prod_{i=1}^{r} B/\mathfrak{P}_i^{e_i}.$$

Каждое кольцо $B/\mathfrak{P}_i^{e_i}$ можно рассматривать как векторное пространство над $A/\mathfrak{p}$; то же относится ко всей прямой сумме. Ядро нашего гомоморфизма состоит из тех элементов кольца B, которые принадлежат всем идеалам $\mathfrak{P}_i^{e_i}$ и, следовательно, идеалу $\mathfrak{p}B$. Кроме того, в силу китайской теоремы об остатках этот гомоморфизм эпиморфен. Очевидно, он является $A/\mathfrak{p}$-гомоморфизмом, так что $B/\mathfrak{p}B$ — пространство, $A/\mathfrak{p}$-изоморфное построенной прямой сумме.

Вычислим теперь размерность пространства $B/\mathfrak{P}^e$ ($\mathfrak{P}$ — один из идеалов $\mathfrak{P}_i$, а $e=e_i$).

Пусть Π — образующий элемент идеала $\mathfrak{P} \subset B$. (В силу предложения 15, $\mathfrak{P}$ — главный идеал.) Пусть $j \geqslant 1$ — целое число. Группу $\mathfrak{P}^j/\mathfrak{P}^{j+1}$ можно рассматривать как $A/\mathfrak{p}$-пространство, потому что $\mathfrak{p}\mathfrak{P}^j \subset \mathfrak{P}^{j+1}$. Умножение на Π^j индуцирует отображение

$$B/\mathfrak{P} \longrightarrow \mathfrak{P}^j/\mathfrak{P}^{j+1}.$$

Очевидно, оно является $A/\mathfrak{p}$-гомоморфизмом, который одновременно мономорфен и эпиморфен. Следовательно, пространства $B/\mathfrak{P}$ и $\mathfrak{P}^j/\mathfrak{P}^{j+1}$ $A/\mathfrak{p}$-изоморфны.

Рассмотрим композиционный ряд $A/\mathfrak{p}$-пространства $B/\mathfrak{P}^e$, связанный с цепочкой

$$B \supset \mathfrak{P} \supset \mathfrak{P}^2 \supset \ldots \supset \mathfrak{P}^e.$$

$A/\mathfrak{p}$-размерность пространства $B/\mathfrak{P}$, по определению, равна $f_{\mathfrak{P}}$. Тем самым $A/\mathfrak{p}$-размерность пространства $B/\mathfrak{P}^e$ равна $e_{\mathfrak{P}}f_{\mathfrak{P}}$, что доказывает наше утверждение. Если $e_{\mathfrak{P}}=f_{\mathfrak{P}}=1$ для всех $\mathfrak{P}/\mathfrak{p}$, мы говорим, что идеал $\mathfrak{p}$ *вполне распадается* в поле L. В этом случае ровно $[L:K]$ простых идеалов кольца B лежат над $\mathfrak{p}$.

Разумеется, предложение 21 можно доказать также в терминах абсолютных значений и нормирований, как в [7, гл. I]. Мы привели этот результат здесь, чтобы показать стилистическую разницу между двумя подходами к теории.

Следствие 1. *Пусть $\mathfrak{a}$ — дробный идеал кольца A. Тогда*

$$N_K^L(\mathfrak{a}B) = \mathfrak{a}^{[L:K]}.$$

Доказательство. Очевидно.

Следствие 2. *Предположим, что L — расширение Галуа поля K. Тогда индексы $e_{\mathfrak{P}}$ равны одному и тому же числу e (для всех $\mathfrak{P} \mid \mathfrak{p}$), а степени $f_{\mathfrak{P}}$ — одному и тому же числу f (для всех $\mathfrak{P} \mid \mathfrak{p}$), так что если*

$$\mathfrak{p}B = (\mathfrak{P}_1 \ldots \mathfrak{P}_r)^e,$$

$$efr = [L:K].$$

Доказательство. Все простые идеалы $\mathfrak{P}$, лежащие над $\mathfrak{p}$, сопряжены между собой, и, следовательно, все индексы ветвления и степени полей классов вычетов совпадают. Последнее равенство очевидно.

Следствие 3. *Пусть снова L — расширение Галуа над K с группой G, и пусть $\mathfrak{P}$ — простой идеал кольца B, лежащий над A. Тогда*

$$N_K^L\mathfrak{P}\cdot B=\prod_{\sigma\in G}\sigma\mathfrak{P}=(\mathfrak{P}_1\ \dots\ \mathfrak{P}_r)^{ef},$$

где числа e, f, r имеют те же значения, что и в следствии 2, а идеал слева рассматривается как элемент группы $\mathfrak{J}(B)$. Число ef равно порядку группы разложения идеала $\mathfrak{P}$, а число e — порядку группы инерции.

Доказательство. Группа G транзитивно действует на множество простых идеалов кольца B, лежащих над $\mathfrak{p}$, и порядок группы $G_{\mathfrak{P}}$ равен порядку стационарной подгруппы. Предложение 14 § 5 делает наши утверждения очевидными.

Предложение 22. *Пусть A — дедекиндово кольцо, K — его поле частных, E — конечное сепарабельное расширение поля K, B — целое замыкание кольца A в поле E. Пусть $\mathfrak{b}$ — главный дробный идеал кольца B, $\mathfrak{b}=(\beta)$, $\beta\neq 0$. Тогда*

$$N_K^E\mathfrak{b}=(N_K^E(\beta)),$$

где норма слева — это норма дробного идеала, определенная выше, а норма справа — обычная норма элемента поля E.

Доказательство. Пусть L — наименьшее расширение Галуа поля K, содержащее E. Нормальное отображение из L в E идеала $\mathfrak{b}$ и элемента β состоит в возведении того и другого в степень $[L:E]$. Так как наше утверждение относится к равенству дробных идеалов, достаточно доказать его в случае, когда L — расширение Галуа над K. Но тогда оно немедленно вытекает из следствия 3.

Предложение 23. *Пусть A — дискретно нормированное кольцо, K — его поле частных, L — конечное сепарабельное расширение поля K, B — целое замыкание кольца A в поле L. Предположим, что существует единственный простой идеал $\mathfrak{P}$ кольца B, лежащий над максимальным идеалом $\mathfrak{p}$ кольца A. Пусть β — элемент кольца B, класс вычетов которого $\bmod \mathfrak{P}$ порождает поле $B/\mathfrak{P}$ над $A/\mathfrak{p}$, и пусть Π — элемент кольца B, имеющий порядок 1 относительно $\mathfrak{P}$. Тогда $A[\beta, \Pi] = B$.*

Доказательство. Пусть $C = A[\beta, \Pi]$; C можно рассматривать как подмодуль A-модуля B. В силу леммы Накаяма в применении к фактормодулю B/C, достаточно проверить, что

$$\mathfrak{p}B + C = B.$$

Но $\mathfrak{p}B = \mathfrak{P}^e$, а произведения $\beta^i\Pi^j$ порождают пространство $B/\mathfrak{P}^e$ над полем $A/\mathfrak{p}$ — это проверяется так же, как в доказательстве предложения 21. Тем самым всякий элемент $x \in B$ сравним с линейной комбинацией вида

$$x \equiv \sum c_{ij}\beta^i\Pi^j \pmod{\mathfrak{p}B},$$

где $c_{ij} \in A$. Это доказывает наше утверждение.

Наконец, обобщая рассуждения, использованные в доказательстве предложения 21, получаем следующий результат.

Предложение 24. *Пусть A — дедекиндово кольцо, $\mathfrak{a}$ — ненулевой идеал. Положим $n_\mathfrak{p} = \operatorname{ord}_\mathfrak{p} \mathfrak{a}$. Тогда каноническое отображение*

$$A \to \prod_\mathfrak{p} A/\mathfrak{p}^{n_\mathfrak{p}}$$

индуцирует изоморфизм факторкольца $A/\mathfrak{a}$ с произведением справа.

Доказательство. Эпиморфность отображения следует из китайской теоремы об остатках; то, что ядро совпадает с $\mathfrak{a}$, очевидно.

Следствие. *Пусть факторкольцо $A/\mathfrak{p}$ конечно для всякого простого идеала $\mathfrak{p}$. Обозначим символом $\mathbf{N}\mathfrak{a}$ число элементов в кольце классов вычетов $A/\mathfrak{a}$. Тогда*

$$\mathbf{N}\mathfrak{a} = \prod_{\mathfrak{p}} (\mathbf{N}\mathfrak{p})^{n_{\mathfrak{p}}}.$$

Отметим еще, что функцию $\mathbf{N}$ можно продолжить по мультипликативности на все дробные идеалы.

Глава II

ПОПОЛНЕНИЯ

В этой главе вводятся пополнения числовых полей относительно $\mathfrak{p}$-адических топологий, а также топологий, индуцированных вложениями числового поля в поле вещественных или комплексных чисел.

В книге [7] этот вопрос изучался с точки зрения теории нормирований и был изложен в законченном виде.

В § 3 мы изучим грубую структуру полных полей. В § 4 и 5 изложены основные сведения относительно неразветвленных и слабо разветвленных расширений. По поводу теории высшего ветвления мы отсылаем читателя к книге Артина — Тейта [3]. В § 4 и 5 мы занимаемся полными дедекиндовыми кольцами. Мы вводим понятия неразветвленного, слабо разветвленного и вполне разветвленного идеала $\mathfrak{P}$ над $\mathfrak{p}$. Эти понятия можно определить и глобально, так как они зависят лишь от индекса ветвления и степени поля классов вычетов. Однако в локальном случае они применимы также к расширениям полей, потому что в каждом конечном расширении основного поля K имеется лишь один простой идеал $\mathfrak{P}$, лежащий над $\mathfrak{p}$.

§ 1. Определения и пополнения

Пусть K — поле. *Нормированием* поля K называется вещественнозначная функция v на K, удовлетворяющая следующим трем условиям:

Н1. $v(x) \geqslant 0$; $v(x) = 0$ в том и только том случае, когда $x = 0$.

Н2. $v(xy) = v(x)\,v(y)$ для всех $x, y \in K$.

Н3. $v(x+y) \leqslant v(x) + v(y)$.

Если нормирование вместо условия Н3 удовлетворяет более сильному требованию

$$\text{Н4.}\quad v(x+y)\leqslant \max[v(x),\ v(y)],$$

то оно называется *неархимедовым*.

Нормирование, для которого $v(x)=1$ при всех $x\neq 0$, называется *тривиальным*. В дальнейшем мы будем считать, что все рассматриваемые нормирования нетривиальны.

Так как всякое нормирование поля определяет в нем метрику и тем самым топологию, мы обычно будем писать $|x|_v$ или просто $|x|$ вместо $v(x)$.

Мы будем заниматься в основном следующими примерами.

Пусть $K=\mathbf{Q}$ — поле рациональных чисел. Обычная абсолютная величина является нормированием.

Для каждого простого числа p определено p-адическое нормирование $v_p=|\ |_p$:

$$|p^r m/n|_p = 1/p^r,$$

где r — любое целое число, $m, n\neq 0$ — целые числа, не делящиеся на p.

Пусть $\mathfrak{o}$ — дискретно нормированное кольцо с максимальным идеалом $\mathfrak{m}$, порожденным элементом π. Всякий ненулевой элемент α поля частных K кольца $\mathfrak{o}$ представляется в виде $\alpha=\pi^r u$, где r — целое число, а u — единица кольца $\mathfrak{o}$. Число r называется *порядком* α. Пусть c — положительное вещественное число, $0<c<1$. Положив

$$|\alpha| = c^r,$$

мы определим некоторое нормирование поля K (проверка тривиальна), которое оказывается неархимедовым.

В выборе константы c, конечно, имеется значительный произвол. В числовых полях мы будем иметь дело с двумя возможными вариантами выбора этой константы.

Пусть A — целое замыкание кольца целых чисел $\mathbf{Z}$ в поле алгебраических чисел K, и пусть $\mathfrak{p}\subset A$ — простой идеал. Пусть элемент π имеет порядок 1 относительно $\mathfrak{p}$, и пусть p — простое число, порождающее идеал $\mathfrak{p}\cap\mathbf{Z}$. Тогда $p=\pi^e u$ для некоторого целого числа $e>0$ и некоторой $\mathfrak{p}$-единицы u. Пусть $f=f_{\mathfrak{p}}$ — степень поля $A/\mathfrak{p}$ над

$\mathbf{Z}/p\mathbf{Z}$. Поле классов вычетов $A/\mathfrak{p}$ состоит из p^f элементов: это число мы обозначаем символом $\mathbf{N}\mathfrak{p}$. Идеал $\mathfrak{p}$ однозначно определяет следующие два нормирования: то, для которого

$$|p|_{\mathfrak{p}} = \frac{1}{p}, \qquad |\pi|_{\mathfrak{p}} = \frac{1}{p^{1/e}},$$

и то, для которого

$$\|\pi\|_{\mathfrak{p}} = \frac{1}{\mathbf{N}\mathfrak{p}}.$$

Для всякого элемента $\alpha \in K$, $\alpha \neq 0$, имеем

$$\|\alpha\|_{\mathfrak{p}} = |\alpha|_{\mathfrak{p}}^{e_{\mathfrak{p}} f_{\mathfrak{p}}}.$$

Пусть L — конечное расширение поля K, $\mathfrak{P}$ лежит над $\mathfrak{p}$ в кольце алгебраических чисел B поля L, Π — элемент, имеющий порядок 1 относительно $\mathfrak{P}$. Тогда

$$\mathfrak{p}B = \mathfrak{P}^{e(\mathfrak{P}/\mathfrak{p})} \ldots$$

и

$$|\pi|_{\mathfrak{P}} = |\Pi|_{\mathfrak{P}}^{e(\mathfrak{P}/\mathfrak{p})}.$$

Мультипликативность индексов ветвления и степеней полей классов вычетов при расширениях обеспечивает согласованность этих определений при переходе к расширениям конечной степени.

Всякое продолжение p-адического нормирования поля $\mathbf{Q}$ на числовое поле K определяется некоторым простым идеалом в целом замыкании A кольца $\mathbf{Z}$ в K. Действительно, пусть $\mathfrak{o}$ — кольцо данного нормирования, $\mathfrak{m}$ — его максимальный идеал: пересечение $\mathfrak{m} \cap A$ не может сводиться к нулю и, следовательно, представляет собой некоторый максимальный идеал $\mathfrak{p}$. Тривиальная проверка тогда показывает, что $\mathfrak{o} = A_{\mathfrak{p}}$. Таким способом получаются все нормирования поля K, индуцирующие p-адические нормирования на $\mathbf{Q}$, исходя из принятых нами в качестве основных понятий дедекиндова кольца и целого замыкания.

Пусть K — числовое поле. Всякое вложение K в поле вещественных или комплексных чисел определяет некоторое нормирование на K, которое называется соответственно *вещественным* или *комплексным*.

Множество нормирований поля K, состоящее из p-адических нормирований $|\ |_p$, описанных выше, а также вещественных и комплексных нормирований, называется *канонической системой* и обозначается символом M_K. Вещественные и комплексные нормирования из системы M_K называются также *архимедовыми*.

Очевидно, любые два разных нормирования из канонической системы независимы в том смысле, что они определяют различные топологии поля K. Следующая теорема о приближении является аналогом китайской теоремы об остатках для нормирований.

Теорема 1. *Пусть K — поле, $|\ |_1, \ldots, |\ |_s$ — нетривиальные попарно независимые нормирования K. Пусть $x_1 \ldots, x_s$ — произвольные элементы поля K, $\varepsilon > 0$. Существует такой элемент $x \in K$, что*

$$|x - x_i|_i < \varepsilon$$

для всех i.

◀ Доказательство. Прежде всего отметим, что для любых двух нормирований нашей системы, скажем $|\ |_1$ и $|\ |_s$, существует такой элемент $y \in K$, что $|y|_1 > 1$, $|y|_s < 1$. В самом деле, поскольку эти нормирования определяют разные и недискретные топологии, существует такая последовательность элементов $z_1, z_2, \ldots, z_n, \ldots$ поля K, что $|z_i|_s < 1$, $\lim\limits_{i \to \infty} |z_i|_s = 0$; $|z_i|_1 > \eta_0 > 0$ при всех i. Если существует индекс i такой, что $|z_i|_1 > 1$, то утверждение справедливо; в противном случае $|z_1|_1 < 1$ и для достаточно большого k имеем $|z_i/z_1^k|_1 > 1$ для всех i, $|z_i/z_1^k|_s \to 0$. Элемент $y = z_N z_1^{-k}$ для $N \geqslant N_0(k)$ удовлетворяет требуемым условиям.

Теперь индукцией по s покажем, что можно найти элемент $z \in K$, удовлетворяющий неравенствам $|z|_1 > 1$ и $|z|_j < 1$ для всех $j = 2, \ldots, s$. Случай $s = 2$ уже разобран. Пусть элемент $z \in K$ с условиями $|z|_1 > 1$, $|z_j| < 1$ для всех $j = 2, \ldots, s-1$ уже найден. Если $|z|_s \leqslant 1$, то для любого элемента $y \in K$ с $|y|_s < 1$, $|y|_1 > 1$ и для достаточно больших n элемент $z^n y$ удовлетворяет всем требованиям. Если же $|z|_s > 1$, то, полагая $t_n = \frac{z^n}{1+z^n}$, имеем $|t_n|_1 \to 1$, $|t_n|_s \to 1$, $|t_n|_j \to 0$ при

$j=2, \ldots, s-1$, так что можно положить $z=t_n y$ для достаточно большого n.

Для всякого элемента z, удовлетворяющего неравенствам $|z|_i>1$, $|z|_j<1$ при $j\neq i$, имеем $\left|\frac{z^n}{1+z^n}-1\right|_i\to 0$ при $n\to\infty$, $\left|\frac{z^n}{1+z^n}\right|_j\to 0$ при $n\to\infty$. Следовательно, для всякого индекса i, $1\leqslant i\leqslant s$, можно найти элемент z_i, сколь угодно близкий к единице в метрике $|\ |_i$ и к нулю — в остальных метриках. Тогда элемент $x=z_1x_1+\ldots+z_sx_s$ близок к x_i в метрике $|\ |_i$, что доказывает теорему. ▶

Пусть K — числовое поле, v — некоторое нормирование (в дальнейшем все рассматриваемые нормирования будут принадлежать канонической системе). Так же, как вещественные числа строятся исходя из рациональных, вводится пополнение поля K относительно v. Рассмотрим последовательности Коши элементов поля K. Они образуют кольцо. Последовательности, сходящиеся к нулю, образуют максимальный идеал, факторкольцо по которому является полем K_v. Поле K естественно вкладывается в K_v (элементу сопоставляется класс последовательности, все члены которой равны этому элементу). Нормирование v поля K продолжается на поле K_v по непрерывности. Обычно мы отождествляем поле K с его образом в поле K_v и называем K_v *пополнением* поля K.

Если v — архимедово нормирование, то K_v — поле вещественных или комплексных чисел.

Если v — неархимедово нормирование, соответствующее некоторому простому идеалу $\mathfrak{p}$ кольца алгебраических чисел поля K, то вместо K_v мы иногда будем писать $K_\mathfrak{p}$ и называть его полем $\mathfrak{p}$-*адических чисел*. Сейчас мы подробнее изучим случай $\mathfrak{p}$-адического нормирования $v=v_\mathfrak{p}$.

Пусть A — целое замыкание кольца $\mathbf{Z}$ в поле K, т. е. кольцо целых алгебраических чисел поля K. Обозначим символом A_v замыкание кольца A в поле K_v. Пусть $x\in A_v$. Выберем такой элемент $y\in A$, для которого

$$|x-y|<|x|, \quad |\ |=|\ |_\mathfrak{p}.$$

Тогда $|y|=|y-x+x|=|x|$, потому что наше нормирование неархимедово. Так как $\mathfrak{p}$-адическая норма любого элемента кольца A не превосходит 1, то же верно для элементов кольца A_v. Это же рассуждение показывает, что замыкание идеала $\mathfrak{p}$ состоит из элементов с нормой меньше 1 и что элемент $x\in K_v$, не принадлежащий кольцу A_v, имеет норму больше 1. В частности, нормирование v на поле K_v и на поле K имеет одну и ту же бесконечную циклическую группу значений. Для любого элемента $\pi\in A$, имеющего порядок 1 относительно $\mathfrak{p}$, число $|\pi|$ порождает эту группу.

Пусть $\mathfrak{o}$ — $A_\mathfrak{p}$-локальное кольцо идеала $\mathfrak{p}$; $\mathfrak{p}$-адическая норма всех элементов кольца $\mathfrak{o}$ не превосходит единицы, потому что порядки этих элементов относительно $\mathfrak{p}$ неотрицательны. Следовательно, кольцо $\mathfrak{o}$ лежит в замыкании кольца A и, больше того, замыкания колец $\mathfrak{o}$ и A в поле K_v совпадают. Это общее замыкание называется кольцом *целых $\mathfrak{p}$-адических чисел* поля K_v. Пусть $\mathfrak{m}_\mathfrak{p}$ — максимальный идеал кольца $A_\mathfrak{p}$, $\mathfrak{p}_v$ — замыкание идеала $\mathfrak{p}$ в кольце A_v. Имеют место канонические изоморфизмы

$$A_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}\longleftrightarrow A/\mathfrak{p}\longleftrightarrow A_v/\mathfrak{p}_v.$$

В силу сказанного всякий ненулевой элемент $\alpha\in K_v$ представляется в виде

$$\alpha=\pi^r u,$$

где $|u|_\mathfrak{p}=1$, так что u является единицей в замыкании A_v кольца A. Тем самым A_v — область с однозначным разложением на множители, имеющая единственный простой элемент и потому представляющая собой дискретно нормированное кольцо.

Пусть L — конечное расширение поля K, B — целое замыкание кольца A в поле L, $\mathfrak{P}$ — простой идеал кольца B, лежащий над $\mathfrak{p}$. Пусть w — каноническое нормирование, соответствующее идеалу $\mathfrak{P}$. Имеет место коммутативная диаграмма

$$\begin{array}{ccc} B & \longrightarrow & B_w \\ \uparrow & & \uparrow \\ A & \longrightarrow & A_v \end{array},$$

в которой стрелки вверху, внизу и слева означают вложения, а правая вертикальная стрелка отображает A_v на замыкание кольца A в кольце B_w. Аналогичная коммутативная диаграмма для полей классов вычетов выглядит так:

$$\begin{array}{ccc} B/\mathfrak{P} & \longrightarrow & B_w/\mathfrak{P}_w \\ \uparrow & & \uparrow \\ A/\mathfrak{p} & \longrightarrow & A_v/\mathfrak{p}_v \end{array};$$

здесь вертикальные стрелки — вложения, а горизонтальные — изоморфизмы.

Пусть K_w — замыкание поля K в поле L_w. Композит LK_w является конечным расширением поля K_w, содержащимся в L_w.

◀ Пусть $\omega_1, \ldots, \omega_n$ — базис линейного пространства LK_w над K. Покажем, что индуцированная нормированием w топология поля $LK_w \subset L_w$ совпадает с топологией K_w-пространства $K_w\omega_1 + \ldots + K_w\omega_n$. Для этого следует проверить, что для любой последовательности Коши в поле LK_w

$$x^{(\nu)} = \xi_1^{(\nu)}\omega_1 + \ldots + \xi_n^{(\nu)}\omega_n, \qquad \xi_n^{(\nu)} \in K_w,$$

последовательности коэффициентов $\xi_j^{(\nu)}$ сходятся в K_w. Проведем индукцию по n. При $n = 1$ утверждение очевидно; пусть $n \geqslant 2$. Достаточно разобрать случай, когда $x^{(\nu)} \longrightarrow 0$ (если это не так, можно рассмотреть последовательность $x^{(\nu)} - x^{(2\nu)}$). Предположим, что последовательность $\xi_1^{(\nu)}$ не сходится к нулю. Тогда для некоторого числа $a > 0$ и для бесконечно многих ν будем иметь $|\xi_1^{(\nu)}| > a$. Переходя к подпоследовательности, мы можем считать это неравенство выполненным для всех ν. Последовательность $x^{(\nu)}/\xi_1^{(\nu)}$ сходится к нулю. Кроме того,

$$\frac{x^{(\nu)}}{\xi_1^{(\nu)}} - \omega_1 = \frac{\xi_2^{(\nu)}}{\xi_1^{(\nu)}}\omega_2 + \ldots + \frac{\xi_n^{(\nu)}}{\xi_1(\nu)}\omega_n.$$

Последовательность правых частей сходится; из индуктивного предположения следует, что пределы $\lim \xi_i^{(\nu)}/\xi_1^{(\nu)} = \eta_i$ существуют при всех $i \geqslant 2$. Поэтому

$$-\omega_1 = \eta_2\omega_2 + \ldots + \eta_n\omega_n,$$

что противоречит линейной независимости элементов ω_i. Отсюда вытекает, что поле LK_w полно.▶

Следовательно, поле LK_w замкнуто и, стало быть, совпадает с L_w. Это же рассуждение, разумеется, применимо к случаю, когда v и w индуцированы вложениями в поле вещественных и комплексных чисел.

Предложение 0. *Пусть K — числовое поле, v — одно из его канонических нормирований, L — конечное расширение поля K. Два вложения $\sigma, \tau : L \to \overline{K}_v$ поля L над K индуцируют одно и то же нормирование поля L в том и только том случае, когда они сопряжены над K_v.*

(Сопряженность над K_v означает существование изоморфизма λ поля $\sigma L \cdot K_v$ на поле $\tau L \cdot K_v$, тождественного на K_v.)

◀ Доказательство. Если вложения σ, τ сопряжены над K_v, то на L они индуцируют одинаковые нормирования, потому что нормирование с K_v на $\overline{K}_v$ продолжается однозначно.

Докажем обратное утверждение. Пусть $\lambda : \tau L \to \sigma L$ — некоторый K-изоморфизм. Покажем, что его можно продолжить до K_v-изоморфизма полей $\tau L \cdot K_v$ и $\sigma L \cdot K_v$. Поскольку множество τL плотно в $\tau L \cdot K_v$, всякий элемент $x \in \tau L \cdot K_v$ представляется в виде

$$x = \lim \tau x_n, \qquad x_n \in E.$$

Поскольку нормирования на E, индуцированные σ и τ, совпадают, последовательность $\lambda \tau x_n = \sigma x_n$ сходится. Обозначим ее предел символом λx. Легко проверить, что λx не зависит от выбора последовательности $\tau x_n \to x$ и что отображение $\lambda : \tau L \cdot K_v \to \sigma L \cdot K_v$ представляет собой изоморфизм. Очевидно, он оставляет поле K_v инвариантным.▶

Это предложение дает ясную картину строения продолжений нормирования v на поле L, включая архимедовы нормирования.

Пусть K — числовое поле конечной степени N над полем $\mathbf{Q}$, v — некоторое нормирование поля K. Символом N_v обозначим локальную степень

$$N_v = [K_v : \mathbf{Q}_v].$$

Имеем

$$\sum_{v \mid v_0} N_v = N,$$

где сумма берется по всем продолжениям v фиксированного нормирования v_0 поля $\mathbf{Q}$.

Из предложения 0 и определения нормы вытекает

Следствие. *Пусть K — числовое поле, v_0 — некоторое нормирование из системы $M_{\mathbf{Q}}$. Для любого элемента $\alpha \in K$*

$$\prod_{v \mid v_0} |\alpha|_v^{N_v} = |N_{\mathbf{Q}}^K(\alpha)|_{v_0}.$$

Пусть A — дедекиндово кольцо. Группа его дробных идеалов изоморфна свободной абелевой группе, порожденной простыми идеалами. Пусть $\mathfrak{p}$ — простой идеал, $A_{\mathfrak{p}}$ — соответствующее локальное кольцо. Группа его дробных идеалов — бесконечная циклическая. Она порождена максимальным идеалом $\mathfrak{m}_{\mathfrak{p}}$ кольца $A_{\mathfrak{p}}$. Пусть v — нормирование, соответствующее идеалу $\mathfrak{p}$, A_v — пополнение кольца A (или $A_{\mathfrak{p}}$). Тогда A_v — также дедекиндово кольцо, а его группа дробных идеалов — бесконечная циклическая группа, порожденная идеалом $\mathfrak{p}_v$. Тем самым определены естественные отображения

$$\mathfrak{I}(A_v) \to \mathfrak{I}(A_{\mathfrak{p}}) \to \mathfrak{I}(A),$$

первое из которых — изоморфизм, а второе — вложение. Для краткости удобно иногда отождествлять $\mathfrak{p}_v$, $\mathfrak{m}_{\mathfrak{p}}$ и $\mathfrak{p}$, обозначая символом $\mathfrak{p}$ любой из этих идеалов. Произведение

$$\mathfrak{d} = \prod_{\mathfrak{p}} \mathfrak{p}^{r_{\mathfrak{p}}},$$

в котором $r_{\mathfrak{p}}$ — целые числа, все, кроме конечного числа, равные нулю, можно назвать *формальным идеалом* и в зависимости от контекста интерпретировать как элемент любой из групп $\mathfrak{I}(A)$, $\mathfrak{I}(A_{\mathfrak{p}})$, $\mathfrak{I}(A_v)$. Идеал $\mathfrak{p}^{r_{\mathfrak{p}}}$ называется $\mathfrak{p}$-*компонентой* формального идеала $\mathfrak{d}$ и обозначается символом $\mathfrak{d}_{\mathfrak{p}}$. Число $\mathfrak{p}^r$ называется *порядком* идеала $\mathfrak{d}$ относи-

тельно $\mathfrak{p}$ и обозначается так:

$$r_{\mathfrak{p}} = \operatorname{ord}_{\mathfrak{p}} \mathfrak{d}.$$

Для любого ненулевого элемента α поля частных одного из колец A, A_v можно образовать главные дробные идеалы αA, $\alpha A_{\mathfrak{p}}$ или αA_v, порядки которых относительно $\mathfrak{p}$ совпадают с $\operatorname{ord}_{\mathfrak{p}} \alpha$.

Для любых двух элементов α, β запись

$$\alpha \equiv \beta \pmod{\mathfrak{d}}$$

означает, что $\operatorname{ord}_{\mathfrak{p}} (\alpha - \beta) \geqslant \operatorname{ord}_{\mathfrak{p}} \mathfrak{d}$. Если α, β принадлежат полю частных кольца A, а $\mathfrak{d}$ рассматривается как дробный идеал, то это — обычное сравнение, означающее, что разность $\alpha - \beta$ принадлежит $\mathfrak{d}$. Если $\mathfrak{d} = \mathfrak{p}^r$, удобно рассматривать это сравнение как относящееся одновременно ко всем трем кольцам.

Пусть A — дедекиндово кольцо, $\mathfrak{p}$ — некоторый простой идеал, v — соответствующее нормирование. Пусть A_v — замыкание кольца A в пополнении K_v его поля частных, $\mathfrak{p}_v$ — замыкание идеала $\mathfrak{p}$ в кольце A_v. Тогда A_v — дискретно нормированное кольцо. Для любого дробного идеала $\mathfrak{a}$ кольца A имеем тривиальное соотношение

$$\mathfrak{a} A_v = \mathfrak{p}_v^{r_{\mathfrak{p}}},$$

где $r_{\mathfrak{p}} = \operatorname{ord}_{\mathfrak{p}} \mathfrak{a}$. Обратно,

$$\mathfrak{p}_v^r \cap A = \mathfrak{p}^r,$$

если $r > 0$. Замыкание дробного идеала $\mathfrak{a}$ в поле частных кольца A_v равно $\mathfrak{a} A_v$. Все эти утверждения проверяются тривиально, и мы оставляем эту проверку читателю.

§ 2. Многочлены над полными полями

В этом параграфе мы будем считать, что K — поле, полное относительно некоторого неархимедова нормирования; символом $\mathfrak{o}$ обозначим его подкольцо целых чисел, т. е. множество элементов с неархимедовой нормой $\leqslant 1$. Нет нужды предполагать нормирование дискретным.

Пусть $\mathfrak{p}$ — максимальный идеал кольца $\mathfrak{o}$. Заметим, что ряд

$$\sum_{n=1}^{\infty} a_n,$$

где $a_n \in K$, сходится в том и только том случае, когда

$$\lim_{n\to\infty} a_n = 0.$$

Таким образом, в этом случае легче обращаться со сходимостью, чем в архимедовом.

Займемся теперь вопросом существования корней у некоторых многочленов в полных полях.

Предложение 1. *Пусть m — положительное целое число с условием*

$$m \not\equiv 0 \pmod{\mathfrak{p}}.$$

Тогда для любого элемента $x \in \mathfrak{p}$ биномиальный ряд $(1+x)^{1/m}$ сходится к некоторому корню степени m из элемента $1+x$ группы U.

Доказательство. Очевидно, потому что знаменатели биномиальных коэффициентов не делятся на простое число p, входящее в идеал $\mathbf{Z} \cap \mathfrak{p}$.

Часто полезен более тонкий критерий существования корня.

Предположение 2. *Пусть $f(X)$ — многочлен с коэффициентами в кольце $\mathfrak{o}$. Пусть α_0 — такой элемент из $\mathfrak{o}$, для которого*

$$|f(\alpha_0)| < |f'(\alpha_0)|^2$$

(здесь f' означает формальную производную многочлена f). Тогда последовательность

$$\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}$$

сходится к некоторому корню α многочлена $f(X)$ в кольце $\mathfrak{o}$. Кроме того,

$$|\alpha - \alpha_0| \leqslant \left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right| < 1.$$

Доказательство. Положим $c = |f(\alpha_0)/f'(\alpha_0)^2| < 1$. Индукцией покажем, что

$$\text{(I)}\quad |\alpha_i| \leqslant 1,$$
$$\text{(II)}\quad |\alpha_i - \alpha_0| \leqslant c,$$
$$\text{(III)}\quad \left|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right| \leqslant c^{2^i}.$$

Очевидно, что из этих трех утверждений вытекает требуемый результат. При $i = 0$ они сводятся к условиям предложения. Пусть они верны для некоторого i. Тогда

(I) неравенство $\left|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right| \leqslant c^{2^i}$ показывает, что $|\alpha_{i+1} - \alpha_i| \leqslant c^{2^i} < 1$, так что $|\alpha_{i+1}| \leqslant 1$;

(II) $|\alpha_{i+1} - \alpha_0| \leqslant \max\{|\alpha_{i+1} - \alpha_i|, |\alpha_i - \alpha_0|\} = c$;

(III) в силу разложения Тейлора имеем

$$f(\alpha_{i+1}) = f(\alpha_i) - f'(\alpha_i)\frac{f(\alpha_i)}{f'(\alpha_i)} + \beta\left(\frac{f(\alpha_i)}{f'(\alpha_i)}\right)^2$$

для некоторого $\beta \in \mathfrak{o}$, и норма правой части оценивается числом

$$\left|\frac{f(\alpha_i)}{f'(\alpha_i)}\right|^2.$$

С другой стороны, разложение Тейлора для $f'(\alpha_{i+1})$ показывает, что

$$|f'(\alpha_{i+1})| = |f'(\alpha_i)|.$$

Отсюда находим

$$\left|\frac{f(\alpha_{i+1})}{f'(\alpha_{i+1})^2}\right| \leqslant c^{2^{i+1}},$$

что и требовалось доказать.

(Читатель, интересующийся более общей формулировкой этого результата, может обратиться к книге Бурбаки [4].)

В качестве приложения заметим, что в 2-адическом поле $\mathbf{Q}_2$ уравнение $x^2 + 7 = 0$ имеет корень. На самом деле для любого элемента $\gamma \equiv 1 \pmod 8$ из поля $\mathbf{Q}_2$ уравнение $x^2 = \gamma$ имеет корень: достаточно положить $\alpha_0 = 1$ в предложении 2.

Предложение 2 применимо также в тривиальном случае, когда

$$f'(\alpha_0) \not\equiv 0 \pmod{\mathfrak{p}},$$

но $f(\alpha_0) \equiv 0 \pmod{\mathfrak{p}}$. Решение соответствующей цепочки линейных уравнений, необходимое для построения последовательных приближений к корню многочлена f, более тривиально. Можно иначе описать эту ситуацию, сказав, что α_0 — простой корень многочлена f, приведенного $\bmod \mathfrak{p}$; мы будем называть это условие *тривиальным случаем леммы Гензеля*.

Предложение 2 показывает также, что всякая единица кольца $\mathfrak{o}$, достаточно близкая к 1, является m-й степенью, если число m не делится на характеристику поля K. В самом деле, достаточно рассмотреть уравнение

$$X^m - u = 0$$

и положить $\alpha_0 = 1$, если $|u-1| < |m|^2$.

Докажем теперь одну полезную лемму о приближениях в конечном расширении.

Предложение 3. *Пусть* α, β — *два элемента из алгебраического замыкания поля* K, *причем* α *сепарабелен над* $K(\beta)$. *Предположим, что для всех нетождественных изоморфизмов* σ *поля* $K(\alpha)$ *над* K *имеет место неравенство*

$$|\beta - \alpha| < |\sigma\alpha - \alpha|.$$

Тогда $K(\alpha) \subset K(\beta)$.

Доказательство. Достаточно проверить, что элемент α переходит в себя при всех изоморфизмах поля $K(\beta, \alpha)$ над $K(\beta)$. Пусть τ — такой изоморфизм. В силу единственности продолжения нормирований в полных полях, применяя τ к $\beta - \alpha$, получаем для всех нетождественных σ

$$|\beta - \tau\alpha| < |\sigma\alpha - \alpha|.$$

Пользуясь условием предложения, находим

$$|\tau\alpha - \alpha| = |\tau\alpha - \beta + \beta - \alpha| < |\sigma\alpha - \alpha|.$$

Отсюда вытекает, что τ — тождественное отображение на $K(\beta, \alpha)$, так что $K(\beta, \alpha) = K(\beta)$, как и утверждалось.

Предложение 3 называется *леммой Краснера*. Оно полезно при описании расширений поля K.

Теперь отметим непрерывность корней многочлена как функций от коэффициентов.

Пусть $f(X)$ — многочлен в кольце $K(X)$ со старшим коэффициентом 1,

$$f(X) = \Pi (X - \alpha_i)^{r_i}$$

— его разложение в алгебраическом замыкании поля K. Пусть степень f равна n и все корни α_i различны. Как обычно, символом $|g|$ обозначим максимум норм коэффициентов многочлена g. Очевидно, что когда $|g|$ ограничено, нормы корней многочлена тоже ограничены.

Предположим, что многочлен g близок к f в том смысле, что число $|f - g|$ мало. Тогда для любого корня β многочлена g число

$$|f(\beta) - g(\beta)| = |f(\beta)|$$

мало, так что β должен быть близок к одному из корней многочлена f. Когда β приближается, скажем, к корню $\alpha = \alpha_1$, его расстояние до любого другого корня многочлена f приближается к расстоянию α_1 до этого корня и потому ограничено снизу. Можно описать эту ситуацию, сказав, что β *принадлежит* α.

Пусть многочлен g достаточно близок к f, а $\beta_1, \ldots, \beta_s$ — корни g, принадлежащие α (с учетом кратностей); мы утверждаем, что тогда $s = r$ (r—кратность корня α многочлена f).

Действительно, иначе можно найти последовательность многочленов g_ν, приближающихся к f, у которых точно s корней $\beta_1^{(\nu)}, \ldots, \beta_s^{(\nu)}$ принадлежат α и $s \neq r$. Тогда каждый из корней $\beta_1^{(\nu)}, \ldots, \beta_s^{(\nu)}$ стремится к α. Но $\lim\limits_{\nu} g_\nu = f$, так что α должен быть корнем кратности s многочлена f. Противоречие.

В качестве приложения получаем

Предложение 4. *Если многочлен f неприводим и сепарабелен, то любой многочлен g, достаточно близкий к f, также неприводим. (Мы предполагаем, что f и g имеют старшие коэффициенты* 1 *и что степени их*

совпадают.) Далее, для любого корня α *многочлена* f *существует корень* β *многочлена* g, *принадлежащий* α, *и* $K(\alpha)=K(\beta)$.

Доказательство. Если g достаточно близок к f, то все его корни простые и принадлежат разным корням f. Если корень β многочлена g достаточно близок к корню α многочлена f, то лемма Краснера немедленно показывает, что $K(\alpha)=K(\beta)$. Следовательно, многочлен g неприводим, потому что его степень совпадает со степенью f.

Следствие. *Пусть* K *— конечное расширение поля* $\mathbf{Q}_p$. *Тогда существует такое конечное расширение* E *поля* $\mathbf{Q}$, *содержащееся в* K, *что* $[E:\mathbf{Q}]=[K:\mathbf{Q}_p]$ *и* E *плотно в* K, *так что* $K=E\mathbf{Q}_p$.

Доказательство. Пусть $K=\mathbf{Q}_p(\alpha)$, и пусть f — неприводимый многочлен над $\mathbf{Q}_p$, корнем которого является α. В качестве g выберем многочлен, достаточно близкий к f, но с коэффициентами в поле $\mathbf{Q}$, и положим $E=\mathbf{Q}(\beta)$.

Это следствие оправдывает употребление названия *$\mathfrak{p}$-адическое поле* по отношению к любому конечному расширению поля $\mathbf{Q}_p$. Целое замыкание кольца p-адических чисел поля K имеет единственный максимальный идеал, который обозначается буквой $\mathfrak{p}$.

§ 3. Некоторые фильтрации

Пусть $\mathfrak{o}$ — дискретно нормированное кольцо с максимальным идеалом $\mathfrak{p}$, K — его поле частных, полное относительно нормирования, определенного кольцом $\mathfrak{o}$. Пусть π — образующий элемент идеала $\mathfrak{p}$. Эти обозначения сохраняются на протяжении всего параграфа; соответствующее кольцу $\mathfrak{o}$ нормирование также предполагается фиксированным.

Известно, что в топологии, определяемой нормированием, подгруппы $\mathfrak{p}^r$ $(r=1, 2, \ldots)$ *открыты*. В самом деле, для любого элемента $x\in K$ и для всех $\mathfrak{p}\in K$ с условием $|x-y|<|x|$ имеем $|y|=|x|$. Поэтому $\mathfrak{p}^r$ — открытые подгруппы, и их пересечение сводится к нулю. Тем самым они образуют фундаментальную систему окрест-

ностей нуля в поле K (мы полагаем $\mathfrak{p}^0 = \mathfrak{o}$ по определению).

Умножение на π^r определяет изоморфизм аддитивной группы $\mathfrak{p}^r/\mathfrak{p}^{r+1}$ с группой $\mathfrak{o}/\mathfrak{p}$.

Единицы кольца $\mathfrak{o}$ образуют группу по умножению, обозначаемую буквой U. Для всякого целого числа $i \geqslant 1$ положим

$$U_i = 1 + \mathfrak{p}^i$$

и $U_0 = U$. Все U_i — группы, потому что если $x, y \in \mathfrak{p}^i$, то

$$(1+x)(1+y) = 1 + x + y + xy \in 1 + \mathfrak{p}^i \qquad (i \geqslant 1),$$

$$(1+x)(1+y) \equiv 1 + x + y \pmod{\mathfrak{p}^{i+1}},$$

а ряд

$$(1-x)^{-1} = 1 + x + x^2 + \ldots$$

сходится.

Единицы образуют открытое подмножество кольца $\mathfrak{o}$.

Пусть элемент π имеет порядок 1 относительно $\mathfrak{p}$; очевидно, группа K^* топологически и алгебраически изоморфна прямому произведению $\{\pi\} \times U$, где $\{\pi\}$ — циклическая группа, порожденная элементом π.

При каноническом гомоморфизме

$$\mathfrak{o} \longrightarrow \mathfrak{o}/\mathfrak{p}$$

единицы отображаются на ненулевые элементы поля $\mathfrak{o}/\mathfrak{p}$, а ядром индуцированного гомоморфизма

$$U \longrightarrow (\mathfrak{o}/\mathfrak{p})^*$$

является в точности группа U_1. Тем самым $U/U_1 \approx (\mathfrak{o}/\mathfrak{p})^*$.

Далее, при $i \geqslant 1$ имеет место изоморфизм

$$\mathfrak{p}^i/\mathfrak{p}^{i+1} \longrightarrow U_i/U_{i+1},$$

индуцированный отображением идеала $\mathfrak{p}^i$, которое задается формулой

$$x \rightsquigarrow (1+x) \bmod U_{i+1}.$$

То обстоятельство, что это гомоморфизм с ядром $\mathfrak{p}^{i+1}$, проверяется немедленно: это — начало экспоненциального отображения.

Если $\mathfrak{o}/\mathfrak{p}$ — конечное поле из q элементов, то число элементов группы $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ также равно q, а число элементов группы U/U_1 равно $(q-1)$.

Предложение 5. *Если поле $\mathfrak{o}/\mathfrak{p}$ конечно, то $\mathfrak{o}$ и U компактны.*

Доказательство. $\mathfrak{o}$ есть проективный предел конечных групп $\mathfrak{o}/\mathfrak{p}^i$, который компактен (его можно рассматривать как замкнутую подгруппу прямого произведения групп $\mathfrak{o}/\mathfrak{p}^i$). То же верно для группы U, которая является проективным пределом групп U/U_i.

Группы U_i образуют фундаментальную систему окрестностей 1 в группе U.

Тем самым $\mathfrak{p}$-адическое поле локально компактно.

Как отмечалось в предыдущем параграфе, всякая единица в $\mathfrak{p}$-адическом поле, достаточно близкая к 1, является m-й степенью. Поэтому для любого целого положительного числа m индекс $(U : U^m)$ конечен. Сейчас мы вычислим этот индекс.

Нам понадобится одна теоретико-групповая лемма.

Лемма. *Пусть f — гомоморфизм коммутативной группы A в другую группу, A^f — его образ, A_f — ядро. Пусть B — некоторая подгруппа группы B. Тогда*

$$(A : B) = (A^f : B^f)\,(A_f : B_f)$$

в том смысле, что если два из входящих сюда индексов конечны, то конечен и третий, и имеет место выписанное равенство.

Доказательство. Это — легкое следствие обычных теорем о гомоморфизмах. Мы оставляем подробности читателю.

Предложение 6. *Пусть K есть $\mathfrak{p}$-адическое поле, U — группа единиц его кольца целых чисел. Пусть m — положительное целое число. Тогда*

$$(U : U^m) = \frac{m}{\|m\|_{\mathfrak{p}}}\,(K_m^* : 1)$$

и

$$(K^* : K^{*m}) = \frac{m^2}{\|m\|_{\mathfrak{p}}}\,(K_m^* : 1),$$

где K_m^* — группа корней m-й степени из единицы, содержащихся в поле K.

Доказательство. Вторая формула следует из первой, потому что $K^* \approx \mathbf{Z} \times U$.

Доказательство первой формулы, следующее ниже, взято из лекций Артина [1].

Выберем число r настолько большим, что $|m\pi^{r+1}| \geqslant |\pi^{2r}|$, и рассмотрим группу U_r. Тогда для любого целого x имеем

$$(1 + x\pi^r)^m \equiv 1 + mx\pi^r \pmod{m\pi^{r+1}}.$$

Тем самым, полагая $\operatorname{ord}_{\mathfrak{p}} m = s$, получим

$$U_r^m = U_{r+s}.$$

Пусть r, кроме того, настолько велико, что ни один из корней m-й степени из 1, кроме 1, не принадлежит U_r. Применим сформулированную выше лемму к гомоморфизму $f(a) = a^m$ группы единиц. В результате получим

$$(U : U_r) = (U^m : U_{r+s})\,(K_m^* : 1) = \frac{(U : U_{r+s})}{(U : U^m)}\,(K_m^* : 1).$$

Следовательно,

$$(U : U^n) = \frac{(U : U_{r+s})}{(U : U_r)}\,(K_m^* : 1) = (U_r : U_{r+s})\,(K_m^* : 1).$$

Но $(U_r : U_{r+s}) = (\mathbf{N}\mathfrak{p})^s$, откуда следует наше утверждение.

§ 4. Неразветвленные расширения

Мы по-прежнему предполагаем, что K — полное дискретно нормированное поле частных кольца A с максимальным идеалом $\mathfrak{p}$.

Пусть E — конечное расширение поля K, B — целое замыкание кольца A в поле E. В кольце B есть единственный простой идеал $\mathfrak{P}$, лежащий над $\mathfrak{p}$, и B дискретно нормировано. Если e — индекс ветвления, а f — степень поля классов вычетов, имеем

$$ef = [E : K].$$

(Здесь мы доказали это равенство только для сепарабельных расширений E поля K. Поскольку нас интере-

суют преимущественно числовые поля, доказательство в общем случае не приводится. Если угодно, читатель может полагать характеристику поля K равной 0.)

Таким образом, $e=1$ тогда и только тогда, когда

$$[E:K]=[B/\mathfrak{P}:A/\mathfrak{p}].$$

Если это равенство выполнено, а расширение $B/\mathfrak{P}$ поля $A/\mathfrak{p}$ сепарабельно, идеал $\mathfrak{P}$ называется *неразветвленным* над $\mathfrak{p}$, а поле E — *неразветвленным расширением* поля K.

Пусть $\varphi: B \to B/\mathfrak{P}$ — канонический гомоморфизм, $g=\beta_n X^n+\ldots+\beta_0$ — многочлен с коэффициентами в кольце B. Символом g^φ мы обозначаем многочлен $\varphi(\beta_n)X^n+\ldots$ $\ldots+\varphi(\beta_0)$, полученный применением гомоморфизма φ к коэффициентам многочлена g.

Предложение 7. *Пусть E — конечное расширение поля K, и пусть идеал $\mathfrak{P}$ неразветвлен над $\mathfrak{p}$. Пусть $\alpha' \in B^\varphi$ — такой элемент, что $B^\varphi=A^\varphi(\alpha')$, и пусть $\alpha \in B$ — элемент, для которого $\varphi\alpha=\alpha'$. Тогда $E=K(\alpha)$, и образ g^φ K-неприводимого многочлена $g(X)$, корнем которого является α, также неприводим. Обратно, пусть $E=K(\alpha)$, где α — корень некоторого многочлена $g(X) \in A[X]$ со старшим коэффициентом 1, образ которого g^φ не имеет кратных корней. Тогда идеал $\mathfrak{P}$ неразветвлен над $\mathfrak{p}$ и $B^\varphi=A^\varphi(\varphi\alpha)$.*

Доказательство. Предположим сначала, что идеал $\mathfrak{P}$ неразветвлен. Пусть $g'(X)$ — неприводимый многочлен над кольцом A^φ, корнем которого является α'. Пусть $\alpha \equiv \alpha' \pmod{\mathfrak{P}}$ — корень неприводимого над K многочлена $g(X)$. Тогда α цел над A и α' является корнем многочлена g^φ, так что g^φ делится на g'. С другой стороны,

$$\deg g' = [B^\varphi : A^\varphi] = [E:K] \geqslant \deg g,$$

так что $g'=g^\varphi$. Первое утверждение доказано.

Обратно, если элемент α удовлетворяет сформулированному условию, то, не теряя общности, можно считать, что для соответствующего неприводимого многочлена $g(X)$ его образ g^φ не имеет кратных корней. Применяя

к наименьшему расширению Галуа поля K, содержащему E, следствие 2 предложения 14 гл. I, § 5, заключаем, что g^{φ} является степенью неприводимого многочлена, а потому неприводим. Из неравенств

$$[A^{\varphi}(\varphi\alpha) : A^{\varphi}] \leqslant [B^{\varphi} : A^{\varphi}] \leqslant [E : K]$$

тогда следует, что в действительности всюду стоят знаки равенства и что

$$B^{\varphi} = A^{\varphi}(\varphi\alpha).$$

Предложение доказано.

Предложение 8. *Пусть E — конечное расширение поля K.*

(I) *Пусть $E \supset F \supset K$; поле E неразветвлено над K в том и только том случае, когда E неразветвлено над F, а F неразветвлено над K.*

(II) *Пусть E неразветвлено над K, а K_1 — конечное расширение поля K. Тогда поле EK_1 неразветвлено над K_1.*

(III) *Пусть E_1, E_2 — конечные неразветвленные расширения поля K. Тогда поле E_1E_2 также неразветвлено.*

Доказательство. Первое утверждение вытекает из того, что степени полей классов вычетов ограничены степенями полей и мультипликативны при расширениях. Кроме того, следует воспользоваться тем, что утверждение (I) справедливо, если заменить условие неразветвленности условием сепарабельности конечных расширений. Второе утверждение немедленно следует из предложения 7. Третье формально вытекает из первого и второго.

Предложение 9. *Для всякого конечного расширения E поля K в данном алгебраическом замыкании $\overline{K}$ этого поля обозначим символом B_E целое замыкание кольца A в E. Пусть $\overline{A}$ — целое замыкание кольца A в поле $\overline{K}$. Пусть φ — гомоморфизм кольца $\overline{A}$, пересечение ядра которого с каждым из колец B_E является максимальным идеалом $\mathfrak{P}_E$ этого кольца. Тогда отображение*

$$B_E \rightsquigarrow B_E^{\varphi}$$

индуцирует взаимно однозначное соответствие между неразветвленными расширениями E поля K и сепарабельными расширениями поля A^{φ}.

Доказательство. Упражнение для читателя.

Если предположить, что поле A^{φ} конечно, как это имеет место в теории чисел, то все алгебраические расширения этого поля сепарабельны и даже цикличны. Группа Галуа порождена каноническим автоморфизмом Фробениуса σ, для которого

$$\sigma x = x^q,$$

где q — число элементов поля классов вычетов $A/\mathfrak{p}$. Поэтому всякое конечное неразветвленное расширение поля K циклично, и в его группе Галуа имеется однозначно определенный автоморфизм, индуцирующий σ. В самом деле, согласно предложению 14 гл. I § 5, группа Галуа G неразветвленного расширения совпадает с $G_{\mathfrak{P}}$, потому что существует единственный простой дивизор $\mathfrak{P}$, лежащий над $\mathfrak{p}$, а группа $G_{\mathfrak{P}}$ изоморфна группе расширения поля классов вычетов.

§ 5. Слабо разветвленные расширения

Мы по-прежнему предполагаем, что K — полное дискретно нормированное поле частных дедекиндова кольца A с максимальным идеалом $\mathfrak{p}$, для которого поле классов вычетов $A/\mathfrak{p}$ совершенно.

Пусть E — конечное расширение поля K, $B = B_E$ — целое замыкание кольца A в поле E, $\mathfrak{P} = \mathfrak{P}_E$ — максимальный идеал кольца B.

Идеал $\mathfrak{P}$ называется *вполне разветвленным* над $\mathfrak{p}$, если $[E:K] = e$. В этом случае степень поля классов вычетов равна 1 (потому что $ef = n$). Так как $\mathfrak{P}$ — единственный простой идеал кольца B, лежащий над $\mathfrak{p}$, мы будем говорить, что поле E вполне разветвлено над K.

Предложение 10. *Пусть E — конечное расширение поля K, E_u — композит всех неразветвленных подрасширений поля E. Тогда поле E_u неразветвлено над K, а поле E вполне разветвлено над E_u.*

Доказательство. Первое утверждение следует из предложения 8 предыдущего параграфа. Для доказательства второго утверждения рассмотрим башни

$$\begin{array}{cc} E & B/\mathfrak{P} \\ | & | \\ E_u & B_u/\mathfrak{P}_u \\ | & | \\ K & A/\mathfrak{p}. \end{array}$$

Если бы степень расширения поля классов вычетов в верхнем этаже башни была больше 1, это расширение можно было бы поднять до некоторого неразветвленного над E_u подполя поля E, что противоречит максимальности E_u. Следовательно, эта степень равна 1, так что E вполне разветвлено над E_u.

Пусть E — конечное расширение поля K. Идеал $\mathfrak{P}$ называется *слабо разветвленным* над $\mathfrak{p}$ (а поле E — слабо разветвленным над K), если характеристика p поля классов вычетов $A/\mathfrak{p}$ не делит e. Мы сейчас опишем слабо вполне разветвленные расширения.

Предложение 11. *Пусть поле E вполне разветвлено над K, Π — элемент порядка 1 относительно $\mathfrak{P}$. Он удовлетворяет уравнению Эйзенштейна*

$$X^e + a_{e-1}X^{e-1} + \ldots + a_0 = 0,$$

где $a_i \in \mathfrak{p}$ для всех i и $a_0 \not\equiv 0 \pmod{\mathfrak{p}^2}$. Обратно, всякое такое уравнение неприводимо, а его корень порождает вполне разветвленное расширение степени e.

Доказательство. Все сопряженные к Π элементы над полем K имеют одну и ту же $\mathfrak{p}$-адическую норму (из-за однозначности продолжения нормирования на конечные расширения). Поэтому коэффициенты соответствующего неприводимого уравнения, которые являются формами от корней, принадлежат идеалу $\mathfrak{P} \cap A = \mathfrak{p}$. Последний коэффициент a_0 является произведением элемента Π и всех его сопряженных, которых ровно e. Поэтому

$$|a_0| = |\Pi|^e,$$

так что $a_0 = \pi$ — элемент порядка 1 относительно $\mathfrak{p}$. Обратно, всякое уравнение Эйзенштейна неприводимо. Приведенное выше рассуждение относительно Π можно применить к любому корню β этого многочлена, так что $|\beta|^e = \pi$. Следовательно, $e = [K(\beta) : K]$.

Заметим, что если $p \nmid e$, то расширение слабо разветвлено.

Предложение 12. *Пусть E — слабо вполне разветвленное расширение поля K. Тогда существует элемент $\Pi \in E$ порядка 1 относительно $\mathfrak{P}$, удовлетворяющий уравнению вида*

$$X^e - \pi = 0,$$

где π — некоторый элемент порядка 1 относительно $\mathfrak{p}$ поля K. Обратно, пусть a — любой элемент кольца A, e — положительное целое число, не делящееся на p. Тогда любой корень уравнения

$$X^e - a = 0$$

порождает слабо разветвленное расширение поля K, которое вполне разветвлено, если порядок относительно $\mathfrak{p}$ элемента a взаимно прост с e.

Доказательство. Пусть $f(X) = X^e - a$, где $a \in A$, и e не делится на p. Пусть α — любой корень многочлена f. Запишем a в виде $a = \pi^r u$, где r — некоторое целое число, u — единица кольца A. Тогда $K(\alpha)$ содержится в поле $K(\zeta, u^{1/e}, \pi^{1/e})$, где ζ — примитивный корень e-й степени из 1. Расширение $F = K(\zeta, u^{1/e})$ неразветвлено над K, так что π остается простым элементом идеала $\mathfrak{P}_F$. Расширение $F(\pi^{1/e})$ слабо вполне разветвлено, так что индекс ветвления поля $K(\alpha)$ над K делит индекс ветвления поля $K(\zeta, u^{1/e}, \pi^{1/e})$ над K. Отсюда следует, что поле $K(\alpha)$ слабо разветвлено над K. Если порядок элемента a относительно $\mathfrak{p}$ взаимно прост с e, можно найти два целых числа s, t, для которых

$$se + tr = 1.$$

Положим $\beta = a^t \pi^s$. Элементы β^e и π имеют один и тот же порядок относительно $\mathfrak{P}$, так что интересующий нас индекс ветвления не меньше e. Поэтому он равен e

(так как $[K(\alpha):K]\leqslant e$), и наше расширение слабо вполне разветвлено.

Остается установить, что всякое вполне слабо разветвленное расширение порождено корнем уравнения вида

$$X^e-\pi=0$$

для некоторого простого элемента π идеала $\mathfrak{p}$. Для этого нам понадобится следующая лемма.

Лемма. *Пусть e — положительное целое число, не делящееся на p. Пусть E — конечное вполне разветвленное расширение поля K, π_0 — простой элемент идеала $\mathfrak{p}$, β — такой элемент поля E, для которого $|\beta|^e=|\pi_0|$. Тогда существует такой элемент π порядка 1 относительно $\mathfrak{p}$, что один из корней уравнения $X^e-\pi=0$ содержится в поле $K(\beta)$.*

Доказательство. Можно положить $\beta^e=\pi_0 u$, где u — некоторая единица в кольце B. Так как наше расширение вполне разветвлено, степень поля классов вычетов равна 1 и, значит, существует такая единица $u_0\in A$, что $u\equiv u_0 \pmod{\mathfrak{P}}$. Полагая $\pi=\pi_0 u_0$, получим

$$\beta^e=\pi+\pi x,$$

где $x\equiv 0 \pmod{\mathfrak{P}}$. Тем самым

$$|\beta^e-\pi|<|\pi|.$$

Пусть $f(X)=X^e-\pi$ и $\alpha_1, \ldots, \alpha_e$ — корни этого многочлена. Тогда

$$|f(\beta)|=|\beta-\alpha_1|\ldots|\beta-\alpha_e|.$$

Но $|\alpha_i|=|\beta|$ при всех i. Следовательно, хотя бы для одного значения i, скажем $i=1$, имеем

$$|\beta-\alpha_1|<|\alpha_1|.$$

С другой стороны,

$$|f'(\alpha_1)|=|\alpha_1|^{e-1}=|\alpha_1-\alpha_2|\ldots|\alpha_1-\alpha_e|$$

и $|\alpha_i-\alpha_j|\leqslant|\alpha_1|$. Это показывает, что для всех пар i, j, $i\neq j$, имеет место равенство $|\alpha_i-\alpha_j|=|\alpha_1|$. В силу леммы Краснера отсюда следует, что $K(\alpha_1)\subset K(\beta)$, что и требовалось доказать.

Предложение 12 сразу же получается отсюда, если положить $\beta = \pi$.

Предложение 13. *Пусть E — конечное расширение поля K. Все утверждения предложения 8 останутся справедливыми, если слово «неразветвленное» всюду заменить словами «слабо разветвленное».*

Доказательство. Стандартные рассуждения с использованием мультипликативности индекса ветвления и предложения 12.

Следствие. *Пусть E — конечное расширение поля K, E_t — композит всех его слабо разветвленных подрасширений. Тогда поле E_t слабо разветвлено над K, а поле E вполне разветвлено над E_t. Далее, число $[E : E_t]$ является степенью характеристики p поля классов вычетов.*

Доказательство. Пусть e — индекс ветвления поля E,

$$e = e_0 p^r,$$

где e_0 взаимно просто с p. Пусть Π — элемент первого порядка относительно идеала $\mathfrak{P}$ и

$$\beta = \Pi^{p^r}.$$

В силу леммы поле $K(\beta)$ содержит слабо разветвленное подрасширение с индексом ветвления e_0. Композит этого расширения с максимальным неразветвленным расширением поля E является слабо разветвленным расширением F поля K, а из определения β следует, что индекс ветвления поля E над F равен p^r. С другой стороны, поле E вполне разветвлено над F (потому что F содержит E_u) и, значит, $[E : F] = p^2$. Любое слабо разветвленное подрасширение поля E должно содержаться в F, иначе его композит с F был бы слабо разветвлен над F. Это доказывает следствие.

Наконец, мы докажем полезную теорему конечности для $\mathfrak{p}$-адических полей.

Предложение 14. *Пусть K есть $\mathfrak{p}$-адическое поле (конечное расширение поля $\mathbf{Q}_p$). Для всякого целого числа n существует лишь конечное число расширений поля K степени, не превосходящей n.*

Доказательство. Так как существует единственное неразветвленное расширение каждой степени, соответствующее расширению поля классов вычетов, и так как всякое расширение получается в виде последовательности неразветвленного и вполне разветвленного расширения, достаточно показать, что существует только конечное число вполне разветвленных расширений данной степени e. Но все такие расширения задаются корнями уравнений Эйзенштейна

$$X^e + a_{e-1}X^{e-1} + \ldots + u_0\pi = 0,$$

где коэффициенты a_i принадлежат $\mathfrak{p}$, а u_0 — единица (π — фиксированный простой элемент идеала $\mathfrak{p}$). Прямое произведение

$$\mathfrak{p} \times \ldots \times \mathfrak{p} \times U$$

идеала $\mathfrak{p}$, взятого $e-1$ раз, и группы единиц U компактно. Любой элемент этой группы описывает конечное число расширений степени e (соответствующих различным корням уравнения Эйзенштейна). В силу леммы Краснера некоторая окрестность любого элемента определяет то же самое расширение (предложение 4, § 2), так что конечность числа расширений следует из компактности.

Глава III

ДИФФЕРЕНТА И ДИСКРИМИНАНТ

Изучение дифференты и дискриминанта доставляет информацию о разветвленных простых идеалах, а также вводит некоторую двойственность, существенную как в алгебраической теории ветвления, так и в последующих главах об аналитической двойственности. Кроме того, эти понятия позволяют дать хороший метод вычисления кольца целых чисел в числовом поле; см. ниже предложение 10.

§ 1. Дополнительные модули

На протяжении этого параграфа A — дедекиндово кольцо, K — его поле частных, E — конечное сепарабельное расширение поля K, B — целое замыкание кольца A в E. Пусть L — некоторая аддитивная подгруппа поля E. Определим *дополнительное* к ней *множество* L' (относительно следа) как совокупность всех тех $x \in E$, для которых

$$\mathrm{Tr}_K^E(xL) \subset A.$$

L' является аддитивной группой. Если $AL = L$, то $AL' = L'$.

Пусть L, M — две аддитивные подгруппы поля E и $L \subset M$. Тогда $M' \subset L'$.

Кроме того, имеют место следующие утверждения.

Предложение 1. *Пусть* $w_1, \ldots, w_n$ — *базис поля* E *над* K, *и пусть* $L = Aw_1 + \ldots + Aw_n$. *Тогда*

$$L' = Aw_1' + \ldots + Aw_n',$$

где $\{w_i'\}$ — *базис, двойственный относительно следа.*

Доказательство. Пусть $\alpha \in L'$, и пусть

$$\alpha = a_1 w_1' + \ldots + a_n w_n',$$

где $a_i \in K$. Тогда $\mathrm{Tr}(\alpha w_i) = a_i$, так что $a_i \in A$ для всех i. Это доказывает, что $L \subset Aw_1' + \ldots + Aw_n'$. Обратно,

$$\mathrm{Tr}(Aw_i' L) = A \cdot \mathrm{Tr}(w_i' L) \subset A,$$

так что обратное включение также тривиально.

Поскольку всякий дробный идеал кольца B зажат между двумя A-модулями типа $Aw_1 + \ldots + Aw_n$ для подходящих базисов $\{w_i\}$ поля E над K, а кольцо A — нетерово, получаем

Следствие. *Если* $\mathfrak{b}$ *— дробный идеал кольца* B, *то* $\mathfrak{b}'$ *— тоже дробный идеал. Кроме того,* $B \subset B'$.

Предложение 2. *Пусть* $E = K(\alpha)$ *— конечное сепарабельное расширение степени* n. *Пусть* f *— неприводимый многочлен над полем* K, *корнем которого является* α, f' *— его производная, и*

$$\frac{f(X)}{X - \alpha} = b_0 + b_1 X + \ldots + b_{n-1} X^{n-1}.$$

Тогда базис, двойственный к степенному $1, \alpha, \ldots, \alpha^{n-1}$, *состоит из чисел*

$$\frac{b_0}{f'(\alpha)}, \ldots, \frac{b_{n-1}}{f'(\alpha)}.$$

Доказательство. Пусть $\alpha_1, \ldots, \alpha_n$ — различные корни многочлена f. Тогда

$$\sum_{i=1}^{n} \frac{f(X)}{X - \alpha_i} \cdot \frac{\alpha_i^r}{f'(\alpha_i)} = X^r, \quad 0 \leqslant r \leqslant n-1.$$

Для доказательства обозначим символом $g(X)$ разность левой и правой частей этого равенства. Тогда g — многочлен степени не более $n-1$, имеющий n корней: $\alpha_1, \ldots, \alpha_n$; поэтому $g \equiv 0$.

Многочлены

$$\frac{f(X)}{X - \alpha_i} \cdot \frac{\alpha_i^r}{f'(\alpha_i)}$$

все сопряжены друг с другом. Если определить след многочлена с коэффициентами в поле E как многочлен, получающийся применением оператора следа к коэффи-

циентам, мы получим

$$\mathrm{Tr}\left[\frac{f(X)}{X-\alpha}\cdot\frac{\alpha^r}{f'(\alpha)}\right]=X^r.$$

Сравнивая коэффициенты при каждой степени X в левой и правой частях этого равенства, находим

$$\mathrm{Tr}\left(\alpha^i\frac{b_j}{f'(\alpha)}\right)=\delta_{ij},$$

что доказывает наше утверждение.

Следствие. *Предположим, что* $B=A[\alpha]$. *Тогда* $B'=B/f'(\alpha)$.

Доказательство. Пользуясь рекуррентными формулами

$$\begin{aligned} &b_{n-1}=1,\\ &b_{n-2}-\alpha b_{n-1}=a_{n-1},\\ &\ldots\ldots\ldots, \end{aligned}$$

убеждаемся, что числа $1, \alpha, \ldots, \alpha^{n-1}$ порождают над A то же кольцо, что и числа $b_0, \ldots, b_{n-1}$. Отсюда немедленно вытекает наше следствие.

Предложение 3. *Пусть* A*—дискретно нормированное кольцо, пусть существует единственный простой идеал* $\mathfrak{P}$ *в кольце* $B\supset A$, *лежащий над максимальным идеалом* $\mathfrak{p}$ *кольца* A, *и пусть расширение* $B/\mathfrak{P}$ *поля* $A/\mathfrak{p}$ *сепарабельно. Тогда существует такой элемент* $\alpha\in B$, *что* $B=A[\alpha]$.

Доказательство. Пусть β — элемент кольца B, класс вычетов $\bmod\mathfrak{P}$ которого порождает поле $B/\mathfrak{P}$ над $A/\mathfrak{p}$. Пусть f — многочлен над A со старшим коэффициентом 1, редукция которого $\bmod\mathfrak{p}$ является неприводимым многочленом с корнем $\beta\,(\bmod\mathfrak{P})$. Пусть Π — элемент порядка 1 относительно идеала $\mathfrak{P}$ в кольце B.

Тогда

$$f(\beta+\Pi)\equiv f(\beta)+f'(\beta)\,\Pi\qquad(\bmod\mathfrak{P}^2)$$

и $f'(\beta)\not\equiv 0\,(\bmod\mathfrak{P})$. Следовательно, либо элемент $\alpha=\beta$, либо $\alpha=\beta+\Pi$ обладает тем свойством, что его класс

вычетов $\bmod \mathfrak{P}$ порождает поле $B/\mathfrak{P}$ над $A/\mathfrak{p}$, а в кольце $A[\alpha]$ существует элемент порядка 1 относительно $\mathfrak{P}$. В силу предложения 23 гл. I, § 7, заключаем, что $B = A[\alpha]$.

Этот результат доставляет критерий возможности применить предложение 2. Оно применимо, в частности, в локальном случае, когда наше дедекиндово кольцо полно.

Предложение 4. *Пусть* $\mathfrak{b}$ *— дробный идеал кольца* B. *Тогда*

$$\mathfrak{b}' = B'\mathfrak{b}^{-1}.$$

Доказательство. Имеем

$$\mathrm{Tr}\,(B'\mathfrak{b}^{-1}\mathfrak{b}) = \mathrm{Tr}\,(B'B) \subset A,$$

так что $B'\mathfrak{b}^{-1} \subset \mathfrak{b}'$. Обратное включение столь же очевидно.

Для удобства формулировки следующего предложения обозначим символом $B'_{E/K}$ модуль, дополнительный к B. Индекс нужен, потому что мы будем иметь дело больше чем с двумя полями.

Предложение 5. *Пусть* $E \supset F \supset K$ *— сепарабельные расширения,* C *— целое замыкание кольца* A *в поле* F, B *— целое замыкание кольца* A *в поле* E. *Тогда*

$$B'_{E/K} = B'_{E/F}C'_{F/K}.$$

Доказательство. Сначала установим включение $\supset$. Имеем

$$\mathrm{Tr}_K^E\,(B'_{E/F}C'_{F/K}A) = \mathrm{Tr}_K^F\mathrm{Tr}_F^E\,(B'_{E/F}C'_{F/K}B) =$$
$$= \mathrm{Tr}_K^F\,(C'_{F/K}\,\mathrm{Tr}_F^E\,(B'_{E/F}B)) \subset A,$$

откуда следует требуемое.

Обратно, пусть $\beta \in B'_{E/K}$. Тогда

$$\mathrm{Tr}_K^E\,(\beta B) = \mathrm{Tr}_K^F\,(C\,\mathrm{Tr}_F^E\,(\beta B)) \subset A$$

(можно вставить C, потому что $CB = B$). Тем самым

$$\mathrm{Tr}_F^E\,(\beta B) \subset C'_{F/K}$$

и

$$C'^{-1}_{F/K}\,\mathrm{Tr}_F^E\,(\beta B) \subset C.$$

Дробный C-идеал $C'^{-1}_{F/K}$ можно внести под знак оператора Tr^E_F, потому что он содержится в поле F. Следовательно,

$$\beta C'^{-1}_{F/K} \subset B'_{E/F}.$$

Умножая на $C'_{F/K}$, находим, что $\beta \in C'_{F/K} B'_{E/F}$; это завершает доказательство обратного включения.

В прежних обозначениях определим *дифференту* $\mathfrak{D}_{B/A}$ как $B'^{-1}_{E/K}$. Из доказанного результата получается формула

$$\mathfrak{D}_{B/C}\mathfrak{D}_{C/A} = \mathfrak{D}_{B/A},$$

выражающая *мультипликативность дифференты в башне расширений.*

Дифферента есть обращение дробного идеала, содержащего кольцо целых чисел, и потому она сама является идеалом.

Предложение 6. *Пусть S — мультипликативное подмножество кольца A. Тогда*

$$\mathfrak{D}_{S^{-1}B/S^{-1}A} = S^{-1}\mathfrak{D}_{B/A}.$$

Доказательство. Очевидно.

Предложение 6 позволяет вычислять дифференту покомпонентно, локализуя относительно простых идеалов. Преимущество этого способа состоит в том, что $A_\mathfrak{p}$ является кольцом главных идеалов.

Выясним теперь, как дифферента ведет себя при пополнении и как ее вычислять чисто локальными средствами.

Пользуясь предложением 6, мы можем считать, что A — дискретно нормированное кольцо.

Предложение 7. *Пусть A — дискретно нормированное кольцо, v — его нормирование, $\mathfrak{P}$ — простой идеал кольца B, лежащий над простым идеалом $\mathfrak{p}$ кольца A. Пусть $w_\mathfrak{P}$ — нормирование, соответствующее идеалу $\mathfrak{P}$; A_v, $B_{w_\mathfrak{P}}$ — соответствующие пополнения. Тогда*

$$\mathfrak{D}_{B/A} B_{w_\mathfrak{P}} = \mathfrak{D}_{B_{w_\mathfrak{P}}/A_v}.$$

Доказательство. Мы можем вместо дифферент рассматривать модули, дополнительные к кольцам. Поскольку дифференты являются идеалами, достаточно установить, что

$$\operatorname{ord}_{\mathfrak{P}} \mathfrak{D}_{B/A} = \operatorname{ord}_{\mathfrak{P}} \mathfrak{D}_{B_{w_{\mathfrak{P}}}/A_v}.$$

Пусть Tr — оператор следа из E в K, Tr_w — оператор локального следа из E_w в K_v, где w — любое нормирование поля E, индуцирующее v на K. Тогда

$$\mathrm{Tr} = \sum_{w \mid v} \mathrm{Tr}_w$$

(как оператор на E).

Пусть $x \in E_{w_{\mathfrak{P}}}$, и пусть $\mathrm{Tr}_{w_{\mathfrak{P}}}(xB_{w_{\mathfrak{P}}}) \subset A_v$. Выберем элемент $\xi \in E$, близкий к x относительно $w_{\mathfrak{P}}$ и близкий к нулю относительно других нормирований $w \mid v$. Пусть $y \in B$. Тогда элемент $\mathrm{Tr}_w(\xi y)$ близок к нулю, если $w \neq w_{\mathfrak{P}}$, и принадлежит кольцу A_v при $w = w_{\mathfrak{P}}$, потому что локальный след непрерывен. Отсюда вытекает, что элемент $\mathrm{Tr}(\xi y)$ принадлежит кольцу A и, следовательно, ξ лежит в дополнительном модуле B'.

Обратно, пусть $x \in B'$ и $y \in B_{w_{\mathfrak{P}}}$. Найдем элемент $\xi \in E$, близкий к x относительно $w_{\mathfrak{P}}$ и близкий к нулю относительно остальных нормирований $w \mid v$. Найдем также элемент $\eta \in B$, близкий к y относительно $w_{\mathfrak{P}}$ и близкий к нулю относительно остальных нормирований $w \mid v$. Тогда

$$\mathrm{Tr}(\xi\eta) = \mathrm{Tr}_{w_{\mathfrak{P}}}(\xi\eta) + \sum_{w \neq w_{\mathfrak{P}}} \mathrm{Tr}_w(\xi\eta).$$

Глобальный след слева лежит в A. Каждый член суммы справа лежит в A_v. Следовательно, $\mathrm{Tr}_{w_{\mathfrak{P}}}(\xi\eta)$ лежит в A_v. Поскольку элементы ξ, η близки к x, y соответственно, отсюда вытекает, что след $\mathrm{Tr}_{w_{\mathfrak{P}}}(xy)$ принадлежит кольцу A_v.

Приведенные рассуждения показывают, что множество B' плотно в $B'_{w_{\mathfrak{P}}}$ (локально дополнительный

модуль относительно следа $\mathrm{Tr}_{w_{\mathfrak{P}}}$), откуда и следует наше предложение.

Пусть $\mathfrak{D}$ — дифферента кольца B над A. С точки зрения формальных идеалов имеет место разложение

$$\mathfrak{D} = \prod_{\mathfrak{P}} \mathfrak{D}_{\mathfrak{P}}.$$

Каждый идеал $\mathfrak{D}_{\mathfrak{P}}$ можно интерпретировать как $\mathfrak{P}$-компоненту дифференты $\mathfrak{D}_{B/A}$, дифференты $\mathfrak{D}_{B_{\mathfrak{P}}/A_{\mathfrak{P}}}$ (если $\mathfrak{P} \mid \mathfrak{p}$) или как дифференту $\mathfrak{D}_{B_w/A_w}$, где w и v — нормирования, определенные идеалами $\mathfrak{P}$ и $\mathfrak{p}$ соответственно.

Обычно идеал $\mathfrak{D}_{B/A}$ называют *глобальной дифферентой*, а $\mathfrak{D}_{B_w/A_v}$ — *локальной дифферентой*. Мы можем отождествить $\mathfrak{D}_{B_w/A_v}$ и $\mathfrak{D}_{\mathfrak{P}}$ как формальные идеалы и в этом смысле утверждать, что глобальная дифферента является произведением локальных дифферент.

§ 2. Дифферента и ветвление

В этом параграфе A — дедекиндово кольцо, K — его поле частных, E — конечное сепарабельное расширение поля K, B — целое замыкание кольца A в поле E. Мы примем, кроме того, что для всякого простого идеала $\mathfrak{p} \subset A$ поле классов вычетов $A/\mathfrak{p}$ совершенно.

Предложение 8. *Пусть $\mathfrak{P}$ — простой идеал кольца B, лежащий над $\mathfrak{p}$, e — его индекс ветвления. Тогда идеал $\mathfrak{P}^{e-1}$ делит дефференту $\mathfrak{D}_{B/A}$. Если идеал $\mathfrak{P}$ сильно разветвлен, то идеал $\mathfrak{P}^e$ делит дифференту $\mathfrak{D}_{B/A}$. Если идеал $\mathfrak{P}$ не разветвлен, то $\mathfrak{P}$ не делит $\mathfrak{D}_{B/A}$. Существует только конечное число разветвленных простых идеалов. Наконец, дифферента $\mathfrak{D}_{B/A}$ является наибольшим общим делителем всех идеалов $(f'(\alpha))$, где α — целая образующая поля E над K, а f — соответствующий неприводимый многочлен над K, корнем которого является α.*

Доказательство. Так как инварианты ветвления и дифференты хорошо ведут себя при локализации и пополнении, то первые утверждения можно доказывать, считая, что K — полное поле.

Имея дело с полным полем, можно применить предложение 3, § 1, следствие из предложения 2 и предложение 23 гл. I, § 7. Если идеал $\mathfrak{P}$ неразветвлен, это дает $\mathfrak{D}_{B/A}=(1)$. Пользуясь предложением 5, § 1 (мультипликативность относительно башни), мы можем считать также, что идеал $\mathfrak{P}$ вполне разветвлен. В этом случае $B=A[\Pi]$, где Π — некоторый элемент порядка 1 относительно $\mathfrak{P}$, удовлетворяющий уравнению Эйзенштейна

$$f(\Pi)=\Pi^e+a_{n-1}\Pi^{e-1}+\ldots+\pi=0,$$

в котором $a_i\in\mathfrak{p}$, а $\pi\in A$ имеет порядок 1 относительно $\mathfrak{p}$. Тогда

$$f'(\Pi)\equiv e\Pi^{e-1}\pmod{\mathfrak{P}^e},$$

и последнее утверждение вытекает из определений.

Вернемся теперь к глобальному случаю. Пусть α — целая образующая поля E над K и f — соответствующий неприводимый многочлен над K. Элемент $f'(\alpha)$ делится только на конечное число простых идеалов $\mathfrak{P}$, и из предложения 7 гл. II, § 4, следует, что только эти простые делители могут ветвиться (мы можем рассматривать α как образующую пополнения $E_{w_{\mathfrak{P}}}$ над $K_{v_{\mathfrak{p}}}$). Так как $B\supset A[\alpha]$, отсюда следует, что $\mathfrak{D}_{B/A}$ делит $(f'(\alpha))$. Остается доказать, что дифферента совпадает с наибольшим общим делителем всех таких идеалов. Точнее, для всякого простого идеала $\mathfrak{P}$ существует такой элемент α, для которого

$$\operatorname{ord}_{\mathfrak{P}}\mathfrak{D}_{B/A}=\operatorname{ord}_{\mathfrak{P}}(f'(\alpha)).$$

Доказательство представляет собой упражнение в технике применения теоремы о приближениях.

Все получилось бы сразу, если бы мы могли положить $B=A[\alpha]$ для некоторого α. Это можно сделать только локально. Поэтому мы воспользуемся теоремой о приближениях для сведения задачи к локальной.

Пусть $v=v_{\mathfrak{p}}$, $w=w_{\mathfrak{P}}$. Пусть $\{\sigma\}$ пробегает все различные автоморфизмы поля E в алгебраическое замыкание $\overline{K}_v$ поля K_v. Пусть σ_1 — один из таких изоморфизмов, индуцирующий на E нормирование $w_{\mathfrak{P}}$. Для всякой обра-

зующей α поля E над K, являющейся корнем неприводимого над K многочлена f, имеем

$$\sigma_1 f'(\alpha) = f'(\sigma_1\alpha) = \prod_{\sigma \neq \sigma_1} (\sigma_1\alpha - \sigma\alpha).$$

Будем писать $\sigma \sim \tau$, если σ и τ сопряжены над K_v, т. е. если существует такой изоморфизм λ поля $\overline{K}_v$ над K_v, что $\tau = \lambda\sigma$ на E.

Согласно предложению 3, § 1, существует такой элемент $\beta \in B_w$, что $B_w = A_v[\beta]$. Заметим, что всякий элемент кольца B_w, достаточно близкий к β, также порождает B_w над A_v.

Пусть λ пробегает все изоморфизмы поля $\overline{K}_v$ над K_v. Существует такой элемент $a \in A_v$, что

$$|\lambda\beta - a| = 1$$

для всех λ. Действительно, классы вычетов всех сопряженных элементов $\lambda\beta$ сопряжены над $A_v/\mathfrak{p}_v$. Если эти классы вычетов все равны 0, то можно взять $a = 1$, иначе $a = 0$.

Пусть $\sigma_1, \ldots, \sigma_n$ — представители классов эквивалентности вложений поля E в $\overline{K}_v$. В силу теоремы о приближениях можно найти такой элемент $\alpha \in E$, для которого

число $|\sigma_1\alpha - \beta|$ очень мало,

числа $|\sigma_i\alpha - \alpha|$ очень малы при $i \neq 1$.

Не теряя общности, можно считать, кроме того, что элемент α цел над A и что $E = K(\alpha)$. (Если это не так, сначала умножим α на элемент кольца A, который $\equiv 1 \pmod{\mathfrak{p}}$ и делится на большие степени других простых идеалов, чтобы сделать α целым, а затем прибавим $\pi^\nu\gamma$, где γ — любая целая образующая, а ν — достаточно большое целое число. Элемент $\alpha + \pi^\nu\gamma$ будет образующей.)

Так как элемент $\sigma_1\alpha$ близок к β, имеем $B_w = A_v[\sigma_1\alpha]$, и, следовательно, его доля в $\mathfrak{P}$-компоненте дифферента имеет вид

$$\operatorname{ord}_{\mathfrak{P}} \mathfrak{D}_{B_w/A_v} = \operatorname{ord}_{\mathfrak{P}} \prod_{\substack{\sigma \sim \sigma_1 \\ \sigma \neq \sigma_1}} (\sigma_1\alpha - \sigma\alpha).$$

Мы должны установить, что остальные множители не дают вклада в $\mathfrak{P}$-компоненту.

Пусть σ не сопряжен с σ_1 над K_v. Положим $\sigma = \lambda\sigma_i$, $i \neq 1$. Тогда

$$|\sigma_1\alpha - \sigma\alpha| = |\sigma_1\alpha - \lambda\sigma_i\alpha| = |\lambda^{-1}\sigma_1\alpha - \sigma_i\alpha| = \\ = |\lambda^{-1}\sigma_1\alpha - a + a - \sigma_i\alpha|.$$

Но число $|\sigma_i\alpha - a|$ очень мало, а $\lambda^{-1}\sigma_1\alpha$ очень близко к $\lambda^{-1}\beta$. Так как $|\lambda^{-1}\beta - a| = 1$, то и $|\lambda^{-1}\sigma_1\alpha - a| = 1$. Следовательно, $|\sigma_1\alpha - \sigma\alpha| = 1$. Отсюда вытекает последнее утверждение.

§ 3 Дискриминант

На протяжении этого параграфа A — дедекиндово кольцо, K — его поле частных, E — конечное сепарабельное расширение поля K степени n, B — целое замыкание кольца A в поле E.

Пусть $W = (w_1, \ldots, w_n)$ — любое семейство из n элементов поля E. Определим *дискриминант* этого семейства

$$D_{E/K}(W) = \det(\sigma_i w_j)^2$$

как квадрат определителя: σ_i пробегает n различных вложений поля E в данное алгебраическое замыкание поля K.

Пусть W и $V = (v_1, \ldots, v_n)$ — два семейства элементов поля E; предположим, что существует матрица $X = (x_{ij})$ элементов поля K, для которой $W = XV$. Тогда

$$D_{E/K}(W) = (\det X)^2 D_{E/K}(V).$$

Если все элементы матрицы X принадлежат A, то и $(\det X)^2 \in A$. Поэтому в случае, когда W и V порождают один и тот же A-модуль, матрица X обратима в кольце A, и ее определитель является единицей в A. Тем самым соответствующие определители отличаются на квадрат единицы.

В частности, при $A = \mathbf{Z}$ (кольцо обычных целых чисел) дискриминант однозначно определяется модулем. Дискриминант кольца целых алгебраических чисел I_K как I_K-модуля будет называться просто *дискриминантом* (или дискриминантом поля K) и обозначаться символом D_K.

Предложение 9. *Дискриминант* $D_{E/K}(W)$ *принадлежит полю* K *и даже кольцу* A, *если все элементы семейства* W *принадлежат* B. *Дискриминант отличен от нуля в том и только том случае, когда семейство* W *составляет базис поля* E *над* K.

Доказательство. Применение к $\det(\sigma_i w_j)$ любого изоморфизма поля E над K переставляет строки и потому сводится к умножению определителя на ± 1; возведение в квадрат избавляет от этого множителя. Для всякой образующей α поля E над K дискриминант $D_{E/K}(1, \alpha, \ldots, \alpha^{n-1})$ есть квадрат определителя Вандермонда и потому не равен нулю. То же относится, следовательно, к любому базису V поля E над K в силу сделанного выше замечания об изменении дискриминанта при линейных преобразованиях. Если элементы семейства W линейно зависимы над K, дискриминант, очевидно, равен нулю. Если все они целы над A, то и дискриминант, очевидно, принадлежит A (целое замыкание кольца A в любом нормальном расширении поля K, содержащем E, является кольцом). Предложение доказано.

Пусть M — свободный модуль ранга n над кольцом A, содержащийся в поле E. Введем дискриминант модуля M как дискриминант любого его A-базиса; определение однозначно с точностью до квадрата единицы кольца A.

Предложение 10. *Пусть* $M_1 \subset M_2$ — *свободные модули ранга* n *над кольцом* A, *содержащиеся в поле* E. *Тогда* $D_{E/K}(M_1)$ *делит* $D_{E/K}(M_2)$ (*как главный идеал*). *Если для некоторой единицы* $u \in A$ *выполняется равенство* $D_{E/K}(M_1) = D_{E/K}(M_2)u$, *то* $M_1 = M_2$.

Доказательство. Первое утверждение очевидно. Из второго условия следует, что матрица перехода от базиса модуля M_1 к базису модуля M_2 обратима в кольце A, так что $M_1 = M_2$.

Вообще говоря, существуют дробные идеалы кольца B, не являющиеся свободными A-модулями. Поэтому для любого дробного идеала $\mathfrak{b}$ кольца B символом $D_{E/K}(\mathfrak{b})$ мы обозначим A-модуль, порожденный дискриминантами $D_{E/K}(W)$ всевозможных базисов W поля E над K,

принадлежащих идеалу $\mathfrak{b}$. Модуль $D_{E/K}(\mathfrak{b})$ назовем *дискриминантом дробного идеала* $\mathfrak{b}$. Так как существует элемент $c \in A$, $c \neq 0$, с условием $c\mathfrak{b} \subset B$, то дискриминант является дробным идеалом кольца A.

Предложение 11. *Пусть* $\mathfrak{b}$ *— дробный идеал кольца* B, S *— мультипликативное подмножество кольца* A. *Тогда*

$$S^{-1}D_{E/K}(\mathfrak{b}) = D_{E/K}(S^{-1}\mathfrak{b}).$$

Доказательство. Тривиальное следствие определений.

Этот результат позволяет пользоваться локализацией. Для всякого простого идеала $\mathfrak{p} \subset A$ можно вычислить $\mathfrak{p}$-компоненту дискриминанта, локализуя по $\mathfrak{p}$. Значительное преимущество локального случая состоит в том, что $A_{\mathfrak{p}}$ — дискретно нормированное кольцо, а любой дробный идеал кольца B превращается в свободный $A_{\mathfrak{p}}$-модуль. Далее, $B_{\mathfrak{p}}$ — кольцо главных идеалов, имеющее только конечное число идеалов, лежащих над $\mathfrak{p}$. Тем самым дело сводится к подсчету определителей Вандермонда.

Предложение 12. *Пусть* A *— дискретно нормированное кольцо,* $\mathfrak{b}$ *— дробный идеал кольца* B, $\mathfrak{b} = (\beta)$, $\beta \in E$, $B \neq 0$. *Тогда*

$$D_{E/K}(\mathfrak{b}) = (N_K^E(\beta))^2 D_{E/K}(B).$$

Доказательство. Пусть W является A-базисом кольца B. Тогда βW будет A-базисом идеала $\mathfrak{b}$, и результат следует из определений.

С помощью процесса локализации мы можем распространить это предложение на случай не обязательно локального кольца.

Предложение 13. *Пусть* A *— любое дедекиндово кольцо,* $\mathfrak{b}$ *— дробный идеал кольца* B. *Тогда*

$$D_{E/K}(\mathfrak{b}) = (N_K^E(\mathfrak{b}))^2 D_{E/K}(B);$$

норма идеала определена в гл. I, § 7.

Доказательство. Достаточно проверить это утверждение для всякой $\mathfrak{p}$-компоненты дискриминанта, $\mathfrak{p}$ —

простой идеал кольца A. Поэтому можно считать, что A — дискретно нормированное кольцо (предложение 11). В этом случае $\mathfrak{b} = (\beta)$, $\beta \in E$, и требуемый результат следует из предложения 23 гл. I, § 7.

Предложение 14. *Дискриминант и дифферента связаны формулой*

$$N_K^E \mathfrak{D}_{B/A} = D_{E/K}(B).$$

Доказательство. В силу предложения 6, § 1, и предложения 11 мы можем считать, что A — дискретно нормированное кольцо и тем самым B — свободный A-модуль. Для любого A-базиса W кольца B дискриминант $D_{E/K}(B)$ порожден элементом $D_{E/K}(W)$. Пусть W' — дополнительный к W базис относительно оператора следа. Тогда дополнительный модуль B' порожден над W' базисом A. Поэтому $D_{E/K}(B') = D_{E/K}(W')A$. Из определения дискриминанта базиса непосредственно видно, что

$$D_{E/K}(W) D_{E/K}(W') = 1.$$

Следовательно, $D_{E/K}(B) D_{E/K}(B') = A$. Пользуясь предложением 4, § 1, и предложением 13, получаем требуемое.

Наконец, рассмотрим конечное сепарабельное расширение E поля K степени n; пусть $\beta \in E$, $\beta \neq 0$ и $E = K(\beta)$. Введем *дифференту* $\mathfrak{D}_{E/K}(\beta)$ и *дискриминант* $D_{E/K}(\beta)$ элемента β формулами

$$\mathfrak{D}_{E/K}(\beta) = \prod_{\sigma \neq \mathrm{id}} (\beta - \sigma\beta),$$

$$D_{E/K}(\beta) = D_{E/K}(1, \beta, \ldots, \beta^{n-1}).$$

Предложение 15. *Имеем*

$$D_{E/K}(\beta) = (-1)^{n(n-1)/2} N_K^E \mathfrak{D}_{E/K}(\beta).$$

Доказательство. Упражнение на перестановку строк определителя.

Глава IV

КРУГОВЫЕ ПОЛЯ

Эта глава служит одновременно двум целям. Она доставляет примеры к общей теории и, кроме того, более подробно описывает поля деления круга, от которых в значительной мере зависит теория алгебраических чисел в целом. Трудно указать точные границы этой зависимости; известно, однако, что, скажем, центральная часть доказательств в теории полей классов относится к круговым полям. Хотя мы не излагаем здесь теорию полей классов, мы приводим лемму Артина, которую он использовал в своем первоначальном доказательстве закона взаимности. Эта лемма представляет собой хорошую иллюстрацию некоторых общих принципов в теории числовых полей. Я воспроизвожу доказательство этой леммы, данное Артином около десяти лет назад на семинаре в Принстонском университете.

§ 1. Корни из единицы

Пусть ω — корень n-й степени из единицы: $\omega^n = 1$. Расширение $\mathbf{Q}(\omega)$ нормально над $\mathbf{Q}$. В самом деле, пусть ω — примитивный корень (т. е. его период равен в точности n), σ — любой изоморфизм поля $\mathbf{Q}(\omega)$ над $\mathbf{Q}$. Тогда $(\sigma\omega)^n = \sigma(\omega^n) = 1$, так что $\sigma\omega$ — также корень n-й степени из единицы. Следовательно, $\sigma\omega = \omega^i$ для некоторого целого числа $i = i(\sigma)$, которое определено однозначно $\bmod n$. Поэтому поле $\mathbf{Q}(\omega)$ отображается в себя при применении σ и, значит, является нормальным над $\mathbf{Q}$. Для любого другого изоморфизма τ поля $\mathbf{Q}(\omega)$ над $\mathbf{Q}$ имеем $\sigma\tau\omega = \omega^{i(\sigma)i(\tau)}$. Так как σ, τ — изоморфизмы, то числа $i(\sigma)$, $i(\tau)$ взаимно просты с n. Тем самым отображение

$$\sigma \rightsquigarrow i(\sigma)$$

является гомоморфизмом группы Галуа G поля $\mathbf{Q}(\omega)$ над $\mathbf{Q}$ в мультипликативную группу классов вычетов $\bmod n$, взаимно простых с n, и этот гомоморфизм мономорфен. Порядок этой мультипликативной группы равен $\varphi(n)$, где φ — функция Эйлера. Ниже мы убедимся, что $[\mathbf{Q}(\omega):\mathbf{Q}] = \varphi(n)$. Отсюда будет следовать, что группа Галуа расширения $\mathbf{Q}(\omega)/\mathbf{Q}$ определена изоморфизмом $\sigma \rightsquigarrow i(\sigma)$.

Пусть K — любое числовое поле. Группа Галуа поля $K(\omega)$ над K является подгруппой группы G; поэтому она абелева.

Пусть K — любое числовое поле; фиксируем его алгебраическое замыкание $\overline{K}$. *Круговым расширением* поля K называется всякое расширение, содержащееся в одном из полей $K(\omega)$, где ω — корень из единицы ($\omega^n = 1$ для некоторого n). Поскольку поле $K(\omega)$ абелево над K, всякое круговое расширение поля K абелево. Поле K называется *круговым*, если оно является круговым расширением поля $\mathbf{Q}$.

Рассмотрим случай $K = \mathbf{Q}(\omega)$.

Пусть p — простое число, ω — примитивный корень p-й степени из единицы. Тогда ω — корень многочлена

$$X^p - 1 = (X-1)(X^{p-1} + \ldots + 1).$$

Следовательно, $[\mathbf{Q}(\omega):\mathbf{Q}] \leqslant p-1$. Мы утверждаем, что

$$[\mathbf{Q}(\omega):\mathbf{Q}] = p-1.$$

Действительно, пусть $\pi = 1-\omega$. Число π цело над $\mathbf{Z}$. Для любого целого числа i, взаимно простого с p, ω^i — тоже примитивный корень p-й степени из единицы, и

$$\frac{1-\omega^i}{1-\omega} = 1 + \omega + \ldots + \omega^{i-1}$$

— целое алгебраическое число. Но $\omega = (\omega^i)^j$ для некоторого целого числа j, так что это отношение является единицей в кольце I_K целых чисел поля K.

Пусть $\mathfrak{p}$ — простой идеал кольца I_K, лежащий над (p), и

$$f(X) = X^{p-1} + \ldots + 1.$$

Тогда ω^i $(i=1, \ldots, p-1)$ — все корни $f(X)$ (ибо это — корни многочлена X^p-1), так что

$$f(X)=\prod_{i=1}^{p-1}(X-\omega^i).$$

Поэтому

$$p=f(1)=\prod_{i=1}^{p-1}(1-\omega^i).$$

Для любых i, j, взаимно простых с p, как мы уже убедились, отношение

$$\frac{1-\omega^i}{1-\omega^j}$$

является единицей кольца I_K. Все элементы $1-\omega^i$ имеют одну и ту же $\mathfrak{p}$-адическую норму $|\ |=|\ |_{\mathfrak{p}}$, так что

$$|\pi|^{p-1}=|p|.$$

Отсюда следует, что индекс ветвления идеала $\mathfrak{p}$ не меньше, чем $p-1$. В силу предложения 20 гл. I, § 7, получаем

$$e_{\mathfrak{p}}=p-1=[\mathbf{Q}(\omega):\mathbf{Q}].$$

Кроме того, $\mathfrak{p}$ — единственный простой идеал кольца I_K, лежащий над (p), и он вполне разветвлен. Так как ω удовлетворяет также уравнению $X^p-1=0$, любое простое число, отличное от p, неразветвлено в поле $\mathbf{Q}(\omega)$, потому что производная $p\omega^{p-1}$ делится только на p.

Рассмотрим теперь случай степени простого числа: $m=p^r$, $r>0$ — целое число. Положим $Y=X^{p^{r-1}}$ и рассмотрим разложение

$$X^{p^r}-1=Y^p-1=(Y-1)(Y^{p-1}+\ldots+1).$$

Положим

$$f(X)=\frac{X^{p^r}-1}{X^{p^{r-1}}-1}=Y^{p-1}+\ldots+1.$$

Степень многочлена f равна $\varphi(p^r)=(p-1)p^{r-1}$. Пусть ω — примитивный корень p^r-й степени из единицы; ω^i является примитивным корнем p^r-й степени из единицы в том и только том случае, когда i взаимно просто с p.

Таким образом, существует $\varphi(p^r)$ примитивных корней p^r-й степени из единицы. Поэтому

$$f(X)=\prod_{\zeta}(X-\zeta)=\prod_{i}(X-\omega^i),$$

где первое произведение берется по всем примитивным корням p^r-й степени из единицы, а второе — по всем различным классам вычетов $\mathbf{Z}/p^r\mathbf{Z}$, не кратным p.

Так же, как для корней p-й степени, проверяется, что отношение

$$\frac{1-\omega^i}{1-\omega^j}$$

является единицей, если числа i, j взаимно просты с p. Пусть $\pi=1-\omega$. Тогда из тождества

$$f(1)=p=\prod(1-\omega^i)$$

вытекает, что

$$|\pi|^{\varphi(p^r)}=|p|$$

для любого нормирования, продолжающего p-адическое нормирование поля $\mathbf{Q}$, так что идеал p вполне разветвлен. Поэтому имеет место

Теорема 1. *Пусть ω — примитивный корень p^r-й степени из единицы, $K=\mathbf{Q}(\omega)$. Тогда $[K:\mathbf{Q}]=\varphi(p^r)=(p-1)\,p^{r-1}$. Над p лежит единственный простой идеал $\mathfrak{p}$ кольца I_K, и он вполне разветвлен. Все остальные простые идеалы кольца I_K неразветвлены.*

Этот результат можно обобщить следующим образом.

Теорема 2. *Пусть m — положительное целое число, ω — примитивный корень m-й степени из единицы. Тогда $[\mathbf{Q}(\omega):\mathbf{Q}]=\varphi(m)$. В поле $\mathbf{Q}(\omega)$ ветвятся только те простые числа p, которые делят m. Пусть*

$$m=p_1^{r_1}\ldots p_s^{r_s}$$

— разложение m в произведение степеней простых чисел, ω_j — примитивный корень p^{r_j}-й степени из единицы. Тогда

$$\mathbf{Q}(\omega)=\mathbf{Q}(\omega_1,\ldots,\omega_s)=\mathbf{Q}(\omega_1)\ldots\mathbf{Q}(\omega_s).$$

Доказательство. Пусть $g(X)=X^m-1$. Тогда ω — корень уравнения $g(X)=0$, а $g'(\omega)=m\omega^{m-1}$ делится

на простые числа, делящие m. Поэтому любое другое простое число неразветвлено в поле $\mathbf{Q}(\omega)$. Для всякого $j>1$ поле $\mathbf{Q}(\omega_j)$ абелево над $\mathbf{Q}$, а его пересечение с $\mathbf{Q}(\omega_1, \ldots, \omega_{j-1})$ равно $\mathbf{Q}$, потому что p_j вполне разветвлено в поле $\mathbf{Q}(\omega_j)$ и не разветвлено в другом поле. Поэтому степень расширения $\mathbf{Q}(\omega_1, \ldots, \omega_j)$ поля $\mathbf{Q}(\omega_1, \ldots, \omega_{j-1})$ равна $\varphi(p^{r_j})$. Это доказывает теорему.

Пусть G — группа Галуа поля $\mathbf{Q}(\omega)$ над $\mathbf{Q}$. Тогда любой автоморфизм σ этого поля отображает ω на некоторый примитивный корень ω^i, i взаимно просто с m. Так как $[\mathbf{Q}(\omega):\mathbf{Q}]=\varphi(m)$, то для любого такого i существует $\sigma\in G$ с условием $\sigma\omega=\omega^i$. Таким образом, группа G изоморфна мультипликативной группе классов вычетов кольца $\mathbf{Z}/m\mathbf{Z}$, взаимно простых с m. Заметим еще, что для любых двух положительных взаимно простых целых чисел m, n и соответствующих примитивных корней из единицы ζ_n, ζ_m имеем $\mathbf{Q}(\zeta_n)\cap\mathbf{Q}(\zeta_m)=\mathbf{Q}$.

Теорема 3. *Пусть ω — примитивный корень p^r-й степени из единицы, $K=\mathbf{Q}(\omega)$. Тогда $I_K=\mathbf{Z}[\omega]$. Дискриминант поля K равен*

$$D_K=\pm p^{p^{r-1}(pr-r-1)},$$

где знак минус относится к случаям $p^r=4$ или $p\equiv 3 \pmod 4$, плюс — к остальным случаям.

Доказательство. Ограничимся случаем $r=1$; принцип доказательства в общем случае тот же. Итак, ω — корень p-й степени из единицы; пусть $B=\mathbf{Z}[\omega]$. Для доказательства того, что $B=I_K$, достаточно проверить, что дискриминанты колец B и I_K совпадают как $\mathbf{Z}$-идеалы (предложение 10 гл. III, § 3). А это достаточно проверить локально для каждого простого числа. Все простые числа, кроме p, не разветвлены и потому не вносят вклада в дискриминант ни одного из колец I_K, B. Число p вполне разветвлено; пользуясь предложением 23 гл. I, § 7, заключаем, что $S_p^{-1}B=S_p^{-1}I_K$, где S_p — дополнение к идеалу (p) кольца $\mathbf{Z}$. Следовательно, p-компоненты дискриминантов в обоих случаях одинаковы. Поэтому $B=I_K$. Утверждение о точном значении дискриминанта получается прямым вычислением дис-

криминанта элемента ω с учетом знака. Это не составляет трудности (воспользоваться предложением 15 гл. III, § 3).

Для работы с произвольным составным целым числом m нам понадобится один общий результат.

Теорема 4. *Пусть K, E — два числовых поля. Предположим, что они линейно разделены (это означает, что для любого базиса $w_1, \ldots, w_n$ поля K над $\mathbf{Q}$ и любого базиса $v_1, \ldots, v_m$ поля E над $\mathbf{Q}$ система $\{w_i v_j\}$ составляет базис поля KE над $\mathbf{Q}$) и что их дискриминанты взаимно просты. Тогда*

$$I_{KE} = I_K I_E$$

и

$$D_{KE} = D_K^m D_E^n.$$

Доказательство. Из основных свойств дифференты следует, что дифферента $\mathfrak{D}_{KE/\mathbf{Q}}$ равна

$$\mathfrak{D}_{KE/K}\mathfrak{D}_{K/\mathbf{Q}} = \mathfrak{D}_{KE/E}\mathfrak{D}_{E/\mathbf{Q}}.$$

Но дифференты $\mathfrak{D}_{E/\mathbf{Q}}$ и $\mathfrak{D}_{K/\mathbf{Q}}$ взаимно просты (как идеалы кольца I_{KE}). То же верно для других двух множителей. Следовательно,

$$\mathfrak{D}_{KE/E} = \mathfrak{D}_{K/\mathbf{Q}} \quad \text{и} \quad \mathfrak{D}_{KE/K} = \mathfrak{D}_{E/\mathbf{Q}}.$$

Пусть W — базис кольца I_K над $\mathbf{Z}$, V — базис кольца I_E над $\mathbf{Z}$. Из приведенного замечания следует, что дополнительный к W базис W', который порождает идеал $\mathfrak{D}_{K/\mathbf{Q}}^{-1}$, порождает также идеал $\mathfrak{D}_{KE/E}^{-1}$. Это модуль, дополнительный к I_{KE} над I_E.

Беря снова дополнительный модуль, получаем, что W порождает кольцо I_{KE} над I_E. Это доказывает утверждение о кольцах целых чисел. Утверждение о дискриминантах мы оставляем читателю в качестве упражнения.

Следствие. *Пусть m — положительное целое число, ω — примитивный корень m-й степени из единицы. Тогда $\mathbf{Z}[\omega]$ — целое замыкание кольца $\mathbf{Z}$ в поле $\mathbf{Q}(\omega)$.*

Доказательство. Очевидно, композит колец целых чисел круговых полей, степени которых являются степенями простых чисел, делящих m, удовлетворяет условиям теоремы 4.

§ 2. Квадратичные поля

Расширения степени 2 поля рациональных чисел также доставляют интересные примеры.

Теорема 5. *Пусть m — ненулевое целое число, не делящееся на квадрат простого, $K=\mathbf{Q}(\sqrt{m})$. Если $m\equiv 2$ или $m\equiv 3 \pmod 4$, то $[1, \sqrt{m}]$ составляет базис кольца I_K над $\mathbf{Z}$. Если $m\equiv 1 \pmod 4$, то таким базисом является система*

$$\left[1, \frac{1+\sqrt{m}}{2}\right].$$

Доказательство. Упражнение. Для того чтобы элемент $x+y\sqrt{m}$ с $x, y\in\mathbf{Q}$ был цел над $\mathbf{Z}$, необходимо и достаточно, чтобы его норма и след принадлежали $\mathbf{Z}$. С помощью этого соображения легко проверить утверждение теоремы.

Например, при $m=-3$ число

$$\frac{1+\sqrt{-3}}{2}$$

является кубическим корнем из единицы. Поэтому оно цело над $\mathbf{Z}$.

Прежде чем доказывать следующий результат, сделаем несколько замечаний о конечных полях.

Пусть $\mathbf{F}_q$ — конечное поле из q элементов, где q — степень нечетного простого числа p. Мультипликативная группа $\mathbf{F}_q^*$ циклична и имеет порядок $q-1$. Поэтому

$$(\mathbf{F}_q^* : \mathbf{F}_q^{*2}) = 2.$$

Для любого ненулевого целого числа ν положим

$$\left(\frac{\nu}{p}\right) = \begin{cases} 1, & \text{если } \nu \equiv x^2 \pmod p, \\ -1, & \text{если } \nu \not\equiv x^2 \pmod p. \end{cases}$$

Это — определение символа Лежандра, который зависит лишь от класса вычетов $\nu \pmod p$.

Из замечания об индексе следует, что число вычетов равно числу невычетов.

Теорема 6. *Пусть* ζ *— примитивный корень степени* p *из единицы,*

$$S=\sum_{\nu}\left(\frac{\nu}{p}\right)\zeta^{\nu},$$

где сумма взята по ненулевым классам вычетов $\bmod p$. *Тогда*

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

Каждое квадратичное расширение поля $\mathbf{Q}$ *является круговым полем.*

Доказательство. Последнее утверждение немедленно вытекает из явного представления числа $\pm p$ как квадрата в поле $\mathbf{Q}(\zeta)$. Это представление получается так:

$$S^2=\sum_{\nu,\mu}\left(\frac{\nu\mu}{p}\right)\zeta^{\mu+\nu}.$$

Когда ν пробегает все ненулевые классы, а μ фиксировано, $\nu\mu$ тоже пробегает все ненулевые классы. Заменяя ν на $\nu\mu$, находим

$$S^2=\sum_{\nu,\mu}\left(\frac{\nu\mu^2}{p}\right)\zeta^{\mu(\nu+1)}=\sum_{\nu,\mu}\left(\frac{\nu}{p}\right)\zeta^{\mu(\nu+1)}=$$

$$=\sum_{\mu}\left(\frac{-1}{p}\right)\zeta^{0}+\sum_{\nu\neq -1}\left(\frac{\nu}{p}\right)\sum_{\mu}\zeta^{\mu(\nu+1)}.$$

Но $1+\zeta+\ldots+\zeta^{p-1}=0$, так что внутренняя сумма по μ справа равна -1. Следовательно,

$$S_2=\left(\frac{-1}{p}\right)(p-1)+(-1)\sum_{\nu\neq -1}\left(\frac{\nu}{p}\right)=$$

$$=p\left(\frac{-1}{p}\right)+\sum_{\nu}\left(\frac{\nu}{p}\right)=\left(\frac{-1}{p}\right)p,$$

что и требовалось доказать.

Тем самым поле $\mathbf{Q}(\sqrt{p})$ содержится либо в поле $\mathbf{Q}(\zeta, \sqrt{-1})$, либо в поле $\mathbf{Q}(\zeta)$ в зависимости от знака символа $\left(\frac{-1}{p}\right)$. В действительности всякое абелево расширение поля $\mathbf{Q}$ является круговым, что, однако, гораздо труднее доказать (см. [3]). Это — теорема Кронекера.

§ 3. Символ Артина

Пусть k — числовое поле, K — расширение Галуа с группой G. Пусть $\mathfrak{p}$ — простой идеал кольца I_k, $\mathfrak{P}$ — простой идеал кольца I_K, лежащий над $\mathfrak{p}$. Поле классов вычетов $I_k/\mathfrak{p}$ конечно и имеет, по определению, $\mathbf{N}\mathfrak{p}$ элементов. Существует единственный автоморфизм σ' поля $I_K/\mathfrak{P}$ над $I_k/\mathfrak{p}$, для которого $\sigma x = x^{\mathbf{N}\mathfrak{p}}$ при всех $x \in I_K/\mathfrak{P}$.

Пусть идеал $\mathfrak{P}$ неразветвлен над $\mathfrak{p}$. Согласно предложению 14 гл. I, § 5, в группе разложения $G_{\mathfrak{P}}$ существует единственный элемент σ, индуцирующий σ' на поле классов вычетов. Этот элемент обозначается символом $(\mathfrak{P}, K/k)$.

Пусть $\mathfrak{Q}$ — другой простой идеал, лежащий над $\mathfrak{p}$, и $\tau\mathfrak{P} = \mathfrak{Q}$. Тогда элементы $(\mathfrak{Q}, K/k)$ и $(\mathfrak{P}, K/k)$ сопряжены в группе G. Следовательно, если поле K абелево над k, группы разложения $G_{\mathfrak{P}}$ и $G_{\mathfrak{Q}}$ совпадают и $(\mathfrak{P}, K/k) = (\mathfrak{Q}, K/k)$. Тем самым этот элемент группы $G_{\mathfrak{P}}$ определен однозначно; он обозначается символом

$$(\mathfrak{p}, K/k)$$

и называется *символом Артина* (*или автоморфизмом Фробениуса*) идеала $\mathfrak{p}$ в группе G. Его можно отождествлять с соответствующим автоморфизмом расширения поля классов вычетов.

В качестве примера рассмотрим поля $k = \mathbf{Q}$ и $K = \mathbf{Q}(\zeta_m)$, где $m > 1$ — целое число, ζ_m — примитивный корень из единицы степени m. Пусть p — простое число, не делящее m. Оно неразветвлено в поле K. Положим $\sigma = (p, K/\mathbf{Q})$. Тогда $\sigma\zeta_m = \zeta_m^p$.

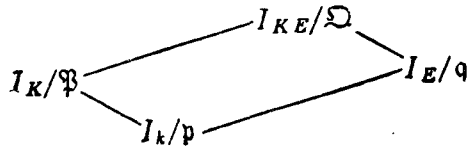
Закон взаимности Артина позволяет определить все $\mathfrak{p}$, имеющие фиксированный символ Артина. Для расширений $\mathbf{Q}(\zeta_m)$ символ Артина зависит от класса вычетов $p \pmod m$. Аналогичное утверждение имеется в общем

случае, но мы не будем входить в подробности. Ограничимся доказательством следующего результата.

Предложение 1. *Пусть k — числовое поле, K — его абелево расширение, E — конечное расширение, $\mathfrak{p}$ — простой идеал кольца I_K, неразветвленный в поле KE. Пусть $\mathfrak{q}$ — идеал кольца I_E, лежащий над $\mathfrak{p}$. Тогда ограничение автоморфизма $(\mathfrak{q}, KE/E)$ на поле K равно $(\mathfrak{p}, K/k)^f$, где f — степень поля классов вычетов:*

$$f = [I_E/\mathfrak{q} : I_K/\mathfrak{p}].$$

Доказательство. Пусть $\mathfrak{P}$ лежит над идеалом $\mathfrak{p}$ в кольце I_K, $\mathfrak{Q}$ лежит над $\mathfrak{q}$ в кольце I_{KE}. Тогда для любого



элемента $x \in I_{KE}/\mathfrak{Q}$ и автоморфизма $\sigma = (\mathfrak{q}, KE/L)$ имеем $\sigma x = x^{\mathrm{N}\mathfrak{q}}$. Ограничение σ на K, очевидно, принадлежит группе разложения идеала $\mathfrak{P}$ и является f-й степенью автоморфизма $(\mathfrak{p}, K/k)$ в силу определения.

Заметим, что этот результат можно представить в виде $(\mathfrak{p}, K/k)^f = (N_K^E \mathfrak{p}, K/k)$, если по мультипликативности распространить на идеалы определение символа Артина.

§ 4. Лемма Артина

Это лемма о существовании некоторых специальных круговых полей. Нам понадобятся вспомогательные результаты, относящиеся к элементарной теории чисел; нижеследующие леммы 1 — 3 принадлежат Ван дер Вардену.

Лемма 1. *Пусть a, r — целые числа, $a > 1$, $r > 0$; q — простое число,*

$$T = \frac{a^{q^r} - 1}{a^{q^{r-1}} - 1}.$$

Если простое число p делит одновременно T и число $a^{q^{r-1}} - 1$, то $p = q$. Если q делит T, то q делит $a^{q^{r-1}} - 1$. Наконец, если $q > 2$ или $r > 1$, то $T \not\equiv 0 \pmod{q^2}$.

Доказательство. Имеем

$$T=(a^{q^{r-1}}-1)^{q-1}+q(a^{q^{r-1}}-1)^{q-2}+\ldots+q.$$

Из этого тождества следуют все наши утверждения при $q>2$; если $q=2$, то

$$T=(a^{2^{r-1}}-1)+2,$$

что также дает требуемое.

Лемма 2. *Пусть a, r, q имеют те же значения, что в лемме* 1. *Существует простое число p, такое, что порядок $a \pmod p$ равен q^r.*

Доказательство. Действительно, $T>q$ и $q^2 \nmid T$. Поэтому существует простое число $p \neq q$, делящее T, но не делящее $a^{q^{r-1}}-1$. Оно и является искомым.

Лемма 3. *Пусть $n=q_1^{r_1}q_2^{r_2}\ldots q_s^{r_s}$ — положительное целое число, $a>1$ — целое число. Можно найти такое целое число*

$$m=p_1p_1'p_2p_2'\ldots p_sp_s',$$

где $p_1, p_1', \ldots, p_s, p_s'$ — различные простые числа, что порядок $a \pmod m$ делится на n и, кроме того, существует положительное число b, порядок которого $\bmod m$ делится на n, причем a, b независимы в группе вычетов $\bmod m$. Можно найти сколь угодно большие простые числа p_i, p_i', удовлетворяющие этим условиям.

Доказательство. Пусть M — большое целое число. Выберем такое целое число $r_1^*=r_1$, что

$$q_1^{r_1^*}>M.$$

По предыдущей лемме, существует такое простое число p_1, что порядок вычета $a \pmod{p_1}$ равен

$$q_1^{r_1^*}.$$

По той же лемме можно найти такое простое число p_1', что порядок вычета $a \pmod{p_1'}$ равен

$$q_1^{r_1^*+1}.$$

Заменим число M числом $p_1 p_1' M$ и продолжим эту процедуру, применяя ее к $r_2, \ldots$.

Мультипликативная группа классов вычетов $\bmod m$, взаимно простых с m, является прямым произведением групп классов вычетов $\bmod p_1$, $\bmod p_1'$, $\bmod p_2$, $\ldots$. Пусть α_i — образующая группы классов вычетов $\bmod p_i$, α_i' — то же для p_i'. Не теряя общности, можно считать, что число a равно

$$\alpha_1^{(p_1-1)/q_1^{r_1^*}} \alpha_1'^{(p_1'-1)/q_1^{r_1^*}+1} \ldots \alpha_s^{(p_s-1)/q_s^{r_s^*}} \alpha_s'^{(p_s'-1)/q_s^{r_s^*}+1}.$$

Положим тогда

$$b = \alpha_1^{(p_1-1)/q_1^{r_1^*}} \ldots \alpha_s^{(p_s-1)/q_s^{r_s^*}}.$$

Без труда проверяется, что b удовлетворяет требуемым условиям.

Лемма 4. *Пусть K — абелево расширение числового поля k, S — конечное множество простых чисел. Пусть $n = [K : k]$, $\mathfrak{p}$ — простой идеал кольца I_k, неразветвленный в поле K. Существует целое число m, взаимно простое с $\mathfrak{p}$ и с числами из множества S, которое удовлетворяет следующим условиям.*

(1) *Порядок символа Артина $(\mathfrak{p}, k(\zeta_m)/k)$ делится на n.*

(2) $K \cap k(\zeta_m) = k$.

(3) *Существует автоморфизм τ поля $k(\zeta_m)$ над k, не зависящий от $(\mathfrak{p}, k(\zeta_m)/k)$, порядок которого делится на n.*

Доказательство. Воспользуемся леммой 3 при $a = \mathbf{N}\mathfrak{p}$. Можно взять m, которое делится лишь на достаточно большие простые числа; тогда $K \cap \mathbf{Q}(\xi_m) = \mathbf{Q}$, и условие (2) будет выполнено. Положим $\sigma = (\mathfrak{p}, k(\zeta_m)/k)$. Тогда

$$\sigma\zeta_m = \zeta_m^a,$$

и условие (1) тоже выполнено. Наконец, выберем b, как в лемме 3, и определим τ формулой

$$\tau\zeta_m = \zeta_m^b.$$

Это дает условие (3).

Лемма Артина. *Пусть k — числовое поле, K — его конечное циклическое расширение, S — конечное множество*

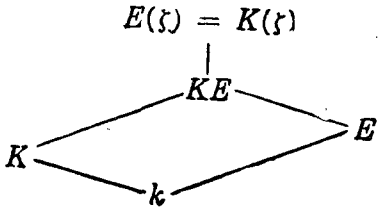
простых чисел. Пусть $\mathfrak{p}$ *— простой идеал кольца* I_k. *Тогда существует целое число* m, *взаимно простое со всеми числами множества* S, *и такое конечное расширение* E *поля* k, *что*

(1) $K \cap E = k$;

(2) $K(\zeta_m) = E(\zeta_m)$ *и* $K \cap k(\zeta_m) = k$;

(3) $\mathfrak{p}$ *вполне распадается в* E.

Доказательство. Схема включений интересующих нас полей:



Выберем m, как в предыдущей лемме, и положим $\zeta = \zeta_m$. Группа Галуа поля $K(\zeta)$ над k является прямым произведением группы G поля K над k и группы поля $k(\zeta)$ над k. Пусть σ — образующая группы G, τ — элемент, существование которого утверждается в предыдущей лемме, H — подгруппа группы Галуа поля $K(\zeta)$ над k, порожденная элементами $\sigma \times \tau$ и $(\mathfrak{p}, K/k) \times (\mathfrak{p}, k(\zeta)/k)$.

Группа H содержит элемент $(\mathfrak{p}, K(\zeta)/k)$ и, значит, по определению, содержит группу разложения идеала $\mathfrak{p}$ в поле $K(\zeta)$. Если E совпадает с полем H-инвариантных элементов, то идеал $\mathfrak{p}$ вполне распадается в поле E.

С другой стороны, очевидно, $H \cap G \times 1$ состоит из единичного элемента. Но $G \times 1$ — подгруппа автоморфизмов поля $K(\zeta)$, оставляющая инвариантной в точности поле $k(\zeta)$. Поэтому поле $k(\zeta)\,E = E(\zeta)$ должно совпадать с $K(\zeta)$. Это доказывает лемму Артина.

Она используется следующим образом. Пусть мы умеем описывать символ Артина в круговых полях. Тогда лемма дает средство сводить изучение символа Артина в циклических расширениях к его изучению в круговых полях. Действительно, с помощью предложения 1 предыдущего параграфа мы можем спуститься от расширения KE/E к расширению K/k.

Глава V

ПАРАЛЛЕЛОТОПЫ

Эта глава содержит количественные результаты о распределении элементов числового поля в параллелотопах.

Речь идет о подсчете количества элементов α в числовом поле k, удовлетворяющих набору неравенств, по одному для каждого нормирования. Оказывается, что это количество асимптотически равно объему области (в подходящем пространстве), определенной этими неравенствами.

Затем мы воспроизведем принадлежащую Минковскому классическую теорию единиц и дискриминанта числового поля и вычислим константу Минковского.

§ 1. Формула произведения

Пусть $M_{\mathbf{Q}}$ — каноническая система нормирований поля рациональных чисел $\mathbf{Q}$. Для любого элемента $\alpha \in \mathbf{Q}$, $\alpha \neq 0$, имеем

$$\prod_{v \in M_{\mathbf{Q}}} |\alpha|_v = 1.$$

Действительно, пусть сначала $\alpha = l$ — простое число, тогда

$$|l|_p = \begin{cases} 1, & \text{если } p \neq l, \ p \text{ — простое число,} \\ 1/p, & \text{если } p = l. \end{cases}$$

Единственное архимедово нормирование для краткости будет называться *бесконечным*: формула произведения верна для l, потому что $|l|_\infty = l$. Отсюда следует по мультипликативности справедливость этой формулы для любого элемента группы $\mathbf{Q}^*$.

Пусть k — конечное расширение поля $\mathbf{Q}$, M_k — система нормирований поля k, продолжающих нормирования системы $M_{\mathbf{Q}}$. Из следствия предложения 0 гл. II, § 1,

получаем для любого элемента $\alpha \in k^*$

$$1 = \prod_{v_0 \in M_{\mathbf{Q}}} |N_{\mathbf{Q}}^k(\alpha)|_{v_0} = \prod_{v_0 \in M_{\mathbf{Q}}} \prod_{v \mid v_0} |\alpha|_v^{N_v} =$$
$$= \prod_{v \in M_k} |\alpha|_v^{N_v} = \prod_{v \in M_k} \|\alpha\|_v.$$

Тем самым здесь также имеет место формула произведения с кратностями

$$N_v = [k_v : \mathbf{Q}_{v_0}].$$

Для всякого числового поля k символом S_∞ обозначим подмножество архимедовых нормирований системы M_k. Обозначим через r_1, r_2 число вещественных и комплексных нормирований соответственно. Тогда

$$r_1 + 2r_2 = [k : \mathbf{Q}];$$

эту степень обозначим буквой N. Положим, кроме того, $r = r_1 + r_2 - 1$. Локальная степень N_v равна 1, если v — вещественное нормирование, 2 — если комплексное.

Теперь мы докажем классические утверждения о конечности числа классов и числа образующих групп единиц.

Начнем с числа классов. Покажем, что *существует константа C, зависящая только от поля k и такая, что для всякого ненулевого идеала $\mathfrak{a}$ в его классе линейной эквивалентности существует идеал $\mathfrak{b}$ с условием $\mathbf{N}\mathfrak{b} \leqslant C$.*

Отсюда следует, что число классов идеалов конечно, потому что существует только конечное число идеалов с ограниченными нормами (в самом деле, существует только конечное число простых чисел, ограниченных данной константой, а для каждого простого числа p в кольце I_k есть только конечное число простых идеалов, лежащих над p).

Пусть $\omega_1, \ldots \omega_N$ — базис кольца I_k над $\mathbf{Z}$, S — множество элементов этого кольца, имеющих вид

$$a_1\omega_1 + \ldots + a_N\omega_N,$$

где a_i — целые числа с условием

$$0 \leqslant a_i \leqslant (\mathbf{N}\mathfrak{a})^{1/N} + 1.$$

Множество S содержит более чем $\mathbf{N}\mathfrak{a}$ элементов. Поэтому существуют такие различные элементы $\alpha, \beta \in S$, разность которых $\alpha - \beta = \xi$ отображается в нуль при гомоморфизме

$$I_k \to \prod I_k/\mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}\mathfrak{a}}$$

(ср. предложение 24 гл. I, § 7). Отсюда вытекает существование идеала $\mathfrak{b}$ со свойством $(\xi) = \mathfrak{a}\mathfrak{b}$. С другой стороны, оценим норму

$$N_{\mathbf{Q}}^{k}(\xi) = \prod_{\sigma} |c_1\omega_1^{\sigma} + \ldots + c_N\omega_N^{\sigma}|,$$

где $0 \leqslant c_i \leqslant (\mathbf{N}\mathfrak{a})^{1/N} + 1$. Очевидно, существует такая константа C (зависящая от максимума архимедовых нормирований элементов ω_i и от степени N), что

$$|N_{\mathbf{Q}}^{k}(\xi)| \leqslant C \cdot \mathbf{N}\mathfrak{a}.$$

Пользуясь предложением 22 гл. I, § 7, получаем, что $\mathbf{N}\mathfrak{b} \leqslant C$ и $\mathfrak{b} \sim \mathfrak{a}^{-1}$, по определению. Это доказывает наш результат.

Теперь докажем теорему о единицах, следуя статье Артина—Уэйплса. Начнем с некоторых общих понятий.

Назовем *M_k-дивизором* $\mathfrak{c}$ вещественнозначную функцию, определенную на множестве нормирований $v \in M_k$ и удовлетворяющую следующим условиям:

(1) $\mathfrak{c}(v) > 0$ для всех $v \in M_k$;

(2) $\mathfrak{c}(v) = 1$ для всех, кроме конечного числа $v \in M_k$;

(3) если v — дискретное нормирование, то в поле k существует такой элемент α, что $\mathfrak{c}(v) = |\alpha|_v$.

Иногда вместо $\mathfrak{c}(v)$ мы будем писать $|\mathfrak{c}|_v$ или $\mathfrak{c}_v$; кроме того, при существовании формулы произведения с кратностями N_v положим

$$\|\mathfrak{c}\|_v = \mathfrak{c}(v)^{N_v}.$$

Назовем *k-величиной* или просто величиной M_k-дивизора $\mathfrak{c}$ число

$$\|\mathfrak{c}\|_k = \prod_v \mathfrak{c}(v)^{N_v}.$$

Символом $L(\mathfrak{c})$ обозначим множество таких элементов $x \in k$, что для всех $v \in M_k$ имеет место неравенство

$$|x|_v \leqslant \mathfrak{c}(v).$$

Каждый элемент $\alpha \in k^*$ определяет некоторый M_k-дивизор, значение которого на нормировании v равно $|\alpha|_v$. Произведение двух M_k-дивизоров является M_k-дивизором, и для любого M_k-дивизора $\mathfrak{c}$ дивизор $\alpha\mathfrak{c}$ определяется равенством

$$(\alpha\mathfrak{c})(v) = |\alpha|_v \mathfrak{c}(v).$$

Ввиду формулы произведения имеем

$$\|\alpha\mathfrak{c}\|_k = \|\mathfrak{c}\|_k.$$

Иначе говоря, величины дивизоров $\mathfrak{c}$ и $\alpha\mathfrak{c}$ совпадают.

При любом $\alpha \in k^*$ множества $L(\alpha\mathfrak{c})$ и $L(\mathfrak{c})$ находятся в каноническом взаимно однозначном соответствии, которое задается отображением

$$x \rightsquigarrow \alpha x, \quad x \in L(\mathfrak{c}).$$

Число элементов множества $L(\mathfrak{c})$ обозначим символом $\lambda(\mathfrak{c})$. Тогда

$$\lambda(\alpha\mathfrak{c}) = \lambda(\mathfrak{c}).$$

Если представить себе, что неравенства, описывающие $\mathfrak{c}$, определяют ящик, все ребра которого, кроме конечного числа их, имеют длину 1, число $\lambda(\mathfrak{c})$ будет количеством элементов поля, попадающих в этот ящик. Величину дивизора $\mathfrak{c}$ можно интерпретировать как объем ящика. Мы докажем сейчас, что количество элементов в ящике приближенно равно его объему. В следующем параграфе мы получим другим методом более сильный асимптотический результат.

Теорема 0. *Пусть k — числовое поле. Существуют такие два числа c_1, $c_2 > 0$, зависящие только от поля k, что для любого M_k-дивизора $\mathfrak{c}$ имеем*

$$c_1 \|\mathfrak{c}\|_k < \lambda(\mathfrak{c}) \leqslant \sup[1, c_2 \|\mathfrak{c}\|_k].$$

Доказательство. Предположим, что во множестве M_k существует хотя бы одно комплексное нормиро-

вание v_0. Отождествим k_{v_0} с комплексной плоскостью и рассмотрим квадрат с центром в начале и сторонами длины $2c(v_0)$. Пусть m — такое целое число, что

$$m < \lambda(c)^{1/2} \leqslant m+1.$$

Не ограничивая общности, мы можем считать, что $m \neq 0$, так что $m \geqslant 1$. Разобьем каждую сторону квадрата на m равных частей, построив, таким образом, m^2 маленьких квадратов внутри большого.

Проекция множества $L(c)$ на k_{v_0} содержится в большом квадрате; так как она состоит более чем из m^2 элементов, то существуют различные элементы x, $y \in L(c)$, попадающие в один и тот же маленький квадрат. Поэтому

$$|x-y|_{v_0} \leqslant \frac{2\sqrt{2}\,c(v_0)}{m}.$$

Для любого другого архимедова нормирования из системы M_k имеем

$$|x-y|_v \leqslant 2c(v),$$

а для любого неархимедова v —

$$|x-y|_v \leqslant c(v).$$

Беря произведение по всем v, получаем

$$1 = \prod_{v \in M_k} |x-y|_v^{N_v} \leqslant \frac{c_3 \| c \|_k}{m^2},$$

где c_3 — некоторая константа. Так как $(m+1)^2 \leqslant 4m^2$, верхняя оценка получается немедленно.

Если в системе M_k нет ни одного комплексного нормирования, действуем аналогично, пользуясь вещественным нормированием v_0 и разбивая интервал с серединой в начале координат и длины $2c(v_0)$ на m равных частей, где

$$m < \lambda(c) \leqslant m+1.$$

После этого применяем прежнее рассуждение.

Докажем теперь нижнюю оценку. Пусть $\omega_1, \ldots, \omega_N$ — базис кольца I_k над $\mathbf{Z}$. Положим

$$c_0 = N \sup_{v,\,i} |\omega_i|_v,$$

где верхняя грань берется по всем архимедовым нормированиям v в системе M_k и по i. Это — число, зависящее только от k.

Пусть $\mathfrak{c}$ — данный M_k-дивизор. В силу теоремы о приближениях существует такой элемент $\alpha \in k^*$, что

$$c_0 \leqslant |\alpha\mathfrak{c}|_v \leqslant 2c_0$$

для всякого архимедова нормирования v в системе M_k. Выберем такое целое число $a \in \mathbf{Z}$, $a \neq 0$, чтобы относительно всех неархимедовых нормирований $v \in M_k$ дивизор $a\alpha\mathfrak{c}$ был по норме $\leqslant 1$. Для этого нужно, чтобы число a делилось на достаточно много простых чисел в достаточно высоких степенях. Учитывая, что ни $\lambda(\mathfrak{c})$, ни $\|\mathfrak{c}\|_k$ не меняются при умножении $\mathfrak{c}$ на элементы группы k^*, мы можем поэтому, не ограничивая общности, считать, что наш M_k-дивизор удовлетворяет неравенствам

$$c_0 |a|_v \leqslant |\mathfrak{c}|_v \leqslant 2c_0 |a|_v,$$

где $a \in \mathbf{Z}$ — некоторое положительное целое число.

Нам следует выяснить, какие элементы попадают в множество $L(\mathfrak{c})$. С этой целью рассмотрим сначала множество L элементов кольца I_k, имеющих вид

$$a_1\omega_1 + \ldots + a_N\omega_N,$$

где $a_i \in \mathbf{Z}$, $0 \leqslant a_i \leqslant a$. Множество L содержит более чем a^N элементов.

Каждое неархимедово нормирование в системе M_k соответствует некоторому простому идеалу $\mathfrak{p}$ кольца I_k. Используя третье условие в определении M_k-дивизора, мы можем очевидным образом ввести понятие порядка $\mathrm{ord}_{\mathfrak{p}}\mathfrak{c}$. Положим $n_{\mathfrak{p}} = \mathrm{ord}_{\mathfrak{p}}\mathfrak{c}$. Аддитивная группа

$$I_k / \prod \mathfrak{p}^{n_{\mathfrak{p}}}$$

состоит из $\prod (\mathbf{N}\mathfrak{p})^{n_{\mathfrak{p}}}$ элементов. Рассмотрим образ множества L относительно канонического гомоморфизма кольца I_k в эту аддитивную группу. Существует подмножество L' множества L, содержащее по крайней мере

$$\frac{a^N}{\prod (\mathbf{N}\mathfrak{p})^{n_{\mathfrak{p}}}}$$

элементов, имеющих один и тот же образ. Фиксируем один элемент $x \in L'$, и пусть y пробегает все остальные элементы. Тогда для любого неархимедова нормирования v в системе M_k получаем

$$|x-y|_v \leqslant \mathfrak{c}(v),$$

потому что $\mathrm{ord}_{\mathfrak{p}}(x-y) \geqslant \mathrm{ord}_{\mathfrak{p}}\mathfrak{c}$. Если же v архимедово, имеет место очевидная оценка

$$|x-y|_v \leqslant c_0 |a|_v \leqslant \mathfrak{c}(v).$$

Поэтому элементы $x-y$ принадлежат множеству $L(\mathfrak{c})$. Следовательно,

$$\lambda(\mathfrak{c}) \geqslant a^N \prod \frac{1}{\mathbf{N}\mathfrak{p}^{n_{\mathfrak{p}}}}.$$

Наконец, заметим, что

$$a^N = \prod_{v \mid v_\infty} |a|_v^{N_v} > c_1 \prod_{v \mid v_\infty} |\mathfrak{c}|_v^{N_v},$$

где произведение берется по архимедовым нормированиям, а c_1 — легко вычисляемая константа, и что

$$\frac{1}{\mathbf{N}\mathfrak{p}^{n_{\mathfrak{p}}}} = \|\mathfrak{c}\|_v,$$

где v — неархимедово нормирование, соответствующее $\mathfrak{p}$. Рассматривая полное произведение по всем нормированиям, получаем требуемую оценку снизу.

Пусть k — числовое поле, S — конечное подмножество системы M_k, содержащее все архимедовы нормирования. Пусть s — количество элементов множества S. Определим множество *S-единиц* k_S как группу тех элементов из k^*, для которых при всех $v \notin S$

$$|\alpha|_v = 1.$$

S_∞-единицы называются также просто единицами поля k. Строго говоря, это единицы (обратимые элементы) кольца алгебраических целых чисел I_k.

Рассмотрим следующее отображение группы k_S в s-мерное евклидово пространство:

$$x \rightsquigarrow (\log \|x\|_1, \ldots, \log \|x\|_s)$$

и обозначим его символом

$$\log : k_s \longrightarrow \mathbf{R}^s.$$

В силу формулы произведения образ группы k_s содержится в гиперплоскости, определяемой уравнением

$$\xi_1 + \ldots + \xi_s = 0.$$

Следовательно, размерность этого образа не превосходит $s-1$.

Теорема о единицах утверждает, что *образ* $\log(k_S)$ *является* $(s-1)$*-мерной решеткой в пространстве* $\mathbf{R}^s$.

Решетка — это дискретная подгруппа пространства $\mathbf{R}^s$; утверждение о размерности означает, что натянутое на эту решетку линейное пространство совпадает с описанной выше гиперплоскостью. Отсюда, в частности, следует, что $\log(k_S)$ — свободная абелева группа с $s-1$ образующей. Ядро отображения log, очевидно, состоит из корней из единицы поля k, потому что оно является группой, элементы которой ограничены по абсолютной величине, так что эта группа конечна.

В качестве следствия из теоремы о единицах получаем.

Пусть k *— числовое поле,* S *— конечное множество нормирований системы* M_k, *содержащее все архимедовы нормирования. Тогда факторгруппа* k_S *по модулю подгруппы корней из единицы поля* k *является свободной абелевой группой с* s *образующими, где* s *— число элементов множества* S.

Заметим, однако, что теорема о единицах дает больше, чем это следствие. В действительности она равносильна некоторому утверждению о компактности, которое мы приведем в гл. VI, § 3.

Докажем теперь теорему о единицах.

Отметим прежде всего, что в любой ограниченной области пространства $\mathbf{R}^s$ может находиться только конечное число элементов группы $\log(k_S)$. В самом деле, если $\log(x)$ принадлежит такой области, то нормы x и всех его сопряженных ограничены, а тогда x может быть корнем одного из конечного числа уравнений степени $\leqslant [k : \mathbf{Q}]$ над полем $\mathbf{Q}$, потому что коэффициентами каждого такого

уравнения являются элементарные симметрические функции от x и всех его сопряженных. По хорошо известному свойству евклидова пространства, доказательство которого мы напомним в конце, отсюда следует, что $\log(k_S)$ является дискретной конечно порожденной подгруппой пространства $\mathbf{R}^s$. Мы должны доказать, что ее размерность равна $s-1$.

С этой целью покажем сначала, что для любого данного индекса i в группе $\log(k_S)$ существует такой вектор $(\xi_1, \ldots, \xi_s)$, что $\xi_i > 0$, а $\xi_j < 0$ при $j \neq i$. После этого мы установим, что $s-1$ векторов такого типа линейно независимы над $\mathbf{R}$.

Нам понадобится следующая

Лемма. *Для любого нормирования $v_0 \in M_k$ можно найти такое число $c(v_0) > 0$, что для всякого M_k-дивизора $\mathfrak{c}$ существует элемент $\beta \in k^*$ с условием*

$$1 \leqslant \| \beta \mathfrak{c} \|_v \leqslant c(v_0)$$

для всех $v \neq v_0$, $v \in M_k$.

Доказательство. Пусть c_1 — константа из теоремы 0. Положим $c_0 = 1$, если v_0 — архимедово нормирование, и $c_0 = \mathbf{N}\mathfrak{p}_0$, если v_0 соответствует простому идеалу $\mathfrak{p}_0$. Пусть $\mathfrak{c}'$ является M_k-дивизором, отличающимся от $\mathfrak{c}$ только в v_0 и таким, что

$$\frac{1}{c_1} \leqslant \| \mathfrak{c}' \|_k \leqslant \frac{c_0}{c_1}.$$

Такой дивизор можно выбрать, потому что если v_0 архимедово, то v_0-компоненту дивизора можно менять как угодно, а если неархимедово, то группа значений состоит из степеней $\mathbf{N}\mathfrak{p}_0$, что в силу выбора c_0 также позволяет добиться требуемого. Положим $c(v_0) = c_0/c_1$.

В силу теоремы 0 $\lambda(\mathfrak{c}') > 1$, так что существует элемент $\alpha \neq 0$, $\alpha \in L(\mathfrak{c}')$. Иначе говоря,

$$\| \alpha \|_v \leqslant \| \mathfrak{c}' \|_v$$

для всех $v \in M_k$. Положим $\beta = 1/\alpha$. Тогда выполняется левое неравенство леммы. Далее,

$$\| \beta \mathfrak{c}' \|_v = \frac{\| \beta \mathfrak{c}' \|_k}{\prod\limits_{w \neq v} \| \beta \mathfrak{c}' \|_w} \leqslant \| \beta \mathfrak{c}' \|_k = \| \mathfrak{c}' \|_k$$

для всех $v \in M_k$. Произведение взято по всем $w \in M_k$, $w \neq v$. Так как $\mathfrak{c}'$ отличается от $\mathfrak{c}$ только в v_0, мы доказали и правое неравенство.

Вернемся к доказательству теоремы. Если $v \notin S$, то группа значений v — бесконечная циклическая, порожденная числом $\mathbf{N}\mathfrak{p}$, и существует только конечное число простых идеалов $\mathfrak{p}$ с условием

$$\mathbf{N}\mathfrak{p} \leqslant c(v_0).$$

Следовательно, существует такая конечная система нормирований $S' \supset S$, что при $v \notin S'$ имеем

$$1 = \| \beta \mathfrak{c} \|_v = \| \beta \|_v,$$

где β выбран, как в лемме. Далее, величины

$$\| \beta \mathfrak{c} \|_v = \| \beta \|_v, \quad v \in S' - S,$$

могут принимать только конечное множество значений. Пусть $\beta_1, \ldots, \beta_r$ — все эти значения. Для любого дивизора $\mathfrak{c}$ и любого элемента β, удовлетворяющего лемме, имеем

$$\| \beta \|_v = \| \beta_j \|_v$$

для некоторого j при всех $v \in S' - S$. Отсюда вытекает, что $\beta = \beta_j u$, $u \in k_S$. Подставляя это в неравенство леммы, находим

$$\| u \mathfrak{c} \|_v \leqslant \frac{c(v_0)}{\| \beta_j \|_v}$$

при всех $v \neq v_0$, $v \in M_k$. Так как элементы $\beta_1, \ldots, \beta_r$ фиксированы, изменим $\mathfrak{c}$ так, чтобы $\mathfrak{c}(v) = 1$ при $v \notin S$, $\mathfrak{c}(v)$ очень велико при всех $v \in S$. Тогда норма $\| u \|_v$ очень мала при всех $v \in S$, $v \neq v_0$. В силу формулы произведения норма $\| u \|_{v_0}$ должна быть велика. Это доказывает наше первое утверждение.

Итак, мы нашли такие элементы $x_1, \ldots, x_{s-1} \in k_S$, что матрица знаков векторов

$$\log x_1 = (\xi_{11}, \ldots, \xi_{1s})$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$\log x_{s-1} = (\xi_{s-1,1}, \ldots, \xi_{s-1,s})$$

имеет вид

$$\begin{bmatrix} + & - & - & \dots & - & - \\ - & + & - & \dots & - & - \\ - & - & + & \dots & - & - \\ \dots & \dots & \dots & \dots & \dots & \dots \\ - & - & - & & + & - \end{bmatrix}.$$

Пусть $Y_1, \dots, Y_s$ — столбцы матрицы, составленной из координат. Покажем, что первые $s-1$ из них линейно независимы над $\mathbf{R}$. Предположим, что имеет место соотношение

$$a_1 Y_1 + \dots + a_{s-1} Y_{s-1} = 0,$$

в котором не все коэффициенты нулевые. Можно считать, что $a_1 > 0$ и $a_1 \geqslant a_j$ при всех j. Рассматривая соответствующую линейную комбинацию элементов первой строки, получаем

$$\begin{aligned} 0 = a_1\xi_{11} + a_2\xi_{12} + \dots + a_{s-1}\xi_{1,\,s-1} \geqslant \\ \geqslant a_1\xi_{11} + a_1\xi_{12} + \dots + a_1\xi_{1,\,s-1} = \\ = a_1(\xi_{11} + \xi_{12} + \dots + \xi_{1,\,s-1}), \end{aligned}$$

потому что $\xi_{1j} < 0$ при $j = 2, \dots, s-1$. Но по формуле произведения

$$\xi_{11} + \xi_{12} + \dots + \xi_{1,\,s-1} > 0.$$

Мы пришли к противоречию.

Для удобства читателя воспроизведем доказательство того, что дискретная подгруппа евклидова пространства является свободной абелевой группой. Проведем индукцию по размерности подгруппы, т. е. по максимальному числу ее элементов, линейно независимых над $\mathbf{R}$.

Пусть Γ — такая подгруппа, $\xi_1, \dots, \xi_m$ — максимальная система независимых векторов в ней. Пусть Γ_0 — подгруппа группы Γ, содержащаяся в подпространстве, натянутом на $\xi_1, \dots, \xi_{m-1}$. По индуктивному предположению, можно считать, что любой элемент группы Γ_0 является целочисленной линейной комбинацией векторов $\xi_1, \dots, \xi_{m-1}$.

Рассмотрим подмножество T всех векторов $\xi \in \Gamma$ вида

$$\xi = a_1\xi_1 + \dots + a_m\xi_m,$$

где a_i — вещественные коэффициенты, удовлетворяющие неравенствам

$$0 \leqslant a_i < 1, \quad i = 1, \ldots, m-1,$$
$$0 \leqslant a_m \leqslant 1.$$

Это множество ограничено. Пусть ξ'_m — вектор из этого множества с наименьшим ненулевым последним коэффициентом

$$\xi'_m = b_1\xi_1 + \ldots + b_m\xi_m.$$

Начав с любого вектора ξ группы Γ, мы можем подобрать целые коэффициенты $c_1, \ldots, c_m$ таким образом, чтобы вектор

$$\xi' = \xi - c_m\xi'_m - c_1\xi_1 - \ldots - c_{m-1}\xi_{m-1}$$

лежал в T, а коэффициент при ξ_m был $< b_m$ и $\geqslant 0$. Тогда этот коэффициент должен быть нулевым, а элемент ξ' принадлежит подгруппе Γ_0. Это доказывает наш результат.

§ 2. Точки решетки в параллелотопах

В этом параграфе мы докажем следующее уточнение теоремы 0.

Теорема 1. *Пусть k — числовое поле, $[k; \mathbf{Q}] = N$. Положим*

$$B_k = \frac{2^{r_1}(2\pi)^{r_2}}{|D_k|^{1/2}}.$$

Тогда для любого M_k-дивизора $\mathfrak{c}$ количество $\lambda(\mathfrak{c})$ элементов в области $L(\mathfrak{c})$ допускает оценку

$$\lambda(\mathfrak{c}) = B_k \| \mathfrak{c} \|_k + O(\| \mathfrak{c} \|_k^{1-1/N}), \qquad \| \mathfrak{c} \|_k \to \infty.$$

Иначе говоря, существуют такие константы $b_1, b_2 > 0$, зависящие только от k, что при $\| \mathfrak{c} \|_k > b_2$ имеем

$$|\lambda(\mathfrak{c}) - B_k \| \mathfrak{c} \|_k| \leqslant b_1(\| \mathfrak{c} \|_k^{1-1/N}).$$

Доказательство. Начнем с некоторых замечаний о M_k-дивизорах. Для всякого M_k-дивизора $\mathfrak{c}$ существует такой дробный идеал $\mathfrak{a}$ кольца I_k, что $\alpha \in \mathfrak{a}$ в том

и только том случае, когда

$$|\alpha|_{\mathfrak{p}} \leqslant \mathfrak{c}(v_{\mathfrak{p}})$$

для всех простых идеалов $\mathfrak{p} \subset I_k$. Это немедленно вытекает из определений. Таким образом, множество $L(\mathfrak{c})$ состоит из тех элементов идеала $\mathfrak{a}$, которые удовлетворяют некоторым неравенствам относительно архимедовых нормирований. Мы будем говорить, что идеал $\mathfrak{a}$ *связан* с дивизором $\mathfrak{c}$.

Для всякого элемента $\beta \in k^*$ имеем $\lambda(\beta\mathfrak{c}) = \lambda(\mathfrak{c})$. Следовательно, при вычислении $\lambda(\mathfrak{c})$ дивизор $\mathfrak{c}$ можно умножить на любой элемент группы k^*.

Мы уже знаем, что группа классов идеалов кольца I_k конечна. Пусть $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ — идеалы, представляющие элементы этой группы. Умножая $\mathfrak{c}$ на подходящий элемент из k^*, мы можем считать, что дробный идеал $\mathfrak{a}$, связанный с $\mathfrak{c}$, равен одному из идеалов $\mathfrak{a}_i$.

Пусть $\mathfrak{c}$ — некоторый M_k-дивизор, $\mathfrak{a}$ — связанный с ним дробный идеал. Тогда

$$\|\mathfrak{c}\|_k = \frac{1}{\mathbf{N}\mathfrak{a}} \prod_{v \in S_\infty} \mathfrak{c}_v^{N_v},$$

где мы пишем $\mathfrak{c}_v$ вместо $\mathfrak{c}(v)$ для упрощения обозначений.

Лемма 1. *Пусть связанный с $\mathfrak{c}$ дробный идеал $\mathfrak{a}$ равен одному из элементов фиксированной системы представителей $\mathfrak{a}_i$. Тогда существует такая единица u кольца I_k, что для всех $v \in S_\infty$ имеем*

$$c_1(k)\,\|\mathfrak{c}\|_k^{1/N} \leqslant |u\mathfrak{c}|_v \leqslant c_2(k)\,\|\mathfrak{c}\|_k^{1/N},$$

где $c_1(k)$, $c_2(k)$ — две положительные константы, зависящие только от k.

Доказательство. Пусть $V = \|\mathfrak{c}\|_k$, $\mathfrak{c}'_v = \mathfrak{c}_v\,(V\mathbf{N}\mathfrak{a})^{-1/N}$ для всех $v \in S_\infty$. Тогда

$$\prod_{v \in S_\infty} \mathfrak{c}_v'^{N_v} = 1.$$

Рассмотрим вектор

$$\log(\mathfrak{c}') = (\ldots, \log\|\mathfrak{c}'_v\|_v, \ldots)_{v \in S_\infty}.$$

Так как векторы, соответствующие единицам, образуют решетку максимальной размерности в гиперплоскости, состоящей из векторов с нулевой суммой координат, то существует такая единица u, что

$$|\log(c') - \log(u^{-1})| < c_3(k),$$

где $c_3(k)$ — некоторая константа, а абсолютное значение вектора — его евклидова длина. Отсюда следует, что $\log(uc)$ — вектор ограниченной длины. Иначе говоря, существуют такие константы c_4, $c_5 > 0$, что

$$c_4 \leqslant |uc'_v|_v \leqslant c_5$$

для всех $v \in S_\infty$. Мы получаем утверждение леммы, подставляя сюда значение c'_v.

Рассмотрим евклидово пространство $\mathbf{R}^N$, которое мы отождествим с

$$\prod_{v \in S_\infty} k_v,$$

потому что это — произведение r_1 вещественных прямых и r_2 комплексных плоскостей и $r_1 + 2r_2 = N$. Каждый идеал кольца I_k представлен решеткой ранга N в этом пространстве, если вложить в него кольцо I_k диагонально. Неравенства, наложенные M_k-дивизором в нормированиях $v \in S_\infty$, определяют некоторую область в этом евклидовом пространстве. Наша задача тем самым сводится к следующей.

Дана решетка L ранга N в N-мерном евклидовом пространстве. Доказать, что при некоторых условиях число точек такой решетки в параллелотопе приближенно равно объему параллелотопа. Этим мы и займемся.

Пусть $\xi_1, \ldots, \xi_N$ — линейно независимые векторы пространства $\mathbf{R}^N$. Порожденная ими абелева группа является решеткой. По определению, *фундаментальной областью* решетки называется любое (измеримое) множество, обладающее тем свойством, что всякий вектор пространства $\mathbf{R}^N$ сравним ровно с одним вектором этого множества по модулю решетки. Мы в качестве фундаментальной области всегда будем выбирать множество F точек вида

$$t_1\xi_1 + \ldots + t_N\xi_N$$

с $0 \leqslant t_i < 1$.

Пусть $\mathfrak{c}$ есть M_k-дивизор. Символом $P_{\mathfrak{c}}$ обозначим множество векторов пространства

$$\prod_{v\in S_\infty} k_v = \mathbf{R}^N,$$

удовлетворяющих неравенствам

$$|x|_v \leqslant \mathfrak{c}_v \quad \text{для всех } v\in S_\infty.$$

Это множество называется *параллелотопом*, соответствующим дивизору $\mathfrak{c}$ (на бесконечности).

Обозначим символом $n(\mathfrak{c})$ количество таких элементов x решетки L, что $F_x \subset P_{\mathfrak{c}}$, где F_x — сдвиг области F на x. Символом $m(\mathfrak{c})$ обозначим число тех точек решетки L, для которых пересечение $F_x \cap P_{\mathfrak{c}}$ непусто.

Пусть $l(\mathfrak{c})$ — число точек решетки в параллелотопе $P_{\mathfrak{c}}$. Очевидно, что

$$n(\mathfrak{c})\,\mathrm{Vol}\,(F) \leqslant \mathrm{Vol}\,(P_{\mathfrak{c}}) \leqslant m(\mathfrak{c})\,\mathrm{Vol}\,(F),$$

где Vol означает объем в евклидовом пространстве.

Единственной точкой решетки, попадающей в F_x, является x. Поэтому

$$n(\mathfrak{c}) \leqslant l(\mathfrak{c}) \leqslant m(\mathfrak{c}).$$

Докажем теперь одну теорему о решетках в пространстве $\mathbf{R}^N$.

Теорема 2. *Пусть* $\mathfrak{c}$ *пробегает множество таких* M_k*-дивизоров, что для всех* $v\in S_\infty$ *имеют место неравенства*

$$c_6\,\mathrm{Vol}\,(P_{\mathfrak{c}})^{1/N} \leqslant \mathfrak{c}_v \leqslant c_7\,\mathrm{Vol}\,(P_{\mathfrak{c}})^{1/N}$$

с некоторыми фиксированными положительными константами c_6, c_7. *Пусть* L *— фиксированная решетка пространства* $\mathbf{R}^N$. *Тогда для всех* $\mathfrak{c}$ *с условием* $\mathrm{Vol}\,(P_{\mathfrak{c}}) > c'$ *имеем*

$$l(\mathfrak{c}) = \frac{\mathrm{Vol}\,(P_{\mathfrak{c}})}{\mathrm{Vol}\,(F)} \pm c''\,\mathrm{Vol}\,(P_{\mathfrak{c}})^{1-1/N},$$

где c', c'' *зависят только от* c_6, c_7 *и* L.

Доказательство. Достаточно проверить, что разность $m(c)-n(c)$ ограничена величиной порядка $B^{1-1/N}$, где $B=\mathrm{Vol}(P_c)$.

Если сдвиг F_x фундаментальной области F не содержится в P_c, но пересекается с P_c, то он пересекается с границей области P_c (отрезок прямой между любой точкой в пересечении $F_x \cap P_c$ и любой точкой в F_x, не содержащейся в P_c, содержится в F_x в силу выпуклости F_x и пересекается с границей P_c). Положим

$$P_c = \prod_{v\in S_\infty} D_v,$$

где D_v — замкнутый отрезок или замкнутый круг радиуса c_v в зависимости от того, является v вещественным или комплексным. Соответственно граница области D_v состоит из двух точек или окружности и

$$\partial P_c = U_{v_0\in S_\infty}\left[\partial D_{v_0}\times\prod_{v\neq v_0} D_v\right].$$

Поэтому размерность границы равна $N-1$. Достаточно дать верхнюю оценку нужного нам вида для количества сдвигов F_x, пересекающихся с множеством

$$\partial D_{v_0}\times\prod_{v\neq v_0} D_v,$$

потому что граница состоит самое большее из N кусков такого вида. Мы сделаем это, параметризуя границу с помощью отображения, частные производные которого удовлетворяют подходящим оценкам. Напомним, что для любого дифференцируемого отображения φ с производной φ' и для всяких двух векторов y, z имеет место неравенство

$$|\varphi(y)-\varphi(z)|\leqslant|\varphi'|\cdot|y-z|,$$

где $|\ |$ — евклидова норма векторов, а $|\varphi'|$ — максимум нормы производной от φ на отрезке между y и z (это теорема о среднем).

Определим параметризацию

$$\varphi: I^N \longrightarrow P_c,$$

отображающую N-мерный куб с единичными ребрами на P_c, с помощью следующих формул. Для вещественного v положим

$$t \rightsquigarrow 2c_v\left(t-\frac{1}{2}\right), \quad 0 \leqslant t \leqslant 1.$$

Для комплексного v, пользуясь полярными координатами, положим

$$(u, \theta) \rightsquigarrow (c_v u, 2\pi\theta), \quad \begin{matrix} 0 \leqslant u \leqslant 1, \\ 0 \leqslant \theta \leqslant 1. \end{matrix}$$

Каждая частная производная отображения φ ограничена величиной $2c_v$ или $2\pi c_v$. Поэтому существует такая константа $c_8 = 2\pi N c_7$, что $|\varphi'| \leqslant c_8 B^{1/N}$.

Граница области P_c параметризована $(N-1)$-мерными кубами I^{N-1}. Разбив каждое ребро куба на $[B^{1/N}]$ отрезков одинаковой длины, мы получим разложение куба I^{N-1} на

$$[B^{1/N}]^{N-1}$$

маленьких кубиков диаметра $\leqslant (N-1)^{1/2}/[B^{1/N}]$. Диаметр образа каждого из таких кубиков при отображении φ не превосходит величины

$$\frac{(N-1)^{1/2}}{[B^{1/N}]} c_8 [B^{1/N}] \leqslant c_9.$$

Число сдвигов F_x, $x \in L$, пересекающихся с областью диаметра $\leqslant c_9$, ограничено константой c_{10}, зависящей только от c_9 и от диаметра области F. Поэтому φ-образ любого кубика пересекается с не более чем c_{10} сдвигами области F на точки решетки. Так как всего имеется $[B^{(N-1)/N}]$ кубиков, то образ $\varphi(I^{N-1})$ пересекается с не более чем $c_{10}[B^{(N-1)/N}]$ сдвигами области F. Граница области P_c состоит из не более чем N кусков, каждый из которых параметризуется $(N-1)$-мерным кубом. Отсюда следует наша теорема.

В следующей лемме вычислен объем фундаментальной области идеала $\mathfrak{a}$ кольца I_k, рассматриваемого как

решетка в евклидовом пространстве

$$\mathbf{R}^N = \prod_{v \in S_\infty} k_v.$$

Лемма 2. *Пусть* $\mathfrak{a}$ *— идеал кольца целых чисел поля* k, F *— фундаментальная область для* $\mathfrak{a}$, *рассматриваемого как решетка в* $\mathbf{R}_N$. *Тогда*

$$\mathrm{Vol}\,(F) = 2^{-r_2} |\, D_{k/\mathbf{Q}}\,(\mathfrak{a})\,|^{1/2}.$$

Доказательство. Пусть $\alpha_1, \ldots, \alpha_N$ — это $\mathbf{Z}$-базис идеала $\mathfrak{a}$; $\sigma_1, \ldots, \sigma_{r_1}$ — вещественные вложения поля k; $\tau_1, \ldots, \tau_{r_2}$ и их сопряженные — комплексные вложения. Всякий элемент $\alpha \in k$ отображается на вектор вида

$$(\sigma_1\alpha, \ldots, \sigma_{r_1}\alpha, \tau_1\alpha, \ldots, \tau_{r_2}\alpha).$$

Пусть

$$\tau_j\alpha = x_j + \sqrt{-1}\, y_j,$$

где x_j, y_j — вещественные координаты на комплексной плоскости $\mathbf{C}$. Тем самым

$$\tau_j\alpha_\nu = x_{j\nu} + \sqrt{-1}\, y_{j\nu}, \qquad \nu = 1, \ldots, N.$$

Дискриминант идеала $\mathfrak{a}$ как $\mathbf{Z}$-модуля равен квадрату определителя

$$\begin{vmatrix} \sigma_1\alpha_1 & \ldots & \sigma_1\alpha_N \\ \vdots & & \vdots \\ \vdots & & \vdots \\ x_{11} + iy_{11} & \ldots & x_{1N} + iy_{1N} \\ \vdots & & \vdots \\ \vdots & & \vdots \\ x_{11} - iy_{11} & \ldots & x_{1N} - iy_{1N} \\ \vdots & & \vdots \\ \vdots & & \vdots \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}\vdots\\\vdots\end{matrix}}\right\} r_1 \\ \left.\vphantom{\begin{matrix}\vdots\\\vdots\end{matrix}}\right\} r_2 \\ \left.\vphantom{\begin{matrix}\vdots\\\vdots\end{matrix}}\right\} r_2 \end{matrix}$$

Заменив каждую пару сопряженных строк парой, состоящей из их суммы и разности, находим, что с точностью

до знака этот определитель равен

$$2^{r_2}\begin{vmatrix} \sigma_1\alpha_1 & \dots & \sigma_1\alpha_N \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ x_{11} & \dots & x_{1N} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \\ y_{11} & \dots & y_{1N} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \cdot & & \cdot \end{vmatrix}.$$

В свою очередь последний определитель составлен из координат базиса решетки $\mathfrak{a}$, разложенного по канонической ортонормированной системе образующих пространства $\mathbf{R}^N$. Поэтому

$$\sqrt{|D_{k/\mathbf{Q}}(\mathfrak{a})|} = 2^{r_2}\operatorname{Vol}(F),$$

что и требовалось доказать.

Покажем теперь, как из теоремы 2 получается теорема 1. Как мы уже убедились, можно считать, что для рассматриваемого M_k-дивизора выполнены условия теоремы 2 и что связанный с ним идеал $\mathfrak{a}$ принадлежит одному из конечного числа представителей всех классов идеалов.

Для всякого M_k-дивизора $\mathfrak{c}$ имеем

$$\operatorname{Vol}(P_{\mathfrak{c}}) = \prod_{v \text{ веществ.}} (2\mathfrak{c}_v) \prod_{v \text{ компл.}} (\pi\mathfrak{c}_v^2) = 2^{r_1}\pi^{r_2} \prod_{v \in S_\infty} \mathfrak{c}_v^{N_v},$$

$$\operatorname{Vol}(F) = 2^{-r_2}\mathbf{N}\mathfrak{a}\sqrt{|D_k|},$$

откуда

$$\frac{\operatorname{Vol}(P_{\mathfrak{c}})}{\operatorname{Vol}(F)} = \frac{2^{r_1}(2\pi)^{r_2}}{|D_k|^{1/2}} \|\mathfrak{c}\|_k,$$

что и доказывает теорему 1.

§ 3. Вычисление одного объема

Начнем с некоторых замечаний о выпуклых телах в пространстве $\mathbf{R}^N$. Пусть μ означает обычную меру в $\mathbf{R}^N$.

Подмножество $C \subset \mathbf{R}^N$ называется *выпуклым*, если для любых двух точек x, $y \in C$ все точки вида

$$tx + (1-t)y, \quad 0 \leqslant t \leqslant 1,$$

тоже принадлежат C (иными словами, отрезок, соединяющий x и y, принадлежит C).

Множество C называется *симметричным* (относительно начала координат), если из того, что $x \in C$, следует, что $-x \in C$.

Теорема 3. *Пусть L — решетка размерности N в пространстве $\mathbf{R}^N$, и пусть C — замкнутое выпуклое симметричное подмножество этого пространства. Если*

$$\mu(C) \geqslant 2^N \mu(F),$$

где F — фундаментальная область решетки L, то в C содержится ненулевая точка решетки.

Доказательство. Сначала докажем теорему в случае строгого неравенства $\mu(C) > 2^N \mu(F)$.

Тогда в множестве $2^{-1}C$ содержатся две различные точки, разность которых принадлежит L. Действительно,

$$\frac{1}{2}C = \bigcup_{x \in L} \left(\frac{1}{2}C \cap F_x\right).$$

Так как множества справа попарно не пересекаются, имеем

$$\mu\left(\frac{1}{2}C\right) = \sum_{x \in L} \mu\left(\frac{1}{2}C \cap F_x\right) = \sum_{x \in L} \mu\left(\left(\frac{1}{2}C\right)_{-x} \cap F\right).$$

Но $\mu(2^{-1}C) = 2^{-N}\mu(C)$. Поэтому множества $(2^{-1}C)_{-x} \cap F$ не могут попарно не пересекаться — это противоречило бы принятому неравенству для меры F. Таким образом, существуют такие векторы y_1, $y_2 \in C$, что

$$\frac{1}{2}y_1 + x_1 = \frac{1}{2}y_2 + x_2,$$

где x_1, $x_2 \in L$, $x_1 \neq x_2$.

Тогда $2^{-1}(y_1 - y_2) \in L$. Но по симметрии из $y_2 \in C$ следует, что $-y_2 \in C$, так что в силу выпуклости $2^{-1}(y_1 - -y_2) \in C$, что и требовалось доказать.

Предположим теперь, что $\mu(C) \geqslant 2^N \mu(F)$. Для всякого $\varepsilon > 0$

$$\mu((1+\varepsilon)C) > \mu(C) \geqslant 2^N \mu(F),$$

так что в теле $(1+\varepsilon)C$ существуют ненулевые точки решетки. Полагая $\varepsilon \to 0$, находим, что хотя бы одна из них должна оставаться в C.

Наша следующая задача состоит в вычислении одного объема.

Лемма 3. *Пусть*

$$\mathbf{R}^N = \prod_{v \in S_\infty} k_v,$$

где среди множителей k_v имеется r_1 вещественных, r_2 комплексных, $N = r_1 + 2r_2$. Для всякого числа $a > 0$ обозначим буквой A выпуклое тело, заданное неравенством

$$\sum_{v \in S_\infty} N_v |z_v| \leqslant a.$$

Тогда его объем $V_{r_1, r_2}(a)$ равен

$$V_{r_1, r_2}(a) = 2^{r_1} 4^{-r_2} (2\pi)^{r_2} \frac{1}{N!} a^N.$$

Доказательство. Прежде всего очевидно, что

$$V_{r_1, r_2}(a) = a^N V_{r_1, r_2}(1),$$

так как

$$\sum_{v \in S_\infty} N_v |z_v| = |z_1| + \ldots + |z_{r_1}| +$$

$$+ |z_{r_1+1}| + |\bar{z}_{r_1+1}| + \ldots + |z_{r_1+r_2}| + |\bar{z}_{r_1+r_2}|.$$

Теперь заменим комплексные переменные $z_{r_1+1}, \ldots$ $\ldots, z_{r_1+r_2}$ полярными координатами.

Мы хотим вычислить объем $V_{r_1, r_2}(1)$. Вместо $(z_j, \bar{z}_j)$ используем полярные координаты $0 \leqslant \theta_j \leqslant 2\pi$ и $u_j \geqslant 0$.

Имеем

$$V_{r_1, r_2}(1) = \int u_{r_1+1} \dots u_{r_1+r_2}\, du_1 \dots du_{r_1}\, du_{r_1+1} \dots$$
$$\dots du_{r_1+r_2}\, d\theta_{r_1+1} \dots d\theta_{r_1+r_2},$$

где интеграл берется по области

$$|u_1| + \dots + |u_{r_1}| + 2u_{r_1+1} + \dots + 2u_{r_1+r_2} \leqslant 1.$$

Значение интеграла не изменится, если ограничиться интегрированием по области, где все $u_i \geqslant 0$, и умножить интеграл на 2^{r_1}.

Сделаем замену переменных $2u_j = w_j$, $2du_j = dw_j$ при $r_1 + 1 \leqslant j \leqslant r_1 + r_2$. Интеграл приобретает вид

$$2^{r_1} 4^{-r_2} (2\pi)^{r_2} W_{r_1, r_2}(1),$$

где

$$W_{r_1, r_2}(b) = \int u_{r_1+1} \dots u_{r_1+r_2}\, du_1 \dots du_{r_1+r_2},$$

а область интегрирования определяется неравенствами $u_i \geqslant 0$ при всех i и

$$u_1 + \dots + u_{r_1+r_2} \leqslant b.$$

Но

$$W_{r_1, r_2}(b) = b^N W_{r_1, r_2}(1).$$

Интегрирование по du_1 между 0 и 1 можно сделать внешним. Это дает

$$W_{r_1, r_2}(1) = \int_0^1 W_{r_1-1, r_2}(1-u_1)\, du_1 = \frac{1}{N} W_{r_1-1, r_2}(1)$$

(тривиальное интегрирование и однородность). По индукции, избавляясь от первых r_1 переменных, находим

$$W_{r_1, r_2}(1) = \frac{1}{N(N-1)\dots(N-r_1+1)} W_{0, r_2}(1).$$

Аналогично

$$W_{0, r_2}(1) = \int_0^1 t_1 (1-t_1)^{2r_2-2}\, dt_1 W_{0, r_2-1}(1).$$

Снова интегрируя, по индукции получаем

$$W_{0,r_2}(1) = \frac{1}{(2r_2)!} W_{0,0}(1) = \frac{1}{(2r_2)!}.$$

Следовательно,

$$W_{r_1,r_2}(1) = \frac{1}{N!},$$

откуда и вытекает требуемое значение для V_{r_1,r_2}.

§ 4. Константа Минковского

Пусть k — расширение поля $\mathbf{Q}$ степени N, $\mathfrak{a}$ — идеал кольца целых чисел I_k, рассматриваемый как решетка в пространстве $\mathbf{R}^N$. Выберем число a, фигурирующее в лемме 3, так, чтобы объем описанной там области был не меньше 2^N-кратного объема фундаментальной области решетки $\mathfrak{a}$. Обозначим через d_k абсолютную величину дискриминанта D_k; тогда достаточно положить

$$a^N = N!\, 4^{r_2}\pi^{-r_2}\mathbf{N}\mathfrak{a}d_k^{1/2}$$

(см. лемму 2, § 2). По теореме 3, в такой области содержится ненулевая точка решетки, т. е. существует элемент $\alpha \in \mathfrak{a}$, $\alpha \neq 0$, с условием

$$|\sigma_1\alpha| + \ldots + |\sigma_N\alpha| \leqslant a.$$

Поскольку среднее геометрическое не превосходит среднего арифметического, имеем

$$|N_{\mathbf{Q}}^k(\alpha)|^{1/N} \leqslant \frac{\sigma_1\alpha + \ldots + \sigma_N\alpha}{N},$$

откуда

$$|N_{\mathbf{Q}}^k(\alpha)| \leqslant \frac{a^N}{N^N} = \frac{N!}{N^N}\, 4^{r_2}\pi^{-r_2}\mathbf{N}\mathfrak{a}d_k^{1/2}.$$

Далее,

$$(\alpha) = \mathfrak{a}\mathfrak{b},$$

где $\mathfrak{b}$ — некоторый идеал. Поэтому

$$|N_{\mathbf{Q}}^k(\alpha)| = \mathbf{N}\mathfrak{a}\mathbf{N}\mathfrak{b}.$$

Сокращая на $\mathbf{N}\mathfrak{a}$, получаем следующий результат.

Теорема 4. *В любом классе идеалов существует идеал* $\mathfrak{b}$, *норма которого ограничена неравенством*

$$N\mathfrak{b} \leqslant C_k d_k^{1/2},$$

где C_k — *константа Минковского*:

$$C_k = \frac{N!}{N^N}\left(\frac{4}{\pi}\right)^{r_2}.$$

Следствие. *Модуль дискриминанта* d_k *всегда больше единицы. Всегда существует простое число, разветвленное в поле* k.

Доказательство. Так как $N\mathfrak{b} \geqslant 1$, имеем

$$d_k \geqslant \left(\frac{\pi}{4}\right)^{2r_2} \frac{N^{2N}}{(N!)^2} \geqslant \left(\frac{\pi}{4}\right)^{N} \frac{N^{2N}}{(N!)^2}.$$

При $N = 2$ получаем $d > 9/4 > 1$. Наше утверждение будет доказано, если мы проверим, что последовательность чисел

$$\left(\frac{\pi}{4}\right)^{N} \frac{N^{2N}}{(N!)^2}$$

монотонно убывает. Достаточно рассмотреть частное двух последовательных чисел; тривиальный подсчет доказывает требуемое.

Следующую таблицу значений константы Минковского я записал на лекциях Артина 12 лет назад.

N	r_1	r_2	$\left(\frac{4}{\pi}\right)^{r_2} \frac{N!}{N^N}$
2	0	1	0,63661
	2	0	0,5
3	1	1	0,28299
	3	0	0,22222
4	0	2	0,15198
	2	1	0,11937
	4	0	0,09375
5	1	2	0,06225
	3	1	0,04889
	5	0	0,0384

Для больших N теорема Минковского дает неравенство $d_k \geqslant (1/N)(\pi e^2/4)^N$.

Закончим это обсуждение примером, который Артин очень любил. Рассмотрим многочлен $f(X) = X^5 - X + 1$. Дискриминант Δ корня многочлена $X^5 + aX + b$ равен $5^5 b^4 + 2^8 a^5$. В нашем случае

$$\Delta = 2869 = 19 \cdot 151;$$

каждый простой делитель входит в первой степени.

Пусть α — корень многочлена $f(X)$ и $k = \mathbf{Q}(\alpha)$. Элемент α цел над $\mathbf{Z}$. Так как многочлен $f(X)$ неприводим по модулю 5, он неприводим и над $\mathbf{Z}$ (и над $\mathbf{Q}$), и k — поле пятой степени над $\mathbf{Q}$. Дискриминант $\mathbf{Z}$-модуля $\mathbf{Z}[\alpha]$ не содержит квадратных множителей, поэтому он совпадает с $D(I_k)$, ибо он может отличаться от $D(I_k)$ только на квадрат целого числа. Следовательно, $\mathbf{Z}[\alpha] = I_k$ в силу предположения 10 гл. III, § 3.

Нетрудно показать, что группой Галуа этого многочлена является вся симметрическая группа, так что поле разложения K имеет над $\mathbf{Q}$ степень 120.

В силу теоремы Минковского в каждом классе идеалов содержится идеал $\mathfrak{b}$ с нормой < 4 (тривиальная оценка с помощью табличного значения константы Минковского). Так как эта норма — целое число, она должна быть равна 1, 2 или 3. Случай $\mathbf{N}\mathfrak{p} = 2$ или $\mathbf{N}\mathfrak{p} = 3$ возможен лишь для простого идеала $\mathfrak{p}$; тогда степень поля классов вычетов $I_k/\mathfrak{p}$ над $\mathbf{Z}/p\mathbf{Z}$ должна быть равна единице, так что многочлен f должен иметь корень по модулю 2 или 3. Прямое вычисление показывает, что это не так. Остается единственная возможность: $\mathbf{N}\mathfrak{b} = 1$; но тогда $\mathfrak{b} = (1)$ и — о, чудо! — всякий идеал оказывается главным. Кольцо целых чисел является кольцом главных идеалов.

Как заметил Артин, можно показать, что поле разложения неразветвлено над расширением $\mathbf{Q}(\sqrt{D}) = \mathbf{Q}(\sqrt{19 \cdot 151})$. Это дает пример неразветвленного расширения с икосаэдральной группой. Артин указал однажды, что для любого нормального расширения K числового поля k с группой Галуа G существует бесконечно много конечных расширений E поля k, таких, что $K \cap E = k$, а композит KE неразветвлен над E. Чтобы получить такое поле E, достаточно построить расширение, которое локально поглощает все

ветвления поля K (это накладывает на E конечное число условий, которым можно удовлетворить в силу теоремы о приближении). Затем нужно обеспечить, чтобы $E \cap K = k$; с этой целью можно, например, воспользоваться теоремой о существовании и плотности простых идеалов с заданным символом Артина, которая будет доказана позже. Мы оставляем это читателю в качестве упражнения.

В качестве последнего приложения теоремы Минковского докажем следующий результат.

Теорема 5. *Пусть k — числовое поле, d_k — модуль его дискриминанта, $N_k = [k : \mathbf{Q}]$. Тогда отношение $N_k/\log d_k$ ограничено на множестве всех числовых полей $k \neq \mathbf{Q}$. Кроме того, существует только конечное число полей k с заданным значением дискриминанта.*

Доказательство. Первое утверждение получается из тривиальной оценки константы Минковского; мы оставляем проверку читателю. Тем самым, если дискриминант ограничен, степень поля тоже ограничена. Следовательно, для доказательства второго утверждения нужно установить конечность числа полей k заданной степени N с данным значением модуля дискриминанта d.

Рассмотрим N-мерное евклидово пространство

$$\mathbf{R}^N = \prod_{v \in S_\infty} k_v.$$

Предположим, что существует хоть одно комплексное нормирование v_0. Рассмотрим область, определенную неравенствами:

$$\begin{aligned} |z_{v_0} - \bar{z}_{v_0}| &\leqslant C_1 d^{1/2}, \\ |z_{v_0} + \bar{z}_{v_0}| &< \frac{1}{2}, \\ |z_v| &< \frac{1}{2}, \qquad v \neq v_0, \end{aligned}$$

где C_1 — большая константа, зависящая от N. Здесь символом z_v обозначен элемент поля k_v, которое отождествляется с $\mathbf{C}$ или $\mathbf{R}$.

Эта область выпукла и симметрична относительно начала координат. Следовательно, она должна содержать ненулевой элемент $\alpha \in I_k$. Так как абсолютная величина

нормы α (будучи ненулевым целым числом) не меньше единицы, из первого неравенства следует, что модуль мнимой части числа α больше нуля. Следовательно, два сопряженных к α числа, соответствующие нормированию v_0, различны. Кроме того, число α не совпадает ни с одним из остальных сопряженных, ибо его v-норма отличается от v_0-норм при всех $v \neq v_0$. Следовательно, α порождает поле k над $\mathbf{Q}$. Коэффициенты его уравнения над $\mathbf{Z}$ являются элементарными симметрическими функциями от α и всех сопряженных к α; поэтому они ограничены величиной, зависящей лишь от α и N. Таких уравнений имеется конечное число, что и доказывает наш результат в этом случае.

Если все нормирования вещественны, доказательство еще проще, ибо тогда можно заменить первую пару неравенств условием

$$|z_{v_0}| \leqslant C_1 d^{1/2},$$

сохранив остальные рассуждения.

Глава VI

ИДЕЛИ И АДЕЛИ

В классической теории числовое поле погружается в прямое произведение его пополнений по всем архимедовым нормированиям, т. е. в евклидово пространство. Сравнительно недавно (точнее, с того времени, как Шевалле ввел идели в 1936 г., а Вейль вскоре после этого дал доказательство теоремы Римана — Роха в терминах аделей) выяснилось, что удобнее рассматривать прямое произведение по всем нормированиям, включая p-адические, хотя и накладывать некоторые ограничения на компоненты (см. ниже). Эта глава содержит лишь самые элементарные сведения об иделях и аделях (конструкции, учитывающие мультипликативную и аддитивную структуры соответственно) и их топологиях. В обоих случаях мы доказываем некоторую теорему компактности и строим фундаментальную область. Хотя позже мы будем пользоваться существованием фундаментальных областей, знание их точного вида нам не понадобится.

Для всякой групповой схемы над кольцом целых чисел l_k числового поля можно рассмотреть ее точки с координатами в кольце аделей и попытаться доказать аналогичные результаты. Этот подход приводит к арифметической теории алгебраических групп, которой мы здесь не будем заниматься. Ограничимся указанием на то, что идели оказываются точками схемы мультипликативной группы над кольцом аделей.

§ 1. Ограниченные прямые произведения

Пусть k — числовое поле. Для всякого нормирования v поля k (мы подразумеваем, что оно индуцирует одно из стандартных нормирований поля $\mathbf{Q}$) определено попол-

ненное поле k_v, которое может быть вещественным, комплексным или $\mathfrak{p}$-адическим. Соответствующий эпитет применяется и к нормированию v.

И аддитивная группа k_v (обозначаемая иногда символом k_v^+), и мультипликативная группа k_v^* локально компактны. В $\mathfrak{p}$-адическом случае каждая из них содержит компактную подгруппу $\mathfrak{p}$-адических целых чисел и $\mathfrak{p}$-адических единиц соответственно.

Опишем общую конструкцию, позволяющую ввести ограниченное прямое произведение групп такого типа.

Пусть $\{v\}$ — некоторое множество индексов, и пусть для каждого v задана локально компактная коммутативная группа G_v. Пусть, далее, для всех, кроме конечного числа индексов v, в группе G_v зафиксирована открытая комплексная подгруппа H_v. *Ограниченным прямым произведением* групп G_v относительно подгрупп H_v называется подгруппа G прямого произведения групп G_v, состоящая из элементов, все компоненты которых, кроме конечного числа их, принадлежат H_v.

Пусть S — конечное множество индексов v, содержащее все v, для которых H_v не определена. Символом G_S обозначим подгруппу тех элементов группы G, компоненты которых принадлежат H_v при $v \notin S$. Тогда

$$G_S = \prod_{v \in S} G_v \times \prod_{v \notin S} H_v$$

— прямое произведение локально компактных групп, из которых все, кроме конечного числа, компактны. Поэтому G_S — локально компактная группа (в топологии произведения); введем на G локально компактную топологию, в которой каждая группа G_S открыта.

Гомоморфизм $G_v \to G$, отображающий G_v на v-компоненту, является вложением G_v как замкнутой подгруппы.

Ограниченное произведение аддитивных групп k_v относительно подгрупп локальных целых чисел $\mathfrak{o}_v$ (которые определены лишь для $\mathfrak{p}$-адических нормирований $v = v_\mathfrak{p}$) называется группой *аделей* поля k и обозначается символом A_k или просто A. Элементы группы A_S называются *S-аделями*.

Ограниченное произведение мультипликативных групп k_v^* относительно подгрупп единиц U_v кольца $\mathfrak{o}_v$ называется

группой *иделей* поля k и обозначается символом J_k или просто J. (Топология группы иделей *не* совпадает с топологией, индуцированной на иделях как подмножестве аделей!) Элементы группы J_s называются *S-иделями*.

Поле k вкладывается в группу аделей по диагонали. Действительно, всякий элемент $\alpha \in k$ является $\mathfrak{p}$-адическим целым для всех, кроме конечного числа $\mathfrak{p}$, так что, вкладывая α в каждое из полей k_v, мы превращаем вектор $(\alpha, \alpha, \alpha, \ldots)$ в адель.

Аналогично мультипликативная группа k^* вкладывается в группу иделей, потому что ненулевой элемент поля k является $\mathfrak{p}$-адической единицей для всех, кроме конечного числа $\mathfrak{p}$.

Оператор следа можно перенести на адели. Пусть E—конечное расширение поля k, $x \in A_E$, $x = (x_w)$, $w \in M_E$. По определению, v-компонента следа $\mathrm{Tr}_k^E(x)$ равна

$$\sum_{w \mid v} \mathrm{Tr}_w(x_w).$$

След является аделем поля k.

Подобным же образом можно ввести норму $N_k^E(a)$ иделя $a = (a_w)$ поля E, определив ее v-компоненту как

$$\prod_{w \mid v} N_w(a_w).$$

Эти определения совпадают с обычными понятиями нормы и следа элементов поля на подмножествах $k \subset A$ и $k^* \subset J$. Иными словами, следующие диаграммы коммутативны:

$$\begin{array}{ccc} E & \subseteq & A_E \\ \mathrm{Tr}\downarrow & & \downarrow\mathrm{Tr} \\ k & \subseteq & A_k \end{array} \qquad \begin{array}{ccc} E^* & \subseteq & J_E \\ N\downarrow & & \downarrow N \\ k^* & \subseteq & J_k \end{array}$$

Теорема 1. *Аддитивная группа k вложена как дискретная подгруппа группы аделей A. Мультипликативная группа k^* вложена как дискретная подгруппа группы иделей J.*

Доказательство. Пусть $\alpha \in k$. Близость α к нулю в топологии аделей означает, что $|\alpha|_v \leqslant 1$ для всех, кроме конечного числа нормирований v, и $|\alpha|_v$ очень

малы для конечного множества нормирований v. Из формулы произведения следует, что тогда $\alpha = 0$. Поэтому 0 — изолированный элемент подгруппы k в группе A; это и означает, что k дискретна в A. То же рассуждение в применении к элементу $\alpha \in k^*$, близкому к 1, показывает, что подгруппа k^* дискретна в J.

§ 2. Адели

Заметим, что если определить умножение аделей покомпонентно, они образуют топологическое кольцо (с делителями нуля). Умножение иделя a на адель x дает адель ax. Отображение

$$h_a : A \to A,$$

определенное для всякого иделя a формулой $h_a(x) = ax$, является топологическим линейным автоморфизмом аддитивной группы кольца A на себя.

Обозначим символом S_∞ подмножество архимедовых нормирований в канонической системе нормирований M_k.

Теорема 2. *Имеем*

$$k + A_{S_\infty} = A.$$

Факторгруппа A/k компактна.

Доказательство. Первое утверждение означает, что для всякого аделя x существует такой элемент $\alpha \in k$, что адель $x - \alpha$ имеет целые компоненты по всем дискретным нормированиям v. Это — простое обобщение китайской теоремы об остатках, которое можно доказать, например, так. Пусть $x \in A$, m — такое целое рациональное число, что mx имеет целые компоненты по всем дискретным нормированиям v. Пусть S — множество простых идеалов $\mathfrak{p} \subset I_k$, делящих m. В поле k существует элемент α, удовлетворяющий сравнениям

$$mx \equiv \alpha \pmod{\mathfrak{p}^\nu}$$

для всех $\mathfrak{p} \in S$, где ν — как угодно большое целое число (это следует из обычной китайской теоремы об остатках). Тогда элемент $x - \alpha/m$ будет $\mathfrak{p}$-цел для всех $\mathfrak{p}$, если ν достаточно велико.

Поле k можно погрузить в евклидово пространство

$$\prod_{v\in S_\infty} k_v = \mathbf{R}^N.$$

При этом целые числа I_k образуют решетку ранга $N = [k:\mathbf{Q}]$ в этом пространстве.

Для доказательства компактности факторгруппы A/k заметим, что любой элемент $x\in A$ сдвигом на число из k можно перевести в A_{S_∞}. После этого, сдвинув на целое число из I_k полученный элемент из A_{S_∞}, можно добиться того, чтобы его компоненты при всех $v\in S_\infty$ были ограничены, потому что целые числа образуют решетку максимального ранга. Следовательно, в каждом классе факторгруппы A/k имеется представитель, содержащийся в компактном подмножестве группы A_{S_∞}. Это означает, что факторгруппа A/k компактна.

На самом деле легко построить фундаментальную область для этой группы.

Теорема 3. *Пусть* $\omega_1, \ldots, \omega_N$ *— базис кольца целых чисел* I_k *поля* k *над* $\mathbf{Z}$. *Пусть* F_∞ *— подмножество произведения*

$$\prod_{v\in S_\infty} k_v,$$

состоящее из векторов вида $\sum t_i\omega_i$ *с* $0\leqslant t_i < 1$. *Тогда множество*

$$F = \prod_{v\notin S_\infty} \mathfrak{o}_v \times F_\infty$$

представляет собой фундаментальную область для группы $A \bmod k$.

Доказательство. Всякий элемент $x\in A$ можно перевести в A_{S_∞} сдвигом на элемент поля k, который определен однозначно по модулю I_k.

Если мы требуем, чтобы координаты t_i лежали в полуоткрытых интервалах $0\leqslant t_i < 1$, то это условие определяет сдвиг уже совсем однозначно.

§ 3. Идели

В этом параграфе мы проведем аналогичное исследование для мультипликативных иделей.

Пусть S — любое конечное множество нормирований в системе M_k, содержащее подмножество S_∞ архимедовых нормирований.

Для всякого $\mathfrak{p}$-адического нормирования $v \in M_k$ определено кольцо $\mathfrak{p}$-адических целых чисел $\mathfrak{o}_v$ и подгруппа единиц U_v этого кольца. Обе эти группы компактны.

Компоненты всякого иделя принадлежат группам k_v^*; все, кроме конечного числа из них, принадлежат даже U_v. Положим

$$\| a \|_v = \| a_v \|_v$$

и

$$\| a \| = \| a \|_k = \prod_{v \in M_k} \| a \|_v.$$

Так как все члены этого произведения, кроме конечного числа, равны 1, оно однозначно определено. Далее, отображение

$$a \rightsquigarrow \| a \|$$

определяет гомоморфизм

$$J \longrightarrow \mathbf{R}^+$$

группы J на мультипликативную группу положительных вещественных чисел. Очевидно, этот гомоморфизм непрерывен, а его ядром является замкнутая подгруппа группы J, которую мы обозначим J^0.

В силу формулы произведения k^* содержится в J^0 в качестве замкнутой дискретной подгруппы.

Можно ввести естественный гомоморфизм группы J на группу дробных идеалов кольца I_k. Действительно, для всякого иделя $a = (a_v)$ компоненты a_v принадлежат k_v, так что можно определить порядок a_v относительно $\mathfrak{p}$, если v есть $\mathfrak{p}$-адическое нормирование. Этот порядок равен целому числу r_v, которое определяется из равенства

$$a_v = \pi_v^{r_v} u,$$

где π_v — простой элемент, u — единица группы U_v. Положим

$$r_v = \operatorname{ord}_{\mathfrak{p}} a.$$

Тогда $r_v = 1$ для почти всех v, и тем самым выражение

$$\prod_{\mathfrak{p}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}} a}$$

представляет собой дробный идеал, обозначаемый также символом (a). Отображение

$$a \rightsquigarrow (a) = \prod \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}} a}$$

является гомоморфизмом группы J на группу дробных идеалов $\mathfrak{I}(k)$, ядро которого равно J_{S_∞}.

Элемент поля k^*, рассматриваемый как идель, называется *главным иделем*. С ним связан главный идеал. Следовательно, описанное выше отображение индуцирует гомоморфизм группы J/k^* на группу классов идеалов. Факторгруппа J/k^* называется группой *классов иделей* и обозначается символом C_k (или C, если очевидно, какое поле k имеется в виду). Она содержит замкнутую подгруппу $C_k^0 = J^0/k^*$.

Пусть S — конечное подмножество системы M_k; содержащее S_∞. J_S является открытой подгруппой группы J, а J_S^0 — открытой подгруппой группы J^0. Пересечение

$$J_S \cap k^*$$

мы будем обозначать символом k_S и называть группой *S-единиц*. Она, очевидно, является дискретной подгруппой группы J_S. При $S = S_\infty$ она совпадает с группой единиц кольца целых чисел I_k, т. е. с множеством тех элементов $\alpha \in k^*$, для которых $|\alpha_v| = 1$ при $v \notin S_\infty$. Факторгруппа J_S/k_S называется группой *классов S-иделей* и обозначается символом C_S. Определены естественные вложения

$$C_S \longrightarrow C, \quad C_S^0 \longrightarrow C^0,$$

при которых меньшая группа отображается на открытую и замкнутую подгруппу большей группы (это проверяется непосредственно). В терминах иделей первое отобра-

жение индуцировано вложениями

$$J_S \subsetneq J,$$
$$k \cap J_S = k_S \subsetneq k,$$
$$J_S/k_S \subsetneq J/k$$

и имеет место изоморфизм топологических групп

$$J/k^* J_S \approx C/C_S.$$

При $S = S_\infty$ группа $J/k^* J_{S_\infty}$ изоморфна группе классов идеалов (дробных) и потому конечна. Следовательно, при любом S группа $J/k^* J_S = C/C_S$ конечна, потому что она является гомоморфным образом группы C/C_{S_∞}. В частности, $k^* J_{S_\infty}$ можно рассматривать как ядро гомоморфизма группы J на группу классов идеалов. Группу $k^* J_S$ можно интерпретировать подобным же образом как ядро гомоморфизма на группу классов идеалов, представленных идеалами, взаимно простыми с S (в очевидном смысле).

Теорема 4. *Факторгруппа $J^0/k^* = C^0$ компактна. То же относится к группам J_S^0/k_S для любого конечного множества $S \supset S_\infty$.*

Доказательство. Пусть

$$\psi : J \longrightarrow \mathbf{R}^+$$

— отображение, ставящее в соответствие каждому иделю a число $\psi(a) = \| a \|$. Так как $\psi(k^*) = 1$, можно считать, что ψ определено на J/k^*. Его ядром является группа C^0. Для всякого вещественного числа $\varrho > 0$ положим $C^\varrho = \psi^{-1}(\varrho)$. Множество C^ϱ топологически изоморфно C^0. В самом деле, рассмотрим идель

$$a_\varrho = (\varrho^{1/N}, \ldots, \varrho^{1/N}, 1, 1, \ldots)$$

с компонентами $\varrho^{1/N}$ в архимедовых нормированиях и 1 — в остальных. Тогда $\psi(a_\varrho) = \varrho$ и $C^\varrho = a_\varrho C^0$. Поэтому достаточно доказать, что для некоторого ϱ множество C^ϱ компактно.

Лемма. *Можно найти такую константу $c_1(k) > 0$, что для $\varrho > c_1$ и всех $a \in J^\varrho$ существует такой элемент $\alpha \in k^*$, что $1 \leqslant \| \alpha a \|_v \leqslant \varrho$ при всех $v \in M_k$.*

Доказательство. Согласно теореме 0 § 1, гл. V, существует такой элемент $\alpha^{-1} \in k^*$, что

$$|\alpha^{-1}|_v \leqslant |a|_v$$

для всех $v \in M_k$. Отсюда вытекают неравенства

$$1 \leqslant \|a\alpha\|_v$$

для всех v и, следовательно, для всякого v

$$\|\alpha a\|_v = \frac{\prod \|\alpha a\|_w}{\prod\limits_{w \neq v} \|\alpha a\|_w} \leqslant \frac{\varrho}{1} = \varrho,$$

что и требовалось.

Для $\mathfrak{p}$-адических нормирований $v = v_{\mathfrak{p}}$ значения $\|\alpha a\|_v$ имеют вид

$$\ldots, \ 1/\mathbf{N}\mathfrak{p}, \ 1, \ \mathbf{N}\mathfrak{p}, \ (\mathbf{N}\mathfrak{p})^2, \ \ldots,$$

и лишь для конечного числа идеалов $\mathfrak{p}$ имеет место неравенство $\mathbf{N}\mathfrak{p} \leqslant \varrho$. Выберем число $\varrho > c_1$, как в лемме. Из сделанного замечания вытекает существование такого множества S, что

$$1 \leqslant \|\alpha a\|_v \leqslant \varrho, \quad v \in S,$$
$$\|\alpha a\|_v = 1, \quad v \notin S.$$

Пусть $X \subset J$ — подмножество, определенное этими неравенствами. Оно имеет вид

$$\prod_{v \in S} (\text{кольцо в } k_v^*) \times \prod_{v \notin S} U_v.$$

Каждый множитель в этом произведении компактен (каждое кольцо — это множество чисел с нормой между 1 и ϱ). Следовательно, множество X компактно. При каноническом гомоморфизме

$$J \longrightarrow C$$

X отображается на компактное подмножество группы C, содержащее C^0. Следовательно, C^0 компактно, что и требовалось доказать. Компактность факторгруппы J_S^0/k_S получается немедленно.

Из компактности группы J^0/k^* можно вывести теорему о единицах, не пользуясь соображениями, изложенными в конце § 1 гл. V. Укажем, как это делается.

Пусть дано множество $S \supset S_\infty$, состоящее из s элементов. Рассмотрим логарифмическое отображение

$$\log J_S \longrightarrow \mathbf{R}^s,$$

$$(\ldots, a_v, \ldots) \rightsquigarrow (\ldots, \log \| a \|_v, \ldots)_{v \in S}.$$

Группа J_S^0 отображается в гиперплоскость H^{s-1}, заданную уравнением

$$\xi_1 + \ldots + \xi_s = 0.$$

Группа k_S отображается на дискретную подгруппу пространства $\mathbf{R}^s$. Действительно, в каждом ограниченном подмножестве пространства $\mathbf{R}^s$ содержится только конечное число элементов группы $\log(k_S)$. (Это очевидно, ибо ограниченное множество определяется неравенствами, наложенными на локальные нормы элемента поля k и потому на коэффициенты уравнения над $\mathbf{Z}$, корнем которого является этот элемент.)

Теорема 5. *Образ* $\log(k_S)$ *является дискретной подгруппой ранга* $s-1$ *пространства* H^{s-1}.

Доказательство. Заметим сначала, что пространство H^{s-1} порождено над $\mathbf{R}$ векторами $\log(J_S^0)$, потому что $s-1$ компонент иделя из множества S можно выбрать произвольными, а затем подобрать последнюю (архимедову) компоненту так, чтобы сумма логарифмов была нулевой. Пусть W — подпространство, порожденное векторами $\log(k_S)$. Рассмотрим непрерывный гомоморфизм

$$J_S^0/k_S \longrightarrow K^{s-1}/W.$$

Его образ порождает H^{s-1}/W как векторное пространство над $\mathbf{R}$. Но это — непрерывный образ компактного множества; следовательно, он компактен. Отсюда вытекает, что $W = H^{s-1}$, что и требовалось доказать.

Ядро логарифмического отображения состоит в точности из корней из единицы, содержащихся в поле k, потому что оно представляет собой подгруппу, состоящую из элементов, все нормы которых ограничены, так что эта подгруппа конечна.

Опишем некоторую фундаментальную область для группы J/k^*; она понадобится нам для вычислений.

Выберем одно нормирование $v_0 \in S_\infty$ и обозначим через S'_∞ дополнение к v_0. Ограничение логарифмического отображения на $J^0_{S_\infty}$ будем обозначать буквой l. Отображение

$$l : J^0_{S_\infty} \longrightarrow \mathbf{R}^r$$

является гомоморфизмом на r-мерное евклидово пространство, $r = r_1 + r_2 - 1$. Эпиморфность следует из того, что r компонент иделя из множества S_∞ можно выбрать произвольно, а затем подобрать оставшуюся компоненту так, чтобы идель попал в J^0.

Пусть $\{\varepsilon_i\}$ $(i = 1, \ldots, r)$ — базис группы единиц по модулю корней из единицы. Тогда векторы $l(\varepsilon_i)$ образуют базис пространства $\mathbf{R}^r$, и для всякого элемента $b \in J^0_{S_\infty}$ имеем

$$l(b) = \sum z_i l(\varepsilon_i),$$

где вещественные числа z_i определены однозначно. Пусть P — параллелотоп в r-мерном пространстве, натянутый на векторы $l(\varepsilon_i)$, т. е. P — множество векторов вида

$$\sum z_i l(\varepsilon_i)$$

с $0 \leqslant z_i < 1$. Пусть, далее, w — число корней из единицы, содержащихся в поле k. Обозначим символом E^0 подмножество всех иделей $b \in l^{-1}(P)$, для которых $0 \leqslant \arg b_{v_0} < 2\pi/w$. Пусть, далее, h — порядок группы классов идеалов, $b^{(1)}, \ldots, b^{(h)}$ — элементы группы J^0, с которыми связаны идеалы, представляющие все классы. Имеет место следующий результат.

Теорема 6. *Подмножество E группы J^0*

$$E^0 b^{(1)} \cup \ldots \cup E^0 b^{(h)}$$

является фундаментальной областью этой группы $\bmod k^*$.

Доказательство. Деля любой идель $b \in J^0$ на однозначно определенный идель $b^{(\nu)}$, мы можем добиться, чтобы связанный с ним идеал был главным. Умножая на элемент поля, мы превратим этот главный идеал в единичный; идель, следовательно, попадет в группу $J^0_{S_\infty}$. Умножение на подходящую единицу сдвигает идель в $l^{-1}(P)$, а затем умножение на соответствующий корень из единицы позволяет исправить аргумент $\arg b_{v_0}$ так, чтобы идель попал в E^0. Очевидно, результат определен однозначно. Это доказывает нашу теорему.

Глава VII

ФУНКЦИОНАЛЬНОЕ УРАВНЕНИЕ

Мы начнем с теории двойственности для локальных полей, т. е. пополнений числовых полей относительно некоторого нормирования. В § 1 содержится аддитивная теория, а в § 2—мультипликативная; обе они используются в дальнейшем.

В § 3 мы устанавливаем локальное функциональное уравнение, а в § 4 проводим некоторые локальные выкладки и вычисляем специальные дзета-функции, которые и употребляются практически. В § 5 обсуждается мера Хаара и интегрирование на ограниченных прямых произведениях, а в § 6 строится аддитивная глобальная двойственность. Основной результат состоит в том, что группа аделей двойственна самой себе, а аддитивная дискретная группа поля k, вложенная в группу аделей, является в ней собственным ортогональным дополнением. Тем самым к этой ситуации можно применить формулу Пуассона (что и делается в § 7), из которой немедленно получается функциональное уравнение для L-рядов в абстрактной форме. На самом деле мы получаем больше (как и в классическом случае), потому что L-ряд представляется в виде всюду сходящегося интеграла плюс простой член, выделяющий возможные простые полюсы в точках $s=1$ или $s=0$.

Наконец, в § 8 мы вычисляем в явном виде объекты, фигурирующие в § 7, и приводим набор тождеств, полезных в последующих приложениях.

Условимся относительно некоторых обозначений. Для всякой локально компактной коммутативной группы G символом $\mathrm{Inv}(G)$ обозначается множество непрерывных комплекснозначных функций f на G, которые принадлежат $L_1(G)$ и обладают тем свойством, что их преобразо-

вание Фурье $\hat{f}$ тоже непрерывно и принадлежит $L_1(\hat{G})$. Для этих функций имеет место формула обращения Фурье, если мы надлежащим (и однозначным) образом выберем меру Хаара на $\hat{G}$ в зависимости от меры Хаара на G. Такая пара мер будет называться *взаимно двойственной*; в нашей теории аддитивные меры постоянно будут взаимно двойственными.

Мы будем часто пользоваться тем обстоятельством, что для всякого характера χ на компактной группе G имеет место тождество

$$\int_G \chi(x)\,dx = \begin{cases} \text{мера } G, & \text{если } \chi = \mathrm{id}, \\ 0, & \text{если } \chi \neq \mathrm{id}. \end{cases}$$

Ввиду тривиальности этого факта напомним его доказательство. Если $\chi \neq \mathrm{id}$, существует такой элемент $y \in G$, для которого $\chi(y) \neq 1$. Сдвигая G на y, что не меняет меры, получаем

$$\int_G \chi(x)\,dx = \int_G \chi(x+y)\,dx = \chi(y) \int_G \chi(x)\,dx.$$

Вычитая и пользуясь тем, что $\chi(y) \neq 1$, находим требуемое.

§ 1. Локальная аддитивная двойственность

Пусть $k = k_v$ означает пополнение числового поля относительно нормирования v. Поле k_v называется *локальным*. Оно является либо вещественным, либо комплексным, либо $\mathfrak{p}$-адическим; тот же эпитет относится к v. Символом $|\ |_v$ обозначается нормирование, индуцирующее обычную абсолютную величину на поле вещественных чисел, если v архимедово, и p-адическое нормирование $|p|_v = 1/p$, если v является $\mathfrak{p}$-адическим. Пусть $N_v = [k_v : \mathbf{Q}_v]$ — локальная степень. Мы полагаем

$$\| x \|_v = |x|_v^{N_v}.$$

Если v есть $\mathfrak{p}$-адическое нормирование, а $\mathbf{N}\mathfrak{p}$ — число элементов поля классов вычетов $\mathfrak{o}/\mathfrak{p}$, то

$$\| x \|_{\mathfrak{p}} = \| x \|_v = (\mathbf{N}\mathfrak{p})^{-\nu},$$

где $\nu = \mathrm{ord}_{\mathfrak{p}} x$.

Пусть сначала $k = \mathbf{Q}_v$. Введем некоторый нетривиальный характер аддитивной (локально компактной) группы k.

Если v — вещественное нормирование, положим

$$\lambda_0(x) \equiv -x \pmod 1.$$

Если v — p-адическое нормирование, $\mathbf{Z}_p$ и $\mathbf{Q}_p$ — кольцо целых p-адических чисел и поле всех p-адических чисел соответственно, то существует каноническое вложение факторгрупп $\mathbf{Q}_p/\mathbf{Z}_p \to \mathbf{Q}/\mathbf{Z}$; образ этого вложения — классы рациональных чисел, знаменатели которых являются степенями p. Вложим группу $\mathbf{Q}/\mathbf{Z}$ в группу $\mathbf{R}/\mathbf{Z}$ (вещественных чисел mod 1) и определим гомоморфизм λ_0 как композицию всех этих отображений:

$$\lambda_0 : \mathbf{Q}_p \to \mathbf{Q}_p/\mathbf{Z}_p \to \mathbf{Q}/\mathbf{Z} \to \mathbf{R}/\mathbf{Z}.$$

Для всякого конечного расширения k поля $\mathbf{Q}_v$ символом $\mathrm{Tr} = \mathrm{Tr}^k_{\mathbf{Q}_v}$ обозначим оператор следа и рассмотрим отображение

$$\lambda = \lambda_0 \circ \mathrm{Tr}.$$

Оно является непрерывным нетривиальным гомоморфизмом поля k в группу вещественных чисел mod 1.

Теорема 1. *Пусть k — локальное поле. Тогда билинейное отображение*

$$(x, y) \rightsquigarrow e^{2\pi i \lambda(xy)}$$

определяет изоморфизм аддитивной группы поля k с ее собственной группой характеров.

Доказательство. Легко проверить, что это спаривание непрерывно, а оба его ядра тривиальны. Этим определяется естественное отображение группы k в группу $\hat{k}$; оно непрерывно и мономорфно, а образ его всюду плотен. В действительности оно является изоморфизмом; в самом деле, если характер λ_x, определяемый формулой

$$\lambda_x(y) = e^{2\pi i \lambda(xy)},$$

близок к единице, он должен принимать близкие к 1 значения на большом компактном подмножестве поля k. Отсюда немедленно получается, что элемент x должен

быть близок к нулю. В свою очередь это означает, что образ k в группе характеров группы k полон и потому замкнут. Следовательно, отображение эпиморфно и, значит, является изоморфизмом.

Мы будем пользоваться той мерой Хаара на группе k, которая двойственна самой себе. Именно, положим:

dx — обычная мера Лебега на вещественной прямой, если k — вещественное поле;

dx — удвоенная обычная мера Лебега, если k — комплексная плоскость;

dx — мера, относительно которой кольцо $\mathfrak{o}$ целых чисел поля k имеет меру $(\mathbf{N}\mathfrak{D})^{-1/2}$, если k — $\mathfrak{p}$-адическое поле.

Здесь, как обычно, $\mathfrak{D} = \mathfrak{D}_{\mathfrak{p}}$ — локальная дифферента, т. е. такой идеал, что $\mathfrak{D}^{-1}$ является ортогональным дополнением к $\mathfrak{D}$ относительно спаривания, определенного в теореме 1.

Для любой меры Хаара μ *на* k *и любого ненулевого элемента* $a \in k^*$ *поля* k *имеем*

$$\mu(a\mathfrak{o}) = \| a \| \mu(\mathfrak{o})$$

или, символически, $d(ax) = \| a \| dx$.

Наше утверждение очевидно в архимедовом случае. Если v — $\mathfrak{p}$-адическое нормирование, достаточно проверить его справедливость для простого элемента $a = \pi$. В этом случае индекс открытой подгруппы $\pi\mathfrak{o}$ равен $\mathbf{Q}\mathfrak{p}$. Отсюда следует требуемое.

Теорема 2. *Определим образ Фурье* $\hat{f}$ *функции* $f \in L_1(k)$ *формулой*

$$\hat{f}(y) = \int f(x)\, e^{-2\pi i \lambda(xy)}\, dx.$$

Тогда при нашем выборе меры формула обращения имеет вид

$$\hat{\hat{f}}(x) = f(-x)$$

для всех $f \in \mathrm{Inv}(k)$.

Доказательство. Достаточно установить эту формулу для одной нетривиальной функции, ибо, как изве-

стно из абстрактного анализа Фурье, формула обращения всегда имеет такой вид с точностью до постоянного множителя. Для вещественного поля k можно рассмотреть $f(x) = e^{-\pi x^2}$, для комплексного — $f(x) = e^{-2\pi|x|^2}$, для $\mathfrak{p}$-адического — характеристическую функцию кольца $\mathfrak{o}$. Детали вычисления мы оставляем читателю (ср. § 4).

§ 2. Локальная мультипликативная теория

Группой *единиц* $U_v = U$ нашего локального поля называется ядро гомоморфизма

$$a \rightsquigarrow \|a\|$$

группы k^*. Если v есть $\mathfrak{p}$-адическое нормирование, U является компактной и открытой подгруппой; компактна она в любом случае.

Квазихарактером группы k^* называется всякий непрерывный гомоморфизм c этой группы в мультипликативную группу комплексных чисел. Тем самым характер — это квазихарактер, значения которого по абсолютной величине равны единице. Квазихарактер называется *неразветвленным*, если на U он тривиален.

Предложение 1. *Неразветвленные квазихарактеры представляют собой отображения вида*

$$c(a) = \|a\|^s = e^{s \log \|a\|},$$

где s — любое комплексное число. Оно однозначно определено, если v — архимедово нормирование, и с точностью до целого кратного $2\pi i/\log \mathbf{N}\mathfrak{p}$, если v является $\mathfrak{p}$-адическим.

Доказательство. Значение неразветвленного квазихарактера зависит только от $\|a\|$. Воспользуемся тем, что

$$k^* \approx U \times \mathbf{R}^+ \quad \text{и} \quad k^* \approx U \times \mathbf{Z}$$

в архимедовом и $\mathfrak{p}$-адическом случаях соответственно. Во втором случае разложение определяется, конечно, неканонически. Оно задается выбором элемента π первого порядка и представлением всякого элемента $a \in k^*$ в виде

$$a = \pi^r u,$$

где r — целое число, u — единица. Отсюда следует наше утверждение.

Ограничение любого квазихарактера c на группу единиц определяет некоторый характер этой группы, потому что она компактна. Обратно, для всякого характера χ группы k^* функция

$$c(a) = \chi(a) \| a \|^s$$

представляет собой квазихарактер.

Если v — архимедово нормирование, то любой характер χ группы k^* можно представить в виде

$$\chi(a) = \left(\frac{a}{|a|}\right)^m \| a \|^{i\varphi},$$

где $m = m_v(\chi)$ — целое число, равное 0 или 1, если v вещественное; $\varphi = \varphi_v(\chi)$ — вещественное число; m и φ однозначно определены характером χ.

Если v есть $\mathfrak{p}$-адическое нормирование, то подгруппы $1 + \mathfrak{p}^\nu (\nu \geqslant 0)$ образуют фундаментальную систему окрестностей единицы в группе U. Поэтому любой квазихарактер c должен на одной из этих подгрупп быть единичным. Пусть m — наименьшее целое число, для которого $c(1 + \mathfrak{p}^m) = 1$. Идеал

$$\mathfrak{f}_\mathfrak{p} = \mathfrak{f}_{\mathfrak{p}, \chi} = \mathfrak{p}^m$$

мы назовем *ведущим идеалом* характера c. (Если $m = 0$, то $\mathfrak{f} = \mathfrak{o}$, по определению.)

Число $m_v(\chi)$ или $\operatorname{ord}_\mathfrak{p} \mathfrak{f}_\chi = m$ в архимедовом и неархимедовом случаях соответственно мы будем одинаково называть *степенью ветвления* квазихарактера c и характера χ.

Зафиксировав простой элемент π в $\mathfrak{p}$-адическом случае и соответствующее разложение

$$k^* \approx U \times \mathbf{R}^+ \quad \text{или} \quad k^* \approx U \times \mathbf{Z},$$

мы будем символом a' обозначать U-компоненту элемента $a \in k^*$ (так что $a' = a/|a|$, если v — архимедово), а символом c' — ограничение c на U. Элементарные свойства групп $\mathbf{R}^+$ и $\mathbf{Z}$ показывают, что

Предложение 2. *Квазихарактерами группы k^* являются всевозможные отображения вида*

$$a \rightsquigarrow c(a) = c'(a') \| a \|^s,$$

где c' — любой характер группы U, однозначно определенный квазихарактером c. Комплексное число s определяется предложением 1.

Вещественная часть числа s, введенного в предложении 2, однозначно определяется квазихарактером. Мы будем называть ее *вещественной частью* этого квазихарактера и обозначать символом $\mathrm{Re}(c)$.

Вернемся теперь к мере Хаара. Если функция $g(a)$ принадлежит пространству $C_c(k^*)$ непрерывных функций на k^* с компактным носителем, то функция $g(x)\|x\|^{-1}$ принадлежит пространству $C_c(k^+ - 0) = C_c(k - 0)$. Следовательно, мы можем определить нетривиальный функционал на $C_c(k^*)$ формулой

$$g \rightsquigarrow \int\limits_{k-0} g(x)\|x\|^{-1}\,dx.$$

Очевидно, он инвариантен относительно мультипликативных сдвигов и положителен, а следовательно, соответствует некоторой мере Хаара. Переходя к пределу, получаем

Предложение 3. *Функция $g(a)$ принадлежит пространству $L_1(k^*)$ в том и только том случае, когда функция $g(x)\|x\|^{-1}$ принадлежит пространству $L_1(k-0)$. Для таких функций имеет место тождество*

$$\int\limits_{k^*} g(a)\,d_1^*a = \int\limits_{k-0} g(x)\|x\|^{-1}\,dx,$$

где d_1^*a — вышеупомянутая мера Хаара на группе k^*, а dx — мера на аддитивной группе k.

На самом деле нам будет удобнее пользоваться мерой Хаара на k^*, отличающейся от описанной в $\mathfrak{p}$-адическом случае некоторым множителем так, чтобы мера группы U почти всегда была равна единице. Тем самым мы положим

$$d^*a = \frac{da}{\|a\|}, \qquad \text{если } v \text{ — архимедово,}$$

$$d^*a = \frac{\mathrm{Np}}{\mathrm{Np}-1}\,\frac{da}{\|a\|}, \qquad \text{если } v \text{ — } \mathfrak{p}\text{-адическое.}$$

Предложение 4. *В* $\mathfrak{p}$*-адическом случае* $\int\limits_U d^*a = (\mathbf{N}\mathfrak{D})^{-1/2}$.

Доказательство. Результат получается немедленно из определения аддитивной меры Хаара, данного в § 1, если учесть, что $\|a\| = 1$ при $a \in U$ и что $U = \mathfrak{o} \setminus \mathfrak{p}$.

§ 3. Локальное функциональное уравнение

В этом параграфе $f(x)$ — некоторая комплекснозначная функция на k^+, $f(a)$ — ее ограничение на k^*. Мы рассматриваем функции, которые удовлетворяют следующим условиям:

Л1$_v$. $f(x)$ и $\hat{f}(x)$ непрерывны и принадлежат пространству $L_1(k^+)$.

Л2$_v$. $f(a)\|a\|^\sigma$ и $\hat{f}(a)\|a\|^\sigma$ при $\sigma > 0$ принадлежат пространству $L_1(k^*)$.

На множестве пар (f, c), состоящих из функции f и квазихарактера c, определим ζ-функцию, полагая

$$\zeta(f, c) = \int f(a)\, c(a)\, d^*a.$$

Если квазихарактер c задан в виде $c(a) = \chi(a)\|a\|^s$, где χ — некоторый характер группы k^*, мы будем пользоваться также записью

$$\zeta(f, \chi, s) = \int f(a)\, \chi(a)\|a\|^s\, d^*a.$$

При фиксированных χ и f дзета-функцию можно рассматривать как функцию одной комплексной переменной, которая в силу условий, наложенных на f, голоморфна при $\mathrm{Re}(s) > 0$ (или $\mathrm{Re}(c) > 0$). В этой области, как легко видеть, можно вносить дифференцирование под знак интеграла. Назовем квазихарактеры c_1, c_2 *эквивалентными*, если $c_1(a) = c_2(a)\|a\|^{s_1}$ для некоторого комплексного числа s_1. На каждом классе эквивалентности квазихарактеров дзета-функция является комплекснозначной функцией; ясно, что́ следует понимать под ее аналитическим продолжением.

Для любого квазихарактера c положим $\hat{c}(a) = \| a \| c^{-1}(a)$. Функциональное уравнение будет следствием основной леммы.

Лемма. *Для любого квазихарактера c в области $0 < \mathrm{Re}(c) < 1$ и любых двух функций f, g, удовлетворяющих условиям $Л1_v$, $Л2_v$, имеем*

$$\zeta(f, c)\,\zeta(\hat{g}, \hat{c}) = \zeta(\hat{f}, \hat{c})\,\zeta(g, c).$$

Доказательство. Произведение $\zeta(f, c)\,\zeta(\hat{g}, \hat{c})$ можно представить в виде абсолютно сходящегося двойного интеграла по $k^* \times k^*$:

$$\int\int f(a)\,\hat{g}(b)\,c(ab^{-1})\,\| b \|\, d^*a\, d^*b.$$

Так как мера инварианта относительно автоморфизма $(a, b) \to (a, ab)$, то этот интеграл равен

$$\int\int f(a)\,\hat{g}(ab)\,c(b^{-1})\,\| ab \|\, d^*a\, d^*b.$$

Подставляя сюда определение функции $\hat{g}$ и мультипликативных мер $d^*a\, d^*b$, находим (с точностью до легко вычислимого постоянного множителя)

$$\int\int\int f(a)\,g(x)\,e^{-2\pi i \lambda(axb)}\,dx\,da\,db.$$

Это выражение симметрично относительно f и g, что и доказывает лемму.

Если мы сможем доказать существование хотя бы одной функции f, для которой $\zeta(\hat{f}, \hat{c}) \neq 0$, отсюда будет следовать, что отношение $\zeta(f, c)/\zeta(\hat{f}, \hat{c})$ определено однозначно и не зависит от f. Мы обозначим это отношение символом $\varrho(c)$, а в следующем параграфе для каждого класса эквивалентности квазихарактеров над локальным полем построим функцию f, для которой $\varrho(c)$ определено. Отсюда будет следовать

Теорема 3. *Дзета-функция допускает аналитическое продолжение на область всех квазихарактеров, определяемое функциональным уравнением вида*

$$\zeta(f, c) = \varrho(c)\,\zeta(\hat{f}, \hat{c}).$$

Множитель $\varrho(c)$, *не зависящий от* f, *является мероморфной функцией, которая определяется функциональным уравнением в области* $0<\mathrm{Re}(c)<1$ *и аналитически продолжается на все квазихарактеры.*

Из функционального уравнения получаются следующие свойства функции $\varrho(c)$ (их проверка тривиальна, и мы оставляем ее читателю):

1) $\varrho(\hat{c})=\dfrac{c(-1)}{\varrho(c)}$,

2) $\varrho(\bar{c})=c(-1)\,\overline{\varrho(c)}$,

3) при $\mathrm{Re}(c)=1/2$ имеем $|\varrho(c)|=1$.

В следующем параграфе мы укажем для каждого класса квазихарактеров весовую функцию f_c, которая придает локальной дзета-функции обычный вид и, в частности, позволяет вычислить множитель $\varrho(c)$.

§ 4. Локальные вычисления

v—архимедово нормирование. Мы пользуемся следующими обозначениями:

x—k_v^+-переменная; a—k_v^*-переменная;

dx—N_v-кратная мера Лебега; $d^*a=da/\|a\|$.

Любой характер χ группы k_v^* представляется в виде

$$\chi(a)=\left(\frac{a}{|a|}\right)^m |a|^{iN_v\varphi},$$

где $m=m_v(\chi)$ и $\varphi=\varphi_v(\chi)$. Если v—вещественное нормирование, то $m=0$ или 1. Положим, далее:

$$s_v=s_v(\chi)=N_v(s+i\varphi)+|m|,$$
$$\hat{s}_v=N_v(1-s-i\varphi)+|m|.$$

В вещественном случае

$$f_{\chi,v}(x)=x^m e^{-\pi x^2}.$$

В комплексном случае

$$f_{\chi,v}(x)=\begin{cases}\dfrac{1}{2\pi}\bar{x}^{|m|}e^{-2\pi|x|^2}, & \text{если } m\geqslant 0,\\ \dfrac{1}{2\pi}x^{|m|}e^{-2\pi|x|^2}, & \text{если } m\leqslant 0.\end{cases}$$

Заметим, что выбранные нами функции $f_{\chi, v}$ зависят только от m, так что их можно обозначать символами $f_m = f_{m_v}$. Далее, для любого квазихарактера c, которому соответствует на группе единиц характер χ, мы пишем f_c вместо f_χ.

Теорема 4. *В описанных обозначениях для всех квазихарактеров* $c(a) = \chi(a)\,\|a\|^s$ *имеют место формулы:*

$$\hat{f}_m(x) = i^{|m|} f_{-m}(x) \text{ (если } v \text{ вещественно, то } f_{-m} = f_m),$$

$$\zeta(f_c, c) = \zeta(f_{\chi, v}, \chi, s) = (N_v\pi)^{-s_v/2}\,\Gamma(s_v/2),$$

$$\zeta(\hat{f}_c, \hat{c}) = \zeta(\hat{f}_{\chi, v}, \chi, 1-s) = i^{|m|}\,(N_v\pi)^{-\hat{s}_v/2}\,\Gamma(\hat{s}_v/2).$$

Доказательство. В вещественном случае первое утверждение проверяется без труда, и мы оставляем эту проверку читателю.

При доказательстве формул для дзета-функций в вещественном случае мы несколько раз пользуемся определением гамма-функции:

$$\Gamma(s) = \int_0^\infty e^{-u} u^{s-1}\,du.$$

Вычисления здесь совсем легкие, и мы также оставляем их читателю.

В комплексном случае доказательство первого тождества слегка сложнее. Сначала мы докажем формулу для $\hat{f}_m$ при $m \geqslant 0$ индукцией по m. В соответствии с классическими обозначениями рассмотрим комплексную переменную

$$z = x + iy = re^{i\theta}.$$

При $m = 0$ разобьем интеграл Фурье на два вещественных интеграла и воспользуемся классической формулой

$$\int_{-\infty}^{\infty} e^{-\pi u^2 + 2\pi i x u}\,du = e^{-\pi x^2}.$$

Пусть мы уже доказали наше тождество для некоторого $m \geqslant 0$, так что

$$\int f_m(w)\, e^{-2\pi i \lambda (zw)}\, dw = i^m f_{-m}(z).$$

Разделяя вещественную и мнимую части, получаем

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} (u-iv)^m e^{-2\pi (u^2+v^2)+4\pi i (xu-yv)} 2\, du\, dv =$$

$$= i^m (x+iy)^m e^{-2\pi (x^2+y^2)}.$$

Положим $D = (4\pi i)^{-1}[\partial/\partial x + i\,(\partial/\partial y)]$ и применим оператор D к обеим частям тождества (это легко, потому что в силу аналитичности функции z^m имеем $D(x+iy)^m = 0$). В результате получится наше утверждение для $m+1$. Общий шаг индукции тем самым проведен.

Для доказательства нашего тождества при $m < 0$ следует рассмотреть преобразование Фурье уже доказанной формулы

$$\hat{f}_{-m}(z) = i^{|m|} f_m(z)$$

и учесть, что $\hat{\hat{f}}(z) = f(-z)$.

При доказательстве формул для дзета-функций можно считать, не ограничивая общности, что $\varphi = 0$, а характер χ имеет вид $c_m(a) = e^{im\theta}$. Тогда

$$\zeta(f_m, c_m, s) = \int f_m(a)\, c_m(a)\, \|a\|^s\, d^*a =$$

$$= \int_0^{\infty}\int_0^{2\pi} \frac{1}{2\pi} r^{2(s-1)+|m|} e^{-2\pi r^2} 2r\, dr\, d\theta =$$

$$= \int_0^{\infty} (r^2)^{(s-1)+|m|/2} e^{-2\pi r^2}\, d(r^2),$$

откуда требуемое тождество немедленно получается заменой переменных. Функция $\zeta(\hat{f}, \hat{c})$ после этого вычисляется с помощью первого утверждения теоремы и определений.

v — **$\mathfrak{p}$-адическое нормирование.** Мы пользуемся следующими обозначениями:

x — k_v^+-переменная; a — k_v^*-переменная;

dx — мера, относительно которой мера $\mathfrak{o}$ равна $(\mathbf{N}\mathfrak{D})^{-1/2}$; $d^*a = \frac{\mathbf{Np}}{\mathbf{Np}-1} \cdot \frac{da}{\|a\|}$.

Символом $m_{\chi, v} = m$ обозначается порядок ведущего идеала характера χ, так что $m \geqslant 0$. Как и в архимедовом случае, функция $f_{\chi, v}$ будет зависеть только от этого целого числа; именно, положим:

$$f_m(x) = \begin{cases} e^{2\pi i \lambda(x)}, & x \in \mathfrak{D}^{-1}\mathfrak{f}_\chi^{-1}, \\ 0, & x \notin \mathfrak{D}^{-1}\mathfrak{f}_\chi^{-1} \end{cases}$$

($\mathfrak{D}$ и $\mathfrak{f}_\chi$ относятся, конечно, к $\mathfrak{p}$).

Для удобства будем писать $\mathfrak{D}_\chi$ вместо $\mathfrak{D}\mathfrak{f}_\chi$.

Предложение 5. *Имеем*

$$\hat{f}_m(x) = \begin{cases} (\mathbf{N}\mathfrak{D})^{1/2}(\mathbf{N}\mathfrak{f}_\chi), & x \equiv 1 \pmod{\mathfrak{f}_\chi}, \\ 0, & x \not\equiv 1 \pmod{\mathfrak{f}_\chi}. \end{cases}$$

Доказательство. Это немедленно следует из того обстоятельства, что интеграл от тривиального характера по компактной группе G равен $\mu(G)$, а от нетривиального — нулю. (Роль компактной группы в нашем случае играет $(\mathfrak{D}_\chi)^{-1}$.)

Отметим, что f_0 — характеристическая функция группы $\mathfrak{D}^{-1}$, а $\hat{f}_0 - (\mathbf{N}\mathfrak{D})^{1/2}$-кратная характеристическая функция группы $\mathfrak{o}$.

Вычислим теперь в явном виде дзета-функцию для неразветвленных характеров. Если характер χ неразветвлен, значение $\chi(\pi)$ не зависит от выбора простого элемента π, и мы будем писать просто $\chi(\mathfrak{p})$.

Теорема 5. *Пусть χ — неразветвленный характер группы k^*, f — характеристическая функция идеала $\mathfrak{p}^n$. Тогда*

$$\zeta(f, \chi, s) \frac{(\mathbf{N}\mathfrak{D})^{-1/2}\chi(\mathfrak{p})^n (\mathbf{Np})^{-ns}}{1 - \frac{\chi(\mathfrak{p})}{\mathbf{Np}^s}}.$$

Доказательство. В несложном подсчете используется определение мультипликативной меры Хаара через аддитивную, а интеграл представляется в виде суммы интегралов по кольцам $\mathfrak{p}^\nu \setminus \mathfrak{p}^{\nu+1}$, где ν меняется от n до ∞. На каждом таком кольце $\|a\|^s$ постоянна, а $\chi(a) = \chi(\pi^\nu)$, потому что характер χ неразветвлен. Детали мы оставляем читателю.

Следствие 1. *Имеем*

$$\zeta(f_0, \chi_0, s) = \frac{(N\mathfrak{D})^{s-1/2}}{1 - 1/N\mathfrak{p}^s}$$

и

$$\zeta(\hat{f}_0, \chi_0, 1-s) = \frac{1}{1 - N\mathfrak{p}^{s-1}}.$$

Доказательство. Применить теорему к $n = -\operatorname{ord}\mathfrak{D}$ в первом случае и к $n = 0$ — во втором.

Следствие 2. *Пусть χ — неразветвленный характер группы k^*, $f_0 = f_\chi$ — характеристическая функция группы $\mathfrak{D}^{-1}$. Тогда*

$$\zeta(f_0, \chi, s) = \frac{(N\mathfrak{D})^{s-1/2}\,\chi(\mathfrak{D}^{-1})}{1 - \dfrac{\chi(\mathfrak{p})}{N\mathfrak{p}^s}}$$

и

$$\zeta(\hat{f}_0, \bar{\chi}, 1-s) = \frac{1}{1 - \chi^{-1}(\mathfrak{p})\,N\mathfrak{p}^{s-1}}.$$

Заметим, что для неразветвленных характеров в знаменателе дзета-функции стоит обычное выражение $1 - \chi(\mathfrak{p})(N\mathfrak{p})^{-s}$. Это не так для разветвленных характеров.

Теорема 6. *Пусть π — некоторый простой элемент, χ — характер группы k^*, $m > 0$ — порядок его ведущего идеала, $\{\varepsilon\}$ — система единиц, представителей классов $U/(1 + \mathfrak{f}_\chi)$. Положим $o(\chi) = \operatorname{ord}(\mathfrak{D}_\chi)$ и*

$$\eta(x) = e^{2\pi i \lambda(x)}.$$

Пусть, далее, $c(a) = \chi(a) \| a \|^s$. *Тогда*

$$\zeta(f_m, c) = \zeta(f_m, \chi, s) = (\mathbf{N}\mathfrak{D}_\chi)^s \mu (1 + f_\chi) \tau(\chi),$$

где $\tau(\chi) = \sum_{\varepsilon} (\chi\eta)(\varepsilon\pi^{-o(\chi)})$. *Далее,*

$$\zeta(\hat{f}_m, \hat{c}) = \zeta(\hat{f}_m, \bar{\chi}, 1-s) = (\mathbf{N}\mathfrak{D})^{1/2} (\mathbf{N}f_\chi) \mu (1 + f_\chi).$$

Замечание: мера μ — это, разумеется, d^*a, а π в обозначении $2\pi i$ — 3,1416... .

Доказательство. По определению,

$$\zeta(f_m, c) = \int_{\mathfrak{D}_\chi^{-1}} \eta(a) \chi(a) \| a \|^s d^*a = \sum_{-o(\chi)}^{\infty} (\mathbf{N}\mathfrak{p})^{-vs} \int_{A_v} \eta(a) \chi(a) d^*a,$$

где A_v — кольцо $\mathfrak{p}^v \setminus \mathfrak{p}^{v+1}$. Мы утверждаем, что все члены в этой сумме, кроме первого, равны нулю.

Случай 1. $v \geqslant -\operatorname{ord}\mathfrak{D}$. Тогда $\eta(a) = 1$ на A_v и интересующий нас интеграл имеет вид

$$\int_{A_v} \chi(a) d^*a = \int_U \chi(a\pi^v) d^*a = \chi(\pi^v) \int_U \chi(a) d^*a.$$

Это — нуль, потому что характер χ нетривиален на U.

Случай 2. $-\operatorname{ord}\mathfrak{D} > v > -\operatorname{ord}\mathfrak{D} - \operatorname{ord} f_\chi$. (Этот случай может представиться лишь при $m > 1$.) Чтобы справиться с ним, разобьем A_v на непересекающиеся подмножества вида $a_0 + \mathfrak{D}^{-1} = a_0(1 + \mathfrak{D}^{-1}\mathfrak{p}^{-v})$. На каждом таком подмножестве функция λ постоянна и равна $\lambda(a_0)$, а наш интеграл равен

$$\eta(a_0) \int_{a_0 + \mathfrak{D}^{-1}} \chi(a) d^*a.$$

Обращение его в нуль следует из того, что мультипликативным сдвигом этот интеграл можно превратить в интеграл по группе $1 + \mathfrak{D}^{-1}\mathfrak{p}^{-v}$, на которой наш характер нетривиален.

Тем самым получаем

$$\zeta(f_m, \chi, s) = (\mathbf{N}\mathfrak{D}_\chi)^s \int\limits_{A_{-0}(\chi)} \eta(a)\,\chi(a)\,d^*a.$$

Превратить это выражение в формулу, выписанную в условии теоремы, не представляет труда.

Для вычисления функции $\zeta(\hat{f}_m, \overline{\chi}, 1-s)$ следует воспользоваться тем, что $\hat{f}_m$ представляет собой $(\mathbf{N}\mathfrak{D})^{1/2}(\mathbf{N}\mathfrak{f}_\chi)$-кратную характеристическую функцию группы $1+\mathfrak{f}_\chi$, а функция $\chi^{-1}(a)\,\|a\|^{1-s}$ на этой подгруппе равна 1. Отсюда немедленно получаем требуемое.

Следствие. *Пусть* $c(a) = \chi(a)\,\|a\|^s$, *где* χ — *характер с ведущим идеалом* $\mathfrak{f}$ *порядка* $m > 0$. *Тогда*

$$\varrho(c) = (\mathbf{N}\mathfrak{D}_\chi)^{s-1/2}(\mathbf{N}\mathfrak{f})^{-1/2}\,\tau(\chi),$$

а число $(\mathbf{N}\mathfrak{f})^{-1/2}\tau(\chi)$ *по модулю равно* 1.

Доказательство. Первое утверждение следует из определения $\varrho(c)$ как отношения соответствующих дзета-функций. Для доказательства второго следует положить $s = 1/2$ и воспользоваться тем, что при $\mathrm{Re}(c) = 1/2$ имеем $|\varrho(c)| = 1$.

§ 5. Ограниченные прямые произведения

В предыдущей главе мы изучили топологию ограниченных прямых произведений и, в частности, групп иделей и аделей. Здесь мы займемся мерой Хаара и двойственностью Понтрягина.

Пусть $\{v\}$ — произвольное множество индексов, G_v — локально компактная коммутативная группа; $H_v \subset G_v$ — компактная открытая подгруппа, заданная для всех, кроме конечного числа индексов v.

Квазихарактером ограниченного произведения G групп G_v называется его непрерывный гомоморфизм в группу $\mathbf{C}^*$.

Ограничение квазихарактера c группы G на подгруппу G_v обозначается символом c_v. В силу непрерывности на G гомоморфизм c_v тривиален на всех, кроме конечного числа групп H_v; это следует из того, что мультипликативная

группа комплексных чисел не содержит нетривиальных подгрупп в малой окрестности единицы. Далее, имеет место формула

$$c(a) = \prod_v c_v(a_v),$$

потому что все, кроме конечного числа членов этого произведения, равны 1.

Обратно, если задан набор квазихарактеров c_v групп G_v, обращающихся в 1 на всех, кроме конечного числа подгрупп H_v, их произведение определяет квазихарактер c группы G.

Отметим, что c является характером в том и только том случае, когда c_v для всех v является характером.

Пусть $\hat{G}$ — группа характеров группы G, $H^\perp$ — ортогональное дополнение замкнутой подгруппы $H \subset G$, состоящее из характеров, тривиальных на H. Имеют место естественные изоморфизмы

$$\hat{G}/H^\perp \approx H \quad \text{и} \quad (G/H)\hat{} \approx H^\perp.$$

В нашем частном случае ограниченных прямых произведений легко проверить следующую теорему.

Теорема 7. *Ограниченное прямое произведение групп $\hat{G}_v$ относительно подгрупп $H_v^\perp$ (которые компактны в силу компактно-дискретной двойственности), естественно изоморфно, топологически и алгебраически, группе характеров $\hat{G}$ группы G.*

Этот изоморфизм, разумеется, задается формулой

$$\chi = \prod \chi_v.$$

Мера Хаара. Предположим, что на каждой из групп G_v выбрана мера Хаара da_v, относительно которой подгруппа H_v имеет меру 1 для почти всех v. Мы хотим определить меру Хаара на группе G, для которой в некотором смысле $da = \prod da_v$. С этой целью привлечем открытые подгруппы G_S, являющиеся произведением локально компактных групп, из которых почти все компактны. На группах G_S можно определить глобальную меру как произведение локальных. На группе G существует единственная

мера Хаара $\prod da_v$, индуцирующая на каждой из подгрупп G_S это произведение мер (проверка тривиальна).

Лемма. *Для всякой функции $f(a)$ на группе G имеем*

$$\int_G f(a)\,da = \lim_S \int_{G_S} f(a)\,da$$

при выполнении одного из двух условий:

1) *функция $f(a)$ измерима и неотрицательна; в этом случае $+\infty$ включается в число допустимых значений интегралов;*

2) *$f(a) \in L_1(G)$; в этом случае значениями интегралов являются комплексные числа.*

Доказательство. В обоих случаях $\int f(a)\,da$ представляет собой предел интегралов по всем большим компактным подмножествам группы G, а любой компакт содержится в одной из подгрупп G_S.

Теорема 8. *Пусть для каждого индекса v задана непрерывная функция $f_v \in L_1(G_v)$, которая для почти всех v равна 1 на H_v. Положим*

$$f(a) = \prod f_v(a_v)$$

на G (произведение в действительности конечно). Функция f непрерывна. Если, кроме того,

$$\prod_v \int |f_v(a_v)|\,da_v = \lim_S \prod_{v \in S} \int |f_v(a_v)|\,da_v$$

конечно, то $f(a) \in L_1(G)$ и

$$\int_G f(a)\,da = \prod_v \int_{G_v} f_v(a_v)\,da_v.$$

Доказательство. Очевидно.

Преобразование Фурье. Мы сохраняем прежние обозначения; ξ — переменный элемент группы $\hat{G}$. Пусть $d\xi_v$ — мера на группе $\hat{G}_v$, двойственная к мере da_v на G_v. Пусть $f_v(a_v)$ — характеристическая функция подгруппы H_v.

Ее преобразование Фурье

$$\hat{f}_v(\xi_v) = \int f_v(a_v)\,\overline{\xi_v(a_v)}\,da_v$$

равно характеристической функции подгруппы $H_v^\perp$, умноженной на меру группы H_v.

Из формулы обращения поэтому следует, что

$$\Big(\int\limits_{H_v} da_v\Big)\Big(\int\limits_{H_v^\perp} d\xi_v\Big) = 1,$$

так что мера группы $H_v^\perp$ для почти всех v равна 1. Тем самым мы можем определить глобальную меру

$$d\xi = \prod d\xi_v.$$

Теорема 9. *Пусть* $f_v(a_v) \in L_1(G_v)$ *— непрерывные функции, принадлежащие пространствам* $\mathrm{Inv}(G_v)$ *соответственно (т. е.* $\hat{f}_v \in L_1(\hat{G}_v)$*). Предположим, кроме того, что* f_v *для почти всех* v *совпадает с характеристической функцией подгруппы* H_v*. Тогда функция*

$$f(a) = \prod f_v(a_v)$$

принадлежит пространству $\mathrm{Inv}(G)$*, и*

$$\hat{f}(\xi) = \prod \hat{f}_v(\xi_v).$$

Доказательство. Применяя теорему 8 к функции $f(a)\,\overline{c(a)} = \prod f_v(a_v)\,\overline{c_v(a_v)}$, получаем, что преобразование Фурье произведения локальных функций совпадает с произведением их преобразований Фурье. Поскольку $f_v \in \mathrm{Inv}(G_v)$, отсюда следует, что $\hat{f}_v \in \mathrm{Inv}(\hat{G}_v)$ при всех v. Для почти всех v функция $\hat{f}_v$ совпадает с характеристической функцией подгруппы $H_v^\perp$. Следовательно, $\hat{f} \in L_1(\hat{G})$ и, стало быть, $f \in \mathrm{Inv}(G)$.

Следствие. *Мера* $d\xi = \prod d\xi_v$ *двойственна к* $\prod da_v$.

§ 6. Глобальная аддитивная двойственность. Теорема Римана—Роха

Пусть k — числовое поле (конечное расширение поля рациональных чисел $\mathbf{Q}$). Его пополнение относительно нормирования v обозначается символом k_v, и все обозначения, относящиеся к локальным объектам в § 1—4, сохраняются с добавлением индекса v или $\mathfrak{p}$ в $\mathfrak{p}$-адическом случае: $\mathfrak{o}_v$, λ_v, $\mathfrak{D}_\mathfrak{p}$, $\| \ \|_v$, c_v и т. п.

Как мы уже отмечали, группа *аделей* поля k представляет собой локально компактную группу — ограниченное прямое произведение групп k_v^+ относительно компактных подгрупп $\mathfrak{o}_\mathfrak{p}$, определенных для неархимедовых нормирований. Символом

$$x = (\ldots, x_v, \ldots)$$

мы будем обозначать переменный элемент группы аделей $A_k = A$. Рассмотрим непрерывный гомоморфизм

$$\lambda(x) = \sum \lambda_0(x_v)$$

группы A в факторгруппу вещественных чисел $\bmod \mathbf{Z}$. Комбинация теоремы 7 с теорией локальной двойственности в нашем случае дает следующий результат.

Теорема 10. *Спаривание*

$$\langle x, y\rangle = \prod_v e^{2\pi i \lambda_v (x_v y_v)} = e^{2\pi i \lambda (xy)}$$

определяет изоморфизм группы аделей с двойственной к ней группой.

Наша следующая задача — доказать, что аддитивная группа поля k, вложенная в A диагонально:

$$\alpha \longrightarrow (\alpha, \alpha, \alpha, \ldots),$$

является своим собственным ортогональным дополнением. Мы будем часто писать k вместо k^+.

Теорема 11. *Аддитивная группа k совпадает со своим ортогональным дополнением относительно описанной двойственности.*

Доказательство. Сначала покажем, что группа k ортогональна самой себе. Это означает, что при $x \in k$ имеем $\sum \lambda_v(x) = 0$. Для поля рациональных чисел $k = \mathbf{Q}$ последняя формула проверяется немедленно (использовать разложение рационального числа в сумму дробей, знаменатели которых являются степенями простых чисел). Пусть теперь k — конечное расширение поля $\mathbf{Q}$, а Tr_v, соответственно Tr, означает оператор локального, соответственно глобального, следа. Тогда

$$\sum_v \lambda_v(x) = \sum_w \sum_{v \mid w} \lambda_w(\mathrm{Tr}_v(x)) = \sum_w \lambda_w(y),$$

где $y = \sum_{v \mid w} \mathrm{Tr}_v(x) = \mathrm{Tr}(x)$, а w пробегает все нормирования поля $\mathbf{Q}$. Этим наше утверждение сводится к случаю поля $\mathbf{Q}$, где оно уже проверено.

Таким образом, мы установили, что $k^\perp \supset k$. Так как факторгруппа A/k компактна, то группа $k^\perp$ дискретна. Поскольку факторгруппа $k^\perp/k$ одновременно дискретна и компактна, она должна быть конечна. Но $k^\perp$, очевидно, является векторным пространством над k. Следовательно, $k^\perp = k$, чем и завершается доказательство теоремы.

Предложение 6. *Пусть множество F_∞ определено как в условии теоремы* 3 *гл.* VI, § 2. *При нашем выборе меры объем F_∞ равен $d_k^{1/2}$.*

Доказательство. Несложный подсчет определителя. Напомним, что мера, соответствующая комплексным v, является удвоенной мерой Лебега.

Предложение 7. *Рассмотрим подмножество группы A_k*

$$F = \prod_{v \notin S_\infty} \mathfrak{o}_v \times F_\infty.$$

Его мера равна 1.

Доказательство. Это следует из того, что при нашем выборе мер dx_v мера подгруппы $\mathfrak{o}_v$ равна $(\mathbf{N}\mathfrak{D}_\mathfrak{p})^{-1/2}$ при $v = v_\mathfrak{p}$.

Теперь мы уже в состоянии применить двойственность теоремы 11 к теории интегрирования.

Нижеследующие рассуждения, по существу, относятся к любой локально компактной коммутативной группе с выделенной замкнутой подгруппой. Однако для сохранения обозначений, которые будут использоваться в приложениях, мы даем доказательство лишь в случае двойственной себе коммутативной группы A с заданной дискретной замкнутой подгруппой k, которая совпадает со своим ортогональным дополнением. Тогда интеграл от функции по k равен сумме ее значений по всем элементам k. Сходимость в этом случае, разумеется, означает абсолютную сходимость. Будем предполагать, кроме того, что мера на A двойственна самой себе.

Формула Пуассона. *Пусть f — непрерывная функция, принадлежащая пространству $L_1(A)$. Предположим, что сумма*

$$\sum_{\alpha \in k} |f(x+\alpha)|$$

равномерно сходится для всех x, принадлежащих некоторому компактному подмножеству группы A, и что сумма

$$\sum_{\alpha \in k} \hat{f}(\alpha)$$

сходится. Тогда

$$\sum_{\alpha \in k} \hat{f}(\alpha) = \sum_{\alpha \in k} f(\alpha).$$

Доказательство. На факторгруппе A/k введем такую меру db, чтобы имела место формула

$$\int_{A/k} \int_{k} f(\alpha+b)\, d\alpha\, db = \int_{A} f(a)\, da,$$

где $d\alpha$ соответствует суммированию по k, а da — данная мера на группе A.

Положим $g(x) = \int_k f(x+\alpha)\, d\alpha$. Мы утверждаем, что $\hat{g}(\alpha) = \hat{f}(\alpha)$ при всех $\alpha \in k$. В самом деле, обозначая символом $\langle , \rangle$ скалярное произведение элемента группы

и характера и учитывая, что

$$(A/k)^{\wedge} = k^{\perp} = k,$$

находим

$$\hat{g}(\beta) = \int\limits_{A/k} g(b)\,\overline{\langle b, \beta\rangle}\,db =$$

$$= \int\limits_{A/k}\int\limits_{k} f(b+\alpha)\,\overline{\langle b, \beta\rangle}\,d\alpha\,db =$$

$$= \int\limits_{A/k}\int\limits_{k} f(b+\alpha)\,\overline{\langle b+\alpha, \beta\rangle}\,d\alpha\,db,$$

так как $\langle \alpha, \beta\rangle = 1$, по предположению. Далее,

$$\hat{g}(\beta) = \int\limits_{A} f(a)\,\overline{\langle \alpha, \beta\rangle}\,da = \hat{f}(\beta).$$

Кроме того, мера на A двойственна самой себе. Следовательно, формулу обращения Фурье можно применить для вычисления значения $\hat{\hat{g}}$ в нуле. Утверждение теоремы немедленно следует из определения $\hat{\hat{g}}(0)$.

В классической теории формула Пуассона применяется к дискретной подгруппе $\mathbf{Z}$ группы вещественных чисел. Мы будем применять ее к группе аделей,

На самом деле нам понадобится формула Пуассона для мультипликативно сдвинутой функции f.

Теорема Римана—Роха. *Предположим, что функция $f(x)$ удовлетворяет следующим условиям:*

1. *$f(x)$ непрерывна и принадлежит пространству $L_1(A)$.*

2. *Ряд $\sum\limits_{a\in k} f(a(x+\alpha))$, где a — идель, x — адель, равномерно сходится, когда a, x меняются в некоторых компактных подмножествах групп иделей и аделей соответственно.*

3. *Ряд $\sum\limits_{a\in k} \hat{f}(a\alpha)$ сходится для всех иделей a. Тогда*

$$\frac{1}{\|\alpha\|}\sum_{a\in k}\hat{f}\left(\frac{\alpha}{a}\right) = \sum_{a\in k} f(a\alpha).$$

Доказательство. Функция $g(x)=f(ax)$ удовлетворяет условиям применимости формулы Пуассона: это вытекает из соотношения

$$\hat{g}(x)=\frac{1}{\|a\|}\hat{f}\left(\frac{x}{a}\right).$$

Отсюда очевидным образом следует наше утверждение.

§ 7. Глобальное функциональное уравнение

В мультипликативной теории мы рассматриваем группу иделей $J=J_k$ как ограниченное прямое произведение локальных мультипликативных групп k_v^* относительно подгрупп единиц U_v и применяем § 5. Квазихарактеры, интересующие нас, будут тривиальны для почти всех U_v, т. е. неразветвлены для почти всех v.

Нам будет удобно рассматривать J как некоторое прямое произведение (топологическое и алгебраическое). Вложим в J группу положительных вещественных чисел $\mathbf{R}^+$ с помощью отображения

$$t\to(t^{1/N},\ \ldots,\ t^{1/N},\ 1,\ 1,\ \ldots)$$

(компонента $t^{1/N}$ для каждого архимедова нормирования и 1 — для всех остальных). Это отображение сохраняет норму, так как

$$\sum_{v\in S_\infty} N_v=N=[k:\mathbf{Q}].$$

Очевидно, что

$$J\approx\mathbf{R}^+\times J^0,$$

т. е. всякий идель a можно единственным способом представить в виде произведения

$$a=tb,$$

где $t\in\mathbf{R}^+$ и $b\in J^0$, и это разложение непрерывно. На группе J^0 существует однозначно определенная мера d^*b, такая, что формально

$$d^*a=d^*b\times\frac{dt}{}$$

Введем одно ограничение на квазихарактеры, которыми мы будем пользоваться в дальнейшем. *Будем считать*, что они тривиальны на k^*. Тогда их можно рассматривать как квазихарактеры *группы классов иделей* $C_k = J_k/k^*$. Такие характеры называются *характерами Гекке*. Поскольку группа $J_k^0/k^* = C_k^0$ компактна, ограничение любого квазихарактера на нее является характером. Тем самым ситуация похожа на локальную (архимедову). Если квазихарактер c тривиален на C_k^0, то

$$c(a) = \|a\|^s,$$

где s — некоторое комплексное число, однозначно определенное квазихарактером. Для произвольного квазихарактера c существует единственное вещественное число σ, такое, что $|c(a)| = \|a\|^\sigma$. Оно называется вещественной частью квазихарактера c и обозначается символом $\mathrm{Re}(c)$. Для любого характера χ группы C_k произведение $\chi(a)\|a\|^s$ представляет собой квазихарактер, и обратно, любой квазихарактер можно представить в таком виде (характер χ, однако, определен не однозначно, а с точностью до множителя вида $\|a\|^{it}$).

Иногда удобно нормализовать характеры группы C_k, потребовав, чтобы они были тривиальны на подгруппе $\mathbf{R}^+$ (выше было определено ее каноническое вложение). Очевидно, это условие равносильно формуле

$$\sum_{v \in S_\infty} N_v \varphi_v(\chi) = 0.$$

Всякий квазихарактер c однозначно определяет так нормализованный характер, для которого $c(a) = \chi(a)\|a\|^s$.

Как и в локальной теории, положим $\hat{c}(a) = \|a\| c(a)^{-1}$, так что $\hat{c}(a) = \chi^{-1}(a)\|a\|^{1-s} = \bar{\chi}(a)\|a\|^{1-s}$ (при описанной нормализации).

Мы дополним конструкцию, предшествовавшую формулировке теоремы 6 гл. VI, § 3, вычислением меры.

Как прежде, фиксируем архимедово нормирование v_0 и полагаем $S'_\infty = S_\infty - v_0$, $r = r_1 + r_2 - 1$.

Пусть $\varepsilon_1, \ldots, \varepsilon_r$ — такие единицы, что векторы $l(\varepsilon_i)$ порождают всю решетку. Эти единицы называются *фундаментальными*. Они порождают группу единиц по

модулю подгруппы корней из единицы. Определитель

$$\det(\log \| \varepsilon_i \|_v),$$

в котором $i = 1, \ldots, r$, а $v \in S'_\infty$, с точностью до знака равен объему фундаментального параллелотопа P в евклидовом пространстве. Его абсолютная величина называется *регулятором* поля k и обозначается символом $R = R_k$. Через $d = d_k$ мы обозначаем абсолютную величину дискриминанта.

Предложение 8. *Мера множества* $l^{-1}(P)$ *равна*

$$\frac{2^{r_1}(2\pi)^{r_2}}{d_k^{1/2}} R$$

(*отображение* l *определено в доказательстве теоремы* 6 *гл.* VI, § 3).

Доказательство. Пусть Q — единичный куб в r-мерном пространстве. Так как l — гомоморфизм, имеем

$$\frac{\text{Мера } l^{-1}(P)}{\text{Мера } l^{-1}(Q)} = \frac{\text{Объем } P}{\text{Объем } Q} = R.$$

Поэтому достаточно вычислить меру $l^{-1}(Q)$; мы оставляем это в качестве нетрудного упражнения читателю (воспользоваться определением мультипликативной меры).

Предложение 9. *Мера фундаментальной области* E *для факторгруппы* J^0/k^* *равна*

$$\frac{2^{r_1}(2\pi)^{r_2} hR}{w d_k^{1/2}}$$

(*обозначения, как в теореме* 6 *гл.* VI, § 3).

Доказательство. Тривиальное следствие предложения 8.

Мы приближаемся к концу нашего путешествия. Для определения глобальной дзета-функции рассмотрим функции f на группе аделей, удовлетворяющие следующим условиям:

Л1. $f(x)$ и $\hat{f}(x)$ непрерывны и принадлежат $L_1(A)$, т. е. $f \in \mathrm{Inv}(A)$.

Л2. Суммы $\sum_{a\in k} f(a(x+\alpha))$ и $\sum_{a\in k} \hat{f}(a(x+\alpha))$ сходятся абсолютно и равномерно, когда a и x меняются в компактных подмножествах групп иделей и аделей соответственно.

Л3. Функции $f(a)\|a\|^{\sigma}$ и $\hat{f}(a)\|a\|^{\sigma}$ при $\sigma>1$ принадлежат пространству $L_1(J)$.

Отметим, что выполнение первых двух условий обеспечивает применимость теоремы Римана — Роха к функциям такого типа. Третье условие необходимо нам для определения дзета-функции. Каждой функции f соответствует дзета-функция на множестве квазихарактеров c с $\mathrm{Re}(c)>1$,

$$\zeta(f, c)=\int f(a)\, c(a)\, d^*a,$$

где интеграл берется по группе иделей. Пусть $c(a)=\chi(a)\|a\|^s$, тогда

$$\zeta(f, \chi, s)=\int f(a)\,\chi(a)\,\|a\|^s\, d^*a.$$

(Мы все время предполагаем, что рассматриваемые квазихарактеры и характеры тривиальны на k^*.) Когда характер χ фиксирован, дзета-функция становится функцией одного параметра s; из условия Л3 следует, что она голоморфна в области $\mathrm{Re}(c)>1$.

Теорема 12. *Всякую дзета-функцию можно аналитически продолжить на область всех квазихарактеров группы J/k^*. Продолженная функция однозначна и голоморфна всюду, кроме $c(a)=1$ и $c(a)=\|a\|$, где она имеет простые полюсы с вычетами $-\varkappa f(0)$ и $+\varkappa\hat{f}(0)$ соответственно; здесь $\varkappa$ — объем фундаментальной области для $J_k^0 \bmod k^*$. Кроме того, имеет место функциональное уравнение*

$$\zeta(f, c)=\zeta(\hat{f}, \hat{c}),$$

где $\hat{c}(a)=\|a\|\, c^{-1}(a)$.

Доказательство. Имеем

$$\zeta(f, c)=\int\limits_{\|a\|\leqslant 1} f(a)\, c(a)\, d^*a+\int\limits_{\|a\|\geqslant 1} f(a)\, c(a)\, d^*a.$$

Второй интеграл, очевидно, сходится для любого вещественного значения $\mathrm{Re}(c)$, потому что он сходится при $\mathrm{Re}(c) > \sigma_0$, где σ_0 — некоторое число, и тем более сходится при $\mathrm{Re}(c) \leqslant \sigma_0$. Займемся преобразованием первого интеграла; докажем следующий результат.

Теорема 13. *Пусть при* $t \in \mathbf{R}^+$ *имеем* $c(t) = t^s$, *и пусть* χ *— характер группы* J^0, *индуцированный квазихарактером* c. *Тогда*

$$\zeta(f, c) = \int\limits_{\|a\| \geqslant 1} f(a)\, c(a)\, d^*a + \int\limits_{\|a\| \geqslant 1} \hat{f}(a)\, \hat{c}(a)\, d^*a + \delta_\chi \left[\frac{\varkappa \hat{f}(0)}{s-1} - \frac{\varkappa f(0)}{s} \right],$$

где $\delta_\chi = 0$ *или* 1 *в зависимости от того, тривиален или нет характер* χ, *индуцированный квазихарактером* c *на подгруппе* J^0. *Оба интеграла сходятся при всех* c *равномерно в каждой полосе* $\sigma_0 \leqslant \mathrm{Re}(c) \leqslant \sigma_1$.

Равномерная сходимость интегралов в полосе очевидна из сделанных выше замечаний. Далее, покажем, как из этой формулы следует функциональное уравнение. Заменим (f, c) на $(\hat{f}, \hat{c})$ в выражении справа. Учтем, что $\hat{\hat{f}}(0) = f(-0) = f(0)$ и $\hat{\hat{f}}(a) = f(-a)$. Замена переменной во втором интеграле выделяет множитель $c(-1)$, но c тривиален на k^*. Следовательно, замена (f, c) на $(\hat{f}, \hat{c})$ не меняет выражения справа — это и есть функциональное уравнение.

Остается преобразовать интеграл по $\|a\| \leqslant 1$ так, чтобы получить требуемое выражение. Запишем группу иделей в качестве произведения:

$$J = J^0 \times \mathbf{R}^+.$$

Будем, кроме того, считать характер нормализованным так, чтобы $c(t) = t^s$. Для всякого фиксированного значения t имеем

$$\int\limits_{J^0} f(tb)\, c(tb)\, d^*b + f(0) \int\limits_E c(tb)\, d^*b = \sum_{a \in k^*} \int\limits_{aE} f(tb)\, c(tb)\, d^*b + f(0) \int\limits_E c(tb)\, d^*b.$$

Пользуясь инвариантностью меры относительно мультипликативных сдвигов и тем, что $c(\alpha)=1$ при $\alpha \in k^*$, преобразуем это выражение так:

$$\sum_{\alpha \in k^*} \int_E f(\alpha t b)\, c(tb)\, d^*b + f(0) \int_E c(tb)\, d^*b.$$

Свойство Л2 позволяет менять местами суммирование и интегрирование; пользуясь затем теоремой Римана—Роха, находим

$$\int_E \sum_{\alpha \in k} f(\alpha t b)\, c(tb)\, d^*b = \int_E \sum_{\alpha \in k} \hat{f}\left(\frac{\alpha}{tb}\right) \frac{1}{\| tb \|} \hat{c}(tb)\, d^*b.$$

Если бы мы начали с выражения

$$\int_{J^0} \hat{f}(t^{-1}b)\, \hat{c}(t^{-1}b)\, d^*b + f(0) \int_E \hat{c}(t^{-1}b)\, d^*b,$$

сделали замену переменной $b \to b^{-1}$, сохраняющую меру, и затем произвели те же преобразования, что и выше, в результате получилось бы то же самое выражение. Иначе говоря, имеет место тождество

$$\int_{J^0} f(tb)\, c(tb)\, d^*b + f(0) \int_E c(tb)\, d^*b =$$

$$= \int_{J^0} f(t^{-1}b)\, c(t^{-1}b)\, d^*b + f(0) \int_E c(t^{-1}b)\, d^*b.$$

Заметим теперь, что $c(tb) = c(t)\, c(b) = t^s c(b)$, откуда

$$\int_E c(tb)\, d^*b = \begin{cases} \varkappa t^s, & \text{если } c(a) = \| a \|^s, \\ 0, & \text{если } c \text{ нетривиален на } J^0. \end{cases}$$

(Мы снова пользуемся тем, что интеграл по компактной группе от нетривиального характера равен нулю, а от тривиального характера — мере группы.)

Теперь следует проинтегрировать наше тождество по t от 0 до 1 и заменить справа t^{-1} на t, а пределы интегрирования — на $(1, \infty)$. Это даст формулу теоремы 13, чем и заканчивается доказательство.

§ 8. Глобальные вычисления

Цель этого параграфа — вывести некоторые явные формулы для глобальных дзета-функций, полезные в приложениях. В качестве весовой функции мы будем использовать некоторую функцию g_χ, тесно связанную с функцией f_χ. Обе они являются произведениями локальных функций; доказательство сходимости этого произведения при $\sigma > 1$ будет дано в следующей главе. Мы должны подчеркнуть, что, несмотря на его простоту (это — классический результат), оно представляет собой последний шаг в установлении того, что теорема 12 непуста и применима к классическим дзета-функциям и L-функциям.

Предложение 10. *Пусть* $g(x) = f(bx)$; *тогда*

$$\hat{g}(y) = \|b\|^{-1} \hat{f}(y/b), \quad \zeta(g, c) = c(b)^{-1} \zeta(f, c).$$

Доказательство. Непосредственное следствие определений.

Этот результат имеет место и в локальном, и в глобальном случае, т. е. для групп k_v^* и J_k. Разумеется, в локальной группе $\| \ \| = \| \ \|_v$; а b означает либо элемент группы k_v^*, либо идель.

Введем некоторые обозначения. Для всякого характера χ положим

$$\mathfrak{D}_\chi = \mathfrak{D}\mathfrak{f}_\chi, \qquad d_\chi = \mathbf{N}\mathfrak{D}_\chi.$$

Если $\chi = \chi_0$, то $d_0 = d_k$ совпадает с абсолютной величиной дискриминанта числового поля k. Подобные же обозначения используются в локальном случае (с добавлением индекса $\mathfrak{p}$).

Пусть v *— архимедово нормирование*, $N = [k : \mathbf{Q}]$. Положим

$$g_{\chi, v}(x) = f_{\chi, v}(d_\chi^{1/2N} x)\,(N_v \pi)^{|m_v(\chi)|/2},$$

где $f_{\chi, v}$ — функция, определенная в § 4.

Пусть v *— $\mathfrak{p}$-адическое нормирование*. Положим

$$g_{\chi, v}(x) = \frac{1}{\mu_v(1 + \mathfrak{f}_{\chi, v})} f_{\chi, v}(x).$$

Как обычно, подразумевается, что для неразветвленных характеров $\mathfrak{f}_{\chi, v} = \mathfrak{o}_v$ и $1 + \mathfrak{f}_{\chi, v} = \mathfrak{o}_v$, так что мера этого множества равна $d_{\mathfrak{p}}^{-1/2}$. Далее,

$$g_\chi(x) = \prod g_{\chi, v}(x_v).$$

В частности, если $\chi = \chi_0$, то для архимедовых v имеем

$$g_{0, v}(x) = f_{0, v}(d_k^{1/2N} x),$$

а для $\mathfrak{p}$-адических—

$$g_{0, v}(x) = d_{\mathfrak{p}}^{1/2} f_{0, v}(x),$$

где $d_{\mathfrak{p}} = \mathbf{N}\mathfrak{D}_{\mathfrak{p}}$.

Заметим, что функция g_χ получается из f_χ с помощью сдвига (для архимедовых v) и умножения на константу, цель которого—устранить некоторые лишние множители в выражениях для дзета-функций от f_χ и $\hat{f}_\chi$.

Начнем со следующего замечания.

Предложение 11. *Пусть $\chi = \chi_0$—тривиальный характер. Тогда функции g_0 и $\hat{g}_0$ неотрицательны, и*

$$g_v(0) = \hat{g}_0(0) = d_k^{1/2} (2\pi)^{-r_2}.$$

Доказательство. Непосредственно следует из определений.

Предложение 12. *Пусть b—идель, компоненты которого относительно архимедовых v равны $b_v = d_k^{1/N}$, а для неархимедовых $b_{\mathfrak{p}} = \pi^{-\nu_{\mathfrak{p}}}$, где $\nu_{\mathfrak{p}} = \mathrm{ord}_{\mathfrak{p}}\mathfrak{D}$. Тогда $\|b\| = 1$ и*

$$\hat{g}_0(x) = g_0(bx).$$

Доказательство. Легко следует из предложения 10 и явного выражения g_0 через f_0.

Пусть χ—характер группы C_k, $\mathfrak{p}$—простой идеал, неразветвленный относительно χ. Тогда значение χ на иделе, имеющем в качестве $\mathfrak{p}$-компоненты простой элемент π, а в качестве остальных компонент—1, не зависит от выбора π. Пусть $\chi(\mathfrak{p})$—это значение, и пусть S_χ—мно-

жество всех $\mathfrak{p}$, разветвленных относительно χ. Положим

$$L(s, \chi) = \prod_{\mathfrak{p} \notin S_\chi} \frac{1}{1 - \frac{\chi(\mathfrak{p})}{N\mathfrak{p}^s}}.$$

Далее, пусть

$$\Lambda(s, \chi) = (2^{r_1}(2\pi)^{-N} d_\chi)^{s/2} \prod_{v \in S_\infty} \Gamma(s_v/2)\, L(s, \chi);$$

напомним, что

$$s_v = s_v(\chi) = N_v(s + i\varphi_v(\chi)) + |m_v(\chi)|.$$

Теорема 14. *Пусть характер χ нормализован так, что*

$$\sum_{v \in S_\infty} N_v \varphi_v(\chi) = 0.$$

Тогда

$$\zeta(g_\chi, \chi, s) = \Lambda(s, \chi) \prod_{\mathfrak{p} \in S_\chi} \tau_{\mathfrak{p}}(\chi) \prod_{\mathfrak{p} \notin S_\chi} \chi(\mathfrak{D}_{\mathfrak{p}}^{-1})\, 2^{-i\Phi},$$

где Φ — сумма чисел $\varphi_v(\chi)$ по всем комплексным v. Кроме того,

$$\zeta(\hat{g}_\chi, \bar{\chi}, 1-s) = \Lambda(1-s, \bar{\chi})\, (N\mathfrak{f}_\chi)^{1/2}\, i^M 2^{i\Phi},$$

где $M = \sum_{v \in S_\infty} |m_v(\chi)|$; эти выражения совпадают.

Доказательство. Следует собрать воедино локальные результаты из § 4, учесть предложение 10 и произвести необходимые сокращения.

Если заменить g_χ на $(N\mathfrak{f}_\chi)^{1/2}$, то функция $\Lambda(s, \chi)$ и дзета-функция будут отличаться от теперешних на множитель, равный 1 по абсолютной величине; то же относится к $\Lambda(1-s, \bar{\chi})$.

Следствие 1. *Имеет место функциональное уравнение вида*

$$W(\chi)\Lambda(s, \chi) = \Lambda(1-s, \bar{\chi}),$$

где $W(\chi)$ — константа, по абсолютной величине равная 1:

$$W(\chi) = 4^{-i\Phi} i^{-M} (N\mathfrak{f}_\chi)^{-1/2} \prod_{\mathfrak{p} \in S_\chi} \tau_{\mathfrak{p}}(\chi) \prod_{\mathfrak{p} \notin S_\chi} \chi(\mathfrak{D}_{\mathfrak{p}}^{-1}).$$

Доказательство. Из локальных результатов § 4 известно, что число $\tau_p(\chi)$ по абсолютной величине равно $(Nf_{\chi,p})^{1/2}$; учитывая это, нужно произвести сокращения в равенстве

$$\zeta(g\chi, \chi, s) = \zeta(\hat{g}\chi, \bar{\chi}, 1-s).$$

Следствие 2. *Пусть χ — фиксированный характер. Положим $\Lambda(s) = \Lambda(s, \bar{\chi})$. Тогда*

$$\Lambda(\bar{s}) = \overline{\Lambda(1-s)}\, u(\chi),$$

где число $u(\chi)$ по абсолютной величине равно 1.

Доказательство. Тривиальный подсчет с использованием тождества

$$\Lambda(\bar{s}, \chi) = \overline{\Lambda(s, \bar{\chi})}.$$

Следствие 3. *Положим $\Lambda_0(s) = \Lambda_k^r(s, \chi_0)$. Тогда*

$$\Lambda_0(s) = \zeta(g_0, \chi_0, s) = (2^{-2r_2}\pi^{-N}d_k)^{s/2}\Gamma^{r_1}(s/2)\,\Gamma^{r_2}(s)\,\zeta_k(s)$$

и

$$\Lambda_0(s) = \Lambda_0(1-s).$$

Предложение 13. *Пусть*

$$\varkappa = \frac{2^{r_1}(2\pi)^{r_2}hR}{wd_k^{1/2}}$$

— объем фундаментальной области группы $J_k^0 \bmod k^*$. Вычет функции $\zeta(g_0, s) = \zeta(g_0, \chi_0, s)$ в точке $s=1$ равен $d_k^{1/2}(2\pi)^{-r_2}\varkappa$, а вычет функции $\zeta_k(s)$ в этой точке равен $\varkappa$.

Доказательство. Значение вычета функции $\zeta(g_0, \chi_0, s)$ получается из теоремы 12, а дзета-функции — из следствия 3, в котором нужно положить $\Gamma(1/2) = \pi^{1/2}$ и учесть, что $\Gamma(1) = 1$.

Теорема 15. *Дзета-функцию можно представить в виде интеграла*

$$\zeta(g_0, s) = \int\limits_{\|a\| \geqslant 1} \hat{g}_0(a)\,(\|a\|^s + \|a\|^{1-s})\,d^*a + \frac{\varkappa g_0(0)}{s(s-1)}.$$

Доказательство. Достаточно подставить в интегральное выражение теоремы 13, § 7, формулу предложения 10, учесть, что $\|b\| = 1$, и воспользоваться инвариантностью мультипликативной меры относительно мультипликативного сдвига.

Мы используем эту формулу в доказательстве теоремы Брауэра — Зигеля, отметив, что при вещественных s интегральный член неотрицателен, так как $\hat{g}_0 \geqslant 0$.

Глава VIII

ПЛОТНОСТЬ ПРОСТЫХ ИДЕАЛОВ И ТАУБЕРОВА ТЕОРЕМА

В этой главе мы докажем тауберову теорему Икеара (см. также книгу Уиддера о преобразовании Лапласа) и теорему о плотности простых идеалов в обобщенных арифметических прогрессиях, соответствующих характерам Гекке. Тауберова теорема дает не только плотности простых идеалов в данных классах, но также плотности простых идеалов, определенным образом распределенных в N-мерном евклидовом пространстве.

Как заметит читатель, из тауберовой теоремы вытекает результат об асимптотическом поведении коэффициентов ряда Дирихле, который имеет простой полюс, скажем в точке $d > 1$ (где d — целое число), и голоморфен в остальных точках с $\mathrm{Re}\,(s) \geqslant d$. Если вычет в точке d равен 1, то сдвиг аргумента приводит к оценке сумм типа

$$\sum_{n<x} n^d a_n.$$

Суммирование или интегрирование по частям показывает, что из асимптотики $\sum_{n<x} a_n \sim x$ следует $\sum_{n<x} n^d a_n \sim x^{d+1}/(d+1)$. Этот результат можно применить к дзета-функции многообразия, заданного над кольцом целых алгебраических чисел числового поля. Редуцируя $\bmod \mathfrak{p}$ по почти всем $\mathfrak{p}$ и применяя оценки Ленга — Вейля (Number of points of varieties in finite fields, *Amer. J. Math.* (1954), 819—827), можно убедиться, что дзета-функция аналитична при $\mathrm{Re}\,(s) \geqslant d$, где d — размерность рассматриваемого многообразия, и потому можно применить тауберову теорему.

§ 1. Интеграл Дирихле

Пусть $\varphi(x)$ — вещественная функция с ограниченной вариацией на всяком конечном подинтервале полупрямой $0 \leqslant x < \infty$. Класс функций

$$f(s) = \int_0^\infty e^{-sx}\, d\varphi(x) \qquad (s = \sigma + it) \tag{1}$$

содержит, в частности, ряды Дирихле, если в качестве $\varphi(x)$ выбрать подходящую ступенчатую функцию. Мы займемся этим позже; пока будем работать с интегралом.

Предположим, что для некоторого фиксированного значения s_0 функция

$$g(y) = \int_0^y e^{-s_0 x}\, d\varphi(x)$$

ограничена на полупрямой $0 \leqslant y < \infty$. Пусть $0 \leqslant y_1 < y_2$. Имеем

$$\int_{y_1}^{y_2} e^{-sx}\, d\varphi(x) = \int_{y_1}^{y_2} e^{-(s-s_0)x} e^{-s_0 x}\, d\varphi(x) =$$

$$= e^{-(s-s_0)x} g(x)\Big|_{y_1}^{y_2} + (s - s_0) \int_{y_1}^{y_2} e^{-(s-s_0)x} g(x)\, dx.$$

Очевидно, что когда $\operatorname{Re}(s - s_0) \geqslant \varepsilon > 0$ и когда значения $\frac{|s - s_0|}{\sigma - \sigma_0}$ ограничены, левая часть при больших y_1 равномерно мала. Поэтому интеграл (1) сходится для этих значений s.

Поскольку предположение о сходимости $g(y)$ выполняется, если в качестве s_0 взять точку сходимости интеграла (1), отсюда вытекает, что (1) сходится в полуплоскости справа от некоторой вертикальной прямой, и притом равномерно в любом компактном подмножестве этой полуплоскости. Поскольку функции $\int_0^y e^{-sx}\, d\varphi(x)$ аналитичны, интеграл (1) аналитичен внутри полуплоскости.

Предположим теперь, что $\varphi(x) \geqslant 0$ и что интеграл (1) сходится для некоторого вещественного числа $s_0 > 0$. Интегрируя дифференциал $d(e^{-sx}\varphi(x))$, получаем

$$(2)\quad \int_0^{\xi} e^{-sx}\, d\varphi(x) = -\varphi(0) + e^{-s\xi}\varphi(\xi) + s\int_0^{\xi} e^{-sx}\varphi(x)\,dx =$$

$$= -\varphi(0) + e^{-(s-s_0)\xi}e^{-s_0\xi}\varphi(\xi) + s\int_0^{\xi} e^{-(s-s_0)x}e^{-s_0x}\varphi(x)\,d_x.$$

Положив в первой строке $s = s_0$, мы убедимся, что наш интеграл ограничен и что два последних слагаемых справа неотрицательны. Тем самым функция $e^{-s_0\xi}\varphi(\xi)$ ограничена по ξ. Отсюда вытекает, что при $\operatorname{Re}(s) > s_0$

$$(3)\qquad f(s) = -\varphi(0) + s\int_0^{\infty} e^{-sx}\varphi(x)\,dx$$

(утверждение о существовании интеграла справа, конечно, подразумевается).

§ 2. Тауберова теорема Икеара

В этом параграфе мы предполагаем, что $\varphi(x)$ — монотонно возрастающая функция и $\varphi(x) = 0$ при $x \leqslant 0$. Положим

$$H(x) = e^{-x}\varphi(x).$$

Монотонность φ означает, что

$$H(x_2) \geqslant H(x_1)\, e^{x_1 - x_2} \qquad \text{при} \qquad x_2 \geqslant x_1.$$

Для заданного $\lambda > 0$ рассмотрим класс монотонно возрастающих функций $\varphi(x)$, $\varphi(x) = 0$ при $x \leqslant 0$, обладающих следующими свойствами:

1. Интеграл (1) сходится при $\operatorname{Re}(s) > 1$.
2. Для всякого $\varepsilon > 0$, $s = 1 + \varepsilon + it$, положим

$$h_\varepsilon(t) = f(s) - \frac{1}{s-1}.$$

Мы требуем, чтобы предел $h(t) = \lim\limits_{\varepsilon \to 0} h_\varepsilon(t)$ существовал равномерно по t на отрезке $|t| \leqslant 2\lambda$ (следовательно, функция $h(t)$ непрерывна на этом отрезке).

Тауберова теорема *устанавливает существование таких двух функций* $P_1(\lambda)$ *и* $P_2(\lambda)$ *от переменной* λ, *что для любой функции* φ *из рассматриваемого класса имеют место неравенства*

$$P_1(\lambda) \geqslant \overline{\lim_{y\to\infty}} H(y) \geqslant \underline{\lim_{y\to\infty}} H(y) \geqslant P_2(\lambda) > 0$$

и, кроме того,

$$\lim_{\lambda\to\infty} P_1(\lambda) = \lim_{\lambda\to\infty} P_2(\lambda) = 1.$$

Если известно, что функция $\varphi(x)$ *принадлежит описанному классу для всех* λ, *то*

$$\lim_{x\to\infty} e^{-x}\varphi(x) = 1.$$

Именно эту формулу мы используем в приложениях.

Докажем тауберову теорему. Число π, по определению, равно

$$\pi = \int_{-\infty}^{+\infty} \frac{\sin^2 v}{v^2}\, dv > 0$$

(что совпадает с обычным значением π).

Лемма. *В сформулированных предположениях имеем*

$$\lim_{y\to\infty} \int_{-\infty}^{\lambda_y} H\left(y - \frac{v}{\lambda}\right) \frac{\sin^2 v}{v^2}\, dv = \pi.$$

Доказательство. Полагая $s = 1 + \varepsilon + it$ и используя формулу (3), находим

$$\frac{h_\varepsilon(t)-1}{s} = \frac{1}{s}\left(f(s) - \frac{1}{s-1} - 1\right) =$$

$$= \int_0^\infty e^{-(s-1)x} H(x)\, dx - \frac{1}{s-1} = \int_0^\infty (H(x)-1)\, e^{-\varepsilon x - itx}\, dx,$$

учитывая, что $\int_0^\infty e^{-(s-1)x}\, dx = 1/(s-1)$. Тем самым

$$\frac{h_\varepsilon(t)-1}{s} = \lim_{\xi\to\infty} \int_0^\xi (H(x)-1)\, e^{-\varepsilon x - itx}\, dx$$

равномерно на отрезке $|t| \leqslant 2\lambda$ при фиксированном ε.

Наша следующая цель — вывести формулу (6) (см. ниже). Умножим последнее соотношение на функцию $e^{ity}(1-|t|/2\lambda)$ и проинтегрируем по t от -2λ до 2λ. Справа мы можем поменять местами интегрирование и предельный переход. Полагая

$$F_\varepsilon(t)=\left(1-\frac{|t|}{2\lambda}\right)\frac{h_\varepsilon(t)-1}{s},$$

находим

$$\int_{-2\lambda}^{2\lambda} e^{ity}F_\varepsilon(t)\,dt=$$

$$=\lim_{\xi\to\infty}\int_{-2\lambda}^{2\lambda} e^{ity}\left(1-\frac{|t|}{2\lambda}\right)\left[\int_0^\xi (H(x)-1)e^{-\varepsilon x-itx}\,dx\right]dt.$$

Интегрирования (оба по конечным отрезкам) можно переставить. Это дает

$$(4)\qquad \int_{-2\lambda}^{2\lambda} e^{ity}F_\varepsilon(t)\,dt=$$

$$=\int_0^{2\lambda}(H(x)-1)\,e^{-\varepsilon x}\left[\int_{-2\lambda}^{2\lambda}\left(1-\frac{|t|}{2\lambda}\right)e^{i(y-x)t}\,dt\right]dx.$$

Внутренний интеграл справа берется в элементарных функциях. Имеем

$$\int_{-2\lambda}^{2\lambda}\left(1-\frac{|t|}{2\lambda}\right)e^{i(y-x)t}\,dt=2\int_0^{2\lambda}\left(1-\frac{|t|}{2\lambda}\right)\cos((y-x)t)\,dt.$$

Замена переменных и интегрирование по частям дает

$$2\,\frac{\sin^2(\lambda(y-x))}{\lambda(y-x)^2}.$$

Тем самым интеграл (4) равен

$$(5)\qquad \int_{-2\lambda}^{2\lambda} e^{ity}F_\varepsilon(t)\,dt=2\int_0^\infty (H(x)-1)\,e^{-\varepsilon x}\,\frac{\sin^2(\lambda(y-x))}{\lambda(y-x)^2}\,dx.$$

Интеграл $\int_0^\infty e^{-\varepsilon x}\frac{\sin^2(\lambda(y-x))}{\lambda(y-x)^2}\,dx$ существует, потому что он определен уже при $\varepsilon=0$. Прибавляя его к обеим частям равенства (5), находим

$$(6)\quad \int_{-2\lambda}^{2\lambda} e^{ity}F_\varepsilon(t)\,dt+2\int_0^\infty e^{-\varepsilon x}\frac{\sin^2(\lambda(y-x))}{\lambda(y-x)^2}\,dx=$$

$$=2\int_0^\infty H(x)\,e^{-\varepsilon x}\frac{\sin^2(\lambda(y-x))}{\lambda(y-x)^2}\,dx.$$

Теперь перейдем к пределу при $\varepsilon\to 0$. Что происходит с левой частью при $\varepsilon\to 0$?

Первый интеграл сходится к

$$\int_{-2\lambda}^{2\lambda} e^{ity}F(t)\,dt,$$

где $F(t)$ — непрерывная функция $\left(1-\frac{|t|}{2\lambda}\right)\frac{h(t)-1}{s}$, ибо сходимость $h_\varepsilon(t)\to h(t)$ равномерна.

Остаточный член второго интеграла оценивается величиной

$$\int_\xi^\infty e^{-\varepsilon x}\frac{\sin^2\lambda(y-x)}{\lambda(y-x)^2}\,dx\leqslant\int_\xi^\infty\frac{\sin^2\lambda(y-x)}{\lambda(y-x)^2}\,dx,$$

которая мала при больших ξ равномерно по ε. Далее, при $\varepsilon\to 0$

$$\int_0^\xi e^{-\varepsilon x}\frac{\sin^2\lambda(y-x)}{\lambda(y-x)^2}\,dx\to\int_0^\xi\frac{\sin^2\lambda(y-x)}{\lambda(y-x)^2}\,dx.$$

Следовательно, предел второго интеграла равен

$$\int_0^\infty\frac{\sin^2\lambda(y-x)}{\lambda(y-x)^2}\,dx=\int_{-\infty}^{\lambda y}\frac{\sin^2 v}{v^2}\,dv.$$

Что происходит с правой частью формулы (6)? Мы доказали, что ее предел при $\varepsilon\to 0$ существует. Подинтеграль-

ная функция положительна и возрастает при $\varepsilon \to 0$. Поэтому интеграл

$$\int_0^{\xi} H(x)\, e^{-\varepsilon x} \frac{\sin^2 \lambda (y-x)}{\lambda (y-x)^2}\, dx$$

меньше этого предела при всех $\varepsilon > 0$. Значит, и интеграл

$$\int_0^{\xi} H(x) \frac{\sin^2 \lambda (y-x)}{\lambda (y-x)^2}\, dx$$

не больше предела. Следовательно,

$$\int_0^{\infty} H(x) \frac{\sin^2 \lambda (y-x)}{\lambda (y-x)^2}\, dx$$

существует. Его остаточный член мал, но больше остаточного члена интеграла в правой части равенства (6). Следовательно, предел правой части равен

$$\int_0^{\infty} H(x) \frac{\sin^2 \lambda (y-x)}{\lambda (y-x)^2}\, dx = \int_{-\infty}^{\lambda y} H\left(y - \frac{v}{\lambda}\right) \frac{\sin^2 v}{v^2}\, dv.$$

Следовательно,

$$(7) \qquad \int_{-2\lambda}^{2\lambda} e^{ity} F(t)\, dt + 2 \int_{-\infty}^{\lambda y} \frac{\sin^2 v}{v^2}\, dv = 2 \int_{-\infty}^{\lambda_y} H\left(y - \frac{v}{\lambda}\right) \frac{\sin^2 v}{v^2}\, dv.$$

Что происходит с этим равенством, когда $y \to \infty$? Первый интеграл слева является коэффициентом Фурье непрерывной функции $F(t)$ и, следовательно, стремится к нулю по лемме Римана — Лебега. Второй интеграл слева стремится к π. Это доказывает лемму.

Теперь мы применим ее. Заметим, что при $v > \lambda y$ имеем $H\left(y - \frac{v}{\lambda}\right) = 0$, так что

$$\lim_{y \to \infty} \int_{-\infty}^{+\infty} H\left(y - \frac{v}{\lambda}\right) \frac{\sin^2 v}{v^2}\, dv = \pi.$$

Начиная с этого места, доказательство становится формальным. Идея вывода обоих неравенств состоит в рассмотрении интеграла в конечных пределах, зависящих от λ.

Отметим, что подинтегральная функция неотрицательна. Уменьшая область интегрирования, получаем

$$\overline{\lim_{y\to\infty}} \int_{-\sqrt{\lambda}}^{\sqrt{\lambda}} H\left(y-\frac{v}{\lambda}\right)\frac{\sin^2 v}{v^2}\,dv \leqslant \pi.$$

Пользуясь монотонностью функции φ и соответствующим неравенством для H, находим, что в интервале $\left[-\sqrt{\lambda}, \sqrt{\lambda}\right]$

$$H\left(y-\frac{v}{\lambda}\right) \geqslant H\left(y-\frac{1}{\sqrt{\lambda}}\right)e^{-2/\sqrt{\lambda}}.$$

Тем самым

$$\overline{\lim_{y\to\infty}} H\left(y-\frac{1}{\sqrt{\lambda}}\right)e^{-2/\sqrt{\lambda}} \int_{-\sqrt{\lambda}}^{\sqrt{\lambda}} \frac{\sin^2 v}{v^2}\,dv \leqslant \pi.$$

Поскольку λ фиксировано, можно заменить y на $y+1/\sqrt{\lambda}$. Поэтому

$$\overline{\lim_{y\to\infty}} H(y) \leqslant \frac{\pi e^{2/\sqrt{\lambda}}}{\int_{-\sqrt{\lambda}}^{\sqrt{\lambda}} \frac{\sin^2 v}{v^2}\,dv} = P_1(\lambda)$$

и $\lim\limits_{\lambda\to\infty} P_1(\lambda) = 1$. Первая половина тауберовой теоремы доказана.

Из нее уже следует, что функция $H(y)$ ограничена. Поэтому

$$\int_{\sqrt{y}}^{\infty} H\left(y-\frac{v}{\lambda}\right)\frac{\sin^2 v}{v^2}\,dv \leqslant C\int_{\sqrt{y}}^{\infty}\frac{\sin^2 v}{v^2}\,dv,$$

и этот интеграл стремится к нулю, когда $y\to\infty$. Тем самым

$$\lim_{y\to\infty}\int_{-\infty}^{\sqrt{y}} H\left(y-\frac{v}{\lambda}\right)\frac{\sin^2 v}{v^2}\,dv = \pi. \tag{8}$$

(Мы берем в качестве предела интегрирования $\sqrt{y}$ так, чтобы $y-\sqrt{y}\to\infty$ при $y\to\infty$.) Если число y достаточно велико, то $H(y)<2P_1(\lambda)$. Поэтому $H\left(y-\frac{v}{\lambda}\right)$ в формуле (8) оценивается сверху величиной $2P_1(\lambda)$ при достаточно больших y.

Положим теперь

$$b=\frac{4}{\pi}P_1(\lambda)+\sqrt{\lambda}$$

и заменим область интегрирования в соотношении (8) при больших y на $(-b,\ b)$. Остаточными членами будут

$$\int_{-\infty}^{-b} H\left(y-\frac{v}{\lambda}\right)\frac{\sin^2 v}{v^2}\,dv\leqslant 2P_1(\lambda)\int_{-\infty}^{-b}\frac{1}{v^2}\,dv=\frac{2P_1(\lambda)}{b}$$

и

$$\int_{b}^{\sqrt{y}} H\left(y-\frac{v}{\lambda}\right)\frac{\sin^2 v}{v^2}\,dv\leqslant 2P_1(\lambda)\int_{b}^{\sqrt{y}}\frac{1}{v^2}\,dv\leqslant\frac{2P_1(\lambda)}{b}.$$

Поэтому

$$\frac{4P_1(\lambda)}{b}+\lim_{y\to\infty}\int_{-b}^{b} H\left(y-\frac{v}{\lambda}\right)\frac{\sin^2 v}{v^2}\,dv\geqslant\pi.$$

Снова из монотонности получаем, что на этом интервале

$$H\left(y+\frac{b}{\lambda}\right)e^{2b/\lambda}\geqslant H\left(y-\frac{v}{\lambda}\right).$$

Тем самым

$$\frac{4P_1(\lambda)}{b}+\lim_{y\to\infty} H\left(y+\frac{b}{\lambda}\right)e^{2b/\lambda}\int_{-b}^{b}\frac{\sin^2 v}{v^2}\,dv\geqslant\pi.$$

Заменяя y на $y-b/\lambda$, а интеграл — числом π, имеем

$$\lim_{y\to\infty} H(y)\geqslant e^{-2b/\lambda}\left(1-\frac{4P_1(\lambda)}{\pi b}\right)=P_2(\lambda).$$

Очевидно, что $\lim\limits_{\lambda\to\infty}P_2(\lambda)=1$. Тауберова теорема доказана.

§ 3. Тауберова теорема для рядов Дирихле

Пусть $f(s)=\sum_{n=1}^{\infty} a_n/n^s=\sum a_n e^{-s\log n}$ — ряд Дирихле с вещественными неотрицательными коэффициентами a_n, который сходится при $\mathrm{Re}\,(s)>1$ и регулярен на прямой $\mathrm{Re}\,(s)=1$, за исключением точки $s=1$, где он имеет полюс первого порядка с вычетом 1.

В интегральном представлении этого ряда $\varphi(x)$ является ступенчатой функцией, которая в нуле равна 0, а в точках $x=\log n$ скачком увеличивается на a_n. Тем самым

$$\varphi(x)=\sum_{\log n<x} a_n.$$

Обозначая символом $\Phi(x)$ функцию $\Phi(x)=\sum_{n<x} a_n$, имеем $\varphi(x)=\Phi(e^x)$ или $\Phi(x)=\varphi(\log x)$. Функция $f(s)$ удовлетворяет условиям тауберовой теоремы при всех λ, и, следовательно,

$$\lim_{x\to\infty}\frac{\Phi(x)}{x}=1, \qquad \text{или} \qquad \Phi(x)\sim x.$$

Мы покажем, как формальным приемом можно обобщить это утверждение на более широкий класс рядов Дирихле.

Теорема 1. *Пусть $f(s)$ — функция, определенная выше; $g(s)=\sum b_n/n^s$ — ряд Дирихле с комплексными коэффициентами b_n, удовлетворяющими неравенству $|b_n|<Ca_n$ для некоторой константы C. Предположим, что ряд $g(s)$ сходится при $\mathrm{Re}\,(s)>1$ и регулярен на прямой $\mathrm{Re}\,(s)=1$, возможно за исключением полюса первого порядка с вычетом α в точке $s=1$. Положим $\Psi(x)=\sum_{n<x} b_n$. Тогда $\Psi(x)\sim\alpha x$.*

Доказательство. Естественно, мы полагаем $\alpha=0$, если в точке $s=1$ нет полюса[1]).

---

[1]) И, естественно, утверждение теоремы в этом случае должно читаться $\frac{\Psi(x)}{x}\sim 0$, а не $\Psi(x)\sim 0$. — *Прим. перев.*

Пусть коэффициенты b_n вещественны. Тогда функция $(Cf+g)/(C+\alpha)$ для достаточно больших C удовлетворяет тем же условиям, что и $f(s)$. Отсюда наше утверждение получается немедленно.

Если коэффициенты b_n комплексны, положим

$$g^*(s)=\sum \bar{b}_n/n^s,$$

так что $g^*(\bar{s})=\overline{g(s)}$, и заметим, что

$$g=\frac{1}{2}(g+g^*)+\frac{1}{2}\frac{(g-g^*)}{i}.$$

Очевидно, отсюда следует наше утверждение для $g(s)$.

Для теоремы о распределении простых идеалов нам нужно знать асимптотическое поведение другой суммы. Сформулируем требуемый результат отдельно.

Предложение 1. *Пусть* b_n $(n=2, 3, \ldots)$ *— такая последовательность комплексных чисел, что*

$$\Psi(N)=\sum_{n=2}^{N} b_n=\alpha N+o(N)$$

для некоторого комплексного числа α. *Тогда*

$$\pi(N)=\sum_{n=2}^{N}\frac{b_n}{\log n}=\alpha\frac{N}{\log N}+o\left(\frac{N}{\log N}\right).$$

Доказательство. Полагая $\Psi(1)=0$, имеем $b_n=\Psi(n)-\Psi(n-1)$ при $n\geqslant 2$. Следовательно,

$$\pi(N)=\sum_{n=2}^{N}\frac{\Psi(n)-\Psi(n-1)}{\log n}=\sum_{2}^{N}\frac{\Psi(n)}{\log n}-\sum_{1}^{N-1}\frac{\Psi(n)}{\log(n+1)}=$$

$$=\frac{\Psi(N)}{\log N}+\sum_{n=2}^{N-1}\Psi(n)\left(\frac{1}{\log n}-\frac{1}{\log(n+1)}\right).$$

Поэтому достаточно показать, что последняя сумма имеет порядок $o(N/\log N)$.

Функция $\Psi(n)$ оценивается сверху величиной Cn; кроме того,

$$\frac{1}{\log n}-\frac{1}{\log(n+1)}=\frac{\log\left(1+\frac{1}{n}\right)}{\log(n)\log(n+1)}<\frac{1/n}{(\log n)^2}.$$

Следовательно, достаточно проверить, что

$$\sum_{2}^{N-1}\frac{1}{(\log n)^2}=o\left(\frac{N}{\log N}\right).$$

Разобьем эту сумму на две, по $2\leqslant n<N^{1/2}$ и по $N^{1/2}\leqslant n<N$. Это даст оценку

$$\frac{N^{1/2}}{(\log 2)^2}+\frac{N}{(\log N^{1/2})^2},$$

которая, очевидно, есть $o(N/\log N)$. Доказательство закончено.

§ 4. Некоторые теоремы о сходимости

Пусть k — конечное расширение поля рациональных чисел $\mathbf{Q}$ степени $[k:\mathbf{Q}]=N$. Пусть $\mathfrak{p}$ пробегает простые идеалы кольца I_k, $\mathfrak{p}\mid p$, степень идеала $\mathfrak{p}$ равна $f_{\mathfrak{p}}$, $\mathbf{N}\mathfrak{p}=p^{f_{\mathfrak{p}}}$. Имеем

$$\sum_{\mathfrak{p}\mid p}f_{\mathfrak{p}}\leqslant N.$$

Символом χ обозначается мультипликативная функция на множестве идеалов поля k с комплексными значениями, для которой либо $|\chi(\mathfrak{p})|=1$, либо $\chi(\mathfrak{p})=0$. Нулевые значения мы включаем для удобства: иногда нужно исключить из рассмотрения некоторые идеалы.

Идеалы записываются мультипликативно; буквой $\mathfrak{a}$ обозначаются целые идеалы,

$$\mathfrak{a}=\prod_{\mathfrak{p}}\mathfrak{p}^{\nu_{\mathfrak{p}}},\qquad \nu_{\mathfrak{p}}\geqslant 0,$$

$\nu_{\mathfrak{p}}=0$ для всех $\mathfrak{p}$, кроме конечного числа. По определению, имеем $\chi(\mathfrak{ab})=\chi(\mathfrak{a})\chi(\mathfrak{b})$. Функция χ с описанными свойствами называется *обобщенным характером*.

Каждому обобщенному характеру χ поставим в соответствие его L-ряд:

$$L(s, \chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N\mathfrak{a}^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{\chi(\mathfrak{p})}{N\mathfrak{p}^s}}.$$

Обобщенный характер, принимающий значения 1 для всех $\mathfrak{p}$, называется *тривиальным характером* и обозначается χ_0. Соответствующий ему L-ряд является дзета-функцией $\zeta_k(s)$ поля k. Покажем, что ряд Дирихле $L(s, \chi)$ сходится при $\operatorname{Re}(s) > 1$.

При $k = \mathbf{Q}$

$$\zeta_{\mathbf{Q}}(s) = \sum_{n=1}^{\infty} n^{-s}$$

представляет собой обычную дзета-функцию. Интегральный критерий показывает, что этот ряд абсолютно сходится при $\operatorname{Re}(s) > 1$ и равномерно — при $\operatorname{Re}(s) \geqslant 1 + \varepsilon$ с любым $\varepsilon > 0$. Отсюда следует, что ряд

$$\sum_{n=2}^{\infty} \frac{\log n}{n^{2s}} \tag{1}$$

сходится абсолютно при $\operatorname{Re}(s) > 1/2$ и равномерно — при $\operatorname{Re}(s) \geqslant 1/2 + \varepsilon$.

Чтобы установить сходимость в общем случае, мы будем сравнивать L-ряд с дзета-функцией или с рядом (1).

Применив к произведению формально оператор логарифмической производной

$$d \log F = F'/F,$$

получим

$$-d \log L(s, \chi) = \sum_{\mathfrak{p},\, m} (\log \mathbf{N}\mathfrak{p})\, \chi(\mathfrak{p}^m)\, \mathbf{N}\mathfrak{p}^{-ms},$$

где сумма берется по всем простым идеалам и всем целым числам $m \geqslant 0$. Если мы докажем, что этот ряд абсолютно сходится при $\operatorname{Re}(s) > 1$, отсюда будет следовать, что ряд для $L(s, \chi)$ тоже сходится абсолютно, и формальное логарифмическое дифференцирование законно для сходящихся рядов.

Но ряд $d \log L(s, \chi)$ мажорируется почленно рядом

$$-d \log \zeta_k(\sigma) = \sum_{\mathfrak{p}, m} (\log \mathbf{N}\mathfrak{p})\, \mathbf{N}\mathfrak{p}^{-m\sigma} = \sum_{p} \sum_{m=1}^{\infty} a_{p,m} p^{-m\sigma},$$

где

$$a_{p,m} = \sum_{\substack{\mathfrak{p} \mid p \\ f_{\mathfrak{p}} \mid m}} f_{\mathfrak{p}} \log p \leqslant N \log p,$$

и, значит, рядом $N \sum_{p} \sum_{m=1}^{\infty} \log(p)\, p^{-m\sigma}$. Если ограничиться только теми $\mathfrak{p}$, для которых $f_{\mathfrak{p}} > 1$, вторую сумму можно начинать с $m = 2$. Суммируя геометрические прогрессии, получаем:

Теорема 2. *Пусть k — числовое поле, χ — обобщенный характер. Ряд $L(s, \chi)$ сходится абсолютно при $\operatorname{Re}(s) > 1$ и равномерно при $\operatorname{Re}(s) \geqslant 1 + \varepsilon$. Далее, произведение*

$$\prod_{f_{\mathfrak{p}} > 1} \frac{1}{1 - \dfrac{\chi(\mathfrak{p})}{\mathbf{N}\mathfrak{p}^s}}$$

сходится абсолютно при $\operatorname{Re}(s) > 1/2$ и равномерно при $\operatorname{Re}(s) \geqslant 1/2 + \varepsilon$.

Очевидно, только простые дивизоры степени $f_{\mathfrak{p}} = 1$ вносят вклад в нули и полюсы ζ-функции при $\operatorname{Re}(s) > 1/2$.

Теорема 3. *Предположим, что функция $L(s, \chi_0)$ имеет полюс первого порядка в точке $s = 1$. Пусть χ — обобщенный характер, $\chi \neq \chi_0$. Если $\chi^2 \neq \chi_0$, примем, кроме того, что функции $L(s, \chi)$ и $L(s, \chi^2)$ голоморфны в окрестности точки $s = 1$; если же $\chi^2 = \chi_0$, примем, что функции $L(s, \chi_0)$ и $L(s, \chi)$ голоморфны при $\operatorname{Re}(s) > 1 - \delta$ для некоторого $\delta > 0$ всюду, за исключением простого полюса функции $L(s, \chi_0)$ в точке $s = 1$. Тогда $L(1, \chi) \neq 0$.*

Доказательство. Пусть $L(1, \chi) = 0$; для вещественного $s > 1$ имеем

$$L(s, \chi) = \exp\Big(\sum_{\mathfrak{p}, m} \frac{\chi(\mathfrak{p}^m)}{m \mathbf{N}\mathfrak{p}^{ms}} \Big),$$

где $\exp(x) = e^x$. Рассмотрим функцию

$$f(s) = L^3(s, \chi_0) L^4(s, \chi) L(s, \chi^2) = \\ = \exp\left(\sum_{\mathfrak{p}, m} \frac{3 + 4\chi(\mathfrak{p}^m) + \chi^2(\mathfrak{p}^m)}{m\mathrm{N}\mathfrak{p}^{ms}} \right).$$

Тогда

$$|f(s)| = \exp\left[\sum_{\mathfrak{p}, m} \frac{3 + 4\cos\theta + \cos 2\theta}{m\mathrm{N}\mathfrak{p}^{ms}} \right],$$

где $\theta = \arg\chi(\mathfrak{p}^m)$. Так как $3 + 4\cos\theta + \cos 2\theta \geqslant 0$, отсюда следует, что $|f(s)| \geqslant 1$ при $\mathrm{Re}(s) > 1$. Предположим, что $\chi^2 \neq \chi_0$. Если $L(1, \chi) = 0$, то функция $f(s)$ должна иметь нуль в точке $s = 1$. Соответствующий ряд представляет эту функцию при $\mathrm{Re}(s) > 1$, и так как f непрерывна в точке $s = 1$, она должна стремиться к нулю при $s \to 1$. Противоречие.

Если $\chi^2 = \chi_0$, рассмотрим функцию

$$L(s, \chi_0) L(s, \chi) = \exp\left(\sum_{\mathfrak{p}, m} \frac{1 + \chi(\mathfrak{p}^m)}{m\mathrm{N}\mathfrak{p}^{ms}} \right).$$

Выражение под знаком экспоненты представляет собой ряд Дирихле с неотрицательными коэффициентами, который мажорирует ряд

$$\sum_{\mathfrak{p}, m} \frac{2}{2m\mathrm{N}\mathfrak{p}^{2ms}},$$

расходящийся при $s = 1/2$ (как логарифм дзета-функции). Это противоречит [1]) следующей лемме о рядах Дирихле с неотрицательными коэффициентами.

Лемма 1. *Пусть $f(s) = \sum a_n n^{-s}$ — ряд Дирихле с неотрицательными вещественными коэффициентами, сходящийся при $\mathrm{Re}(s) > \sigma_0$. Пусть, кроме того, функция $f(s)$ голоморфна в точке σ_0. Тогда ряд сходится при*

[1]) Противоречие связано с предположением $L(1, \chi) = 0$, из которого в силу условий теоремы следовало бы, что функция $L(s, \chi_0) L(s, \chi)$ голоморфна при $s = 1$. — *Прим. перев.*

$\mathrm{Re}(s) > \sigma_0 - \delta$ *для некоторого* $\delta > 0$ (*и, следовательно, представляет* $f(s)$ *в этой большей полуплоскости*).

Доказательство. Пусть $\delta > 0$ — достаточно малое число. Произведя сдвиг, мы можем считать, что $\sigma_0 = 0$. При $0 < \sigma < \delta$ имеем

$$f(\sigma) = \sum_n a_n e^{-(\sigma-\delta)\log(n) e^{-\delta \log(n)}}.$$

Заменим экспоненты e^z рядами $\sum_\nu z^\nu/\nu!$. Так как все коэффициенты положительны, суммирования $\sum_n \sum_\nu$ можно поменять местами. Получится разложение функции f в степенной ряд в окрестности δ, сходящийся при $\sigma = -2\delta$. Этот степенной ряд можно снова превратить в ряд Дирихле в полосе $-2\delta \leqslant \sigma < \delta$, откуда и следует, что этот ряд сходится при $\mathrm{Re}(s) \geqslant -\delta$.

§ 5. Плотности

Пусть χ — характер Гекке, т. е. характер группы классов иделей поля k. Если он неразветвлен в конечном простом идеале $\mathfrak{p}$, т. е. обращается в нуль на группе локальных единиц $U_\mathfrak{p}$, то $\chi(\pi_\mathfrak{p}) = \chi(\mathfrak{p})$ представляет собой функцию только от $\mathfrak{p}$, и мы можем ввести функцию

$$L(s, \chi) = \prod \frac{1}{1 - \frac{\chi(\mathfrak{p})}{\mathrm{N}\mathfrak{p}^s}},$$

где произведение распространено на все $\mathfrak{p}$, в которых характер χ неразветвлен. Из результатов гл. VII следует, что такой L-ряд удовлетворяет условиям, сформулированным в предыдущем параграфе, и условиям применимости тауберовой теоремы.

Пусть $x > 0$; символом P_x обозначим множество простых идеалов с условием $\mathrm{N}\mathfrak{p} \leqslant x$, а символом A_x — множество целых идеалов с условием $\mathrm{N}\mathfrak{a} \leqslant x$. Для всякого конечного множества простых иделов S обозначим символом A_x^S множество тех целых идеалов $\mathfrak{a}$, которые взаимно просты с S и для которых $\mathrm{N}\mathfrak{a} \leqslant x$; аналогичный смысл имеет P_x^S.

В качестве частного случая тауберовой теоремы получаем:

Теорема 4. *Пусть* α *— вычет дзета-функции* $\zeta_k(s)$ *в точке* 1. *Пусть* $n(A_x^S)$ *и* $n(P_x)$ *— число элементов множеств* A_x^S *и* P_x *соответственно. Имеют место следующие асимптотические формулы:*

$$n(A_x^S) \sim \alpha\beta x,$$
$$n(P_x) \sim x/\log x,$$

где $\beta = \prod_{\mathfrak{p}\in S}(1 - 1/\mathbf{N}\mathfrak{p})$.

В самом деле, вычет в точке 1 функции, которая получается из $\zeta_k(s)$ опусканием множителей, относящихся к элементам S, равен $\alpha\beta$. Отсюда следует первое утверждение. Для доказательства второго применим тауберову теорему к логарифмической производной дзета-функции

$$\sum_{\mathfrak{p},m} \frac{\log \mathbf{N}\mathfrak{p}}{\mathbf{N}\mathfrak{p}^{ms}}.$$

Разобьем эту сумму, как обычно, на две: одну по всем $\mathfrak{p}$ и $m = 1$, другую — по $m > 1$. Вторая сумма не вносит вклада в вычет в точке 1, а первая сумма

$$\sum_{\mathfrak{p}} \frac{\log \mathbf{N}\mathfrak{p}}{\mathbf{N}\mathfrak{p}^{s}}$$

представляет собой ряд Дирихле $\sum b_n/n^s$, где $b_n = 0$, если n не является степенью простого числа. Для каждого целого числа $n \geqslant 2$ обозначим символом $\mu(n)$ число идеалов $\mathfrak{p}$, для которых $\mathbf{N}\mathfrak{p} = n$. Тогда $b_n = \mu(n)\log n$. Вычет логарифмической производной функции $\zeta_k(s)$ в точке $s = 1$ равен 1. В силу теоремы 1 получаем

$$\sum_{n<x} b_n \sim x.$$

Для завершения доказательства остается применить предложение 1.

Займемся теперь вопросом о равномерности распределения простых идеалов.

Пусть G — компактная коммутативная группа. Пусть $F = \bigcup F_r$ — объединение конечных подмножеств F_r, $r = 1, 2, \ldots$ и $F_r \subset F_{r+1}$. Рассмотрим некоторое отображение $\lambda : F \longrightarrow G$. Мы будем говорить, что множество F *λ-равномерно распределено* в группе G, если для всякого характера χ этой группы

$$\lim_{r\to\infty} \frac{1}{n(F_r)} \sum_{\xi\in F_r} \chi \circ \lambda(\xi) = \int_G \chi.$$

Напомним, что $\int_G \chi = 1$, если $\chi = \chi_0$, и 0, если $\chi \neq \chi_0$.

Мы примем без доказательства, что всякая непрерывная функция на компактной группе допускает равномерное приближение линейными комбинациями характеров с комплексными коэффициентами.

Назовем вещественную функцию f на G *допустимой*, если существуют такие последовательности вещественных непрерывных функций $\{g_n\}$, $\{h_n\}$, что

$$g_n \leqslant f \leqslant h_n,$$

g_n, h_n сходятся к f, соответственно монотонно возрастая и убывая, и, кроме того,

$$\int_G (g_n - h_n) \longrightarrow 0$$

при $n \longrightarrow \infty$.

Комплексная функция называется допустимой, если ее вещественная и мнимая части допустимы.

Если множество F λ-равномерно распределено в группе G, а f — любая допустимая функция на G, то

$$\lim_{r\to\infty} \frac{1}{n(F_r)} \sum_{\xi\in F_r} f \circ \lambda(\xi) = \int_G f.$$

Это немедленно следует из рассмотрения равномерных приближений функции f линейными комбинациями характеров. На практике в качестве f берется характеристическая функция подходящих подмножеств группы G. Если, например, G конечна, рассмотрим характеристическую функцию f одного элемента; тогда $\int_G f = 1/n(G)$.

Все интересующие нас теоремы о равномерном распределении вытекают из следующего результата.

Теорема 5. *Пусть* χ *— нормализованный характер Гекке,* $\chi \neq \chi_0$, S *— конечное множество простых идеалов, содержащее все идеалы, где* χ *разветвлен. Тогда*

$$\lim_{r\to\infty} \frac{1}{n(A_r^S)} \sum_{\mathfrak{a}\in A_r^S} \chi(\mathfrak{a}) = 0,$$

$$\lim_{r\to\infty} \frac{1}{n(P_r^S)} \sum_{\mathfrak{p}\in P_r^S} \chi(\mathfrak{p}) = 0.$$

Доказательство. Результат получается немедленно. В самом деле, мы знаем, что L-ряд голоморфен в точке 1 и не обращается в ней в нуль. Следовательно, вычеты L-ряда и его производной равны нулю и наше утверждение следует из теоремы 1 и предложения 1 соответственно.

Пусть $J = J_k$ — группа иделей поля k. Пусть S — конечное множество нормирований, содержащее архимедовы нормирования, J^S — подгруппа группы J, состоящая из иделей, компоненты которых являются единицами вне S и 1 в S. Не следует смешивать эту подгруппу с подгруппой J_S, элементы которой имеют компонентами единицы вне S и что угодно — в S. По непрерывности, всякий характер группы классов иделей становится тривиальным на одной из подгрупп J^S; кроме того, он тривиален на мультипликативной группе k^* поля k, вложенной в J. Пусть G — компактная группа, $\lambda : J/k^*J^S \to G$ — непрерывный гомоморфизм. Тогда для любого характера χ группы G функция $\chi \circ \lambda$ является характером группы классов иделей, т. е. характером Гекке. Множество P^S простых идеалов, не принадлежащих S, можно следующим образом погрузить в J/k^*J^S. Пусть π — элемент первого порядка относительно идеала $\mathfrak{p} \notin S$. Этому элементу соответствует идель, у которого $\mathfrak{p}$-компонента равна π, а остальные — 1. Класс π по модулю k^*J^S не зависит от выбора простого элемента; отображение, ставящее в соответствие идеалу $\mathfrak{p}$ этот класс, определяет интересующее

нас вложение P^S в J/k^*J^S. (Мы можем также поставить в соответствие идеалу $\mathfrak{p}$ идель π^{-1}. Это и будет сделано в последующих примерах, чтобы не расходиться с классическим описанием для архимедовых нормирований.)

Гомоморфизм λ индуцирует некоторое отображение $P^S \longrightarrow G$, и из предыдущей теоремы следует, что множество P^S λ-равномерно распределено в группе G.

Подведем итоги этого обсуждения.

Теорема 6. *Пусть P — множество простых идеалов, $\tau : P \longrightarrow J_k$ — отображение, которое определяется так. Для каждого идеала $\mathfrak{p}$ выберем простой элемент $\pi_\mathfrak{p} \in k^*_{v_\mathfrak{p}}$ и обозначим символом $\tau(\mathfrak{p})$ идель, все компоненты которого, кроме $v_\mathfrak{p}$-й, равны 1, а $v_\mathfrak{p}$-я равна $\pi_\mathfrak{p}$. Множество P представим как объединение подмножеств P_r, состоящих из тех $\mathfrak{p}$, для которых $\mathbf{N}\mathfrak{p} \leqslant r$. Пусть G — компактная коммутативная группа, $\sigma : J_k \longrightarrow G$ — непрерывный эпиморфизм, ядро которого содержит k^*, но не содержит J^0, $\lambda = \sigma \circ \tau$. Тогда множество P λ-равномерно распределено в группе G.*

Можно, например, положить $G = J/k^*J_S$ (это — конечная группа), а в качестве λ взять канонический гомоморфизм. Это даст равномерное распределение простых идеалов в S-классах идеалов. Оставляем читателю в качестве упражнения вывод равномерного распределения простых идеалов в обычных арифметических прогрессиях (теорема Дирихле).

Рассмотрим, наконец, гауссово поле $k = \mathbf{Q}(i)$. Пусть S состоит из архимедова нормирования. Имеем

$$J/k^*J^S \approx k^*_\infty \ (\pm 1, \ \pm i),$$

где k^*_∞ — мультипликативная группа комплексных чисел. Идеалы можно рассматривать как точки первого квадранта гауссовой плоскости. Беря в качестве λ радиальную проекцию на единичную окружность, получим равномерное распределение идеалов и простых идеалов в секторах.

Глава IX

ТЕОРЕМА БРАУЭРА—ЗИГЕЛЯ

С помощью интегральных выражений дзета-функции можно получить некоторые оценки для ее вычета и вывести из них один асимптотический результат, связывающий число классов, регулятор и дискриминант числового поля. Формулировка этого результата такова.

Пусть k пробегает последовательность числовых полей, нормальных над $\mathbf{Q}$, степень N которых и абсолютная величина дискриминанта d удовлетворяют условию $N/\log d \to 0$. Тогда

$$\log(hR) \sim \log d^{1/2}.$$

Вопрос о необходимости условия нормальности и предположения $N/\log d \to 0$ связан, с одной стороны, с гипотезой Артина о неабелевых L-рядах, а с другой — с классической задачей о существовании бесконечных неразветвленных расширений[1]). В самом деле, когда K пробегает неразветвленные расширения поля k, отношение $N_K/\log d_K$ остается постоянным.

Заметим, что дискриминант поля $k=\mathbf{Q}(\zeta)$, где ζ — корень из единицы простой степени p, равен $d_k=p^{p-2}$, так что наше утверждение применимо к этим полям. То же относится к башне полей корней p^r-й степени из 1.

Ввиду этого изучение поведения $N/\log d$ представляет значительный интерес. Мы будем пользоваться, по существу, элементарным утверждением об ограниченности числа $N/\log d$ на множестве числовых полей $k \neq \mathbf{Q}$ $(N>1)$. Это немедленно вытекает из теоремы Минковского о существовании в каждом классе идеалов целого идеала $\mathfrak{a}$

---

[1]) Существование бесконечных неразветвленных расширений было недавно доказано Е. Голодом и И. Шафаревичем [11].—*Прим. перев.*

с нормой $\mathbf{N}\mathfrak{a} \leqslant C_N d^{1/2}$, где C_N — константа Минковского. Извлекая корень степени N из обеих частей неравенства и пользуясь тем, что $1 \leqslant \mathbf{N}\mathfrak{a}$, после несложного вычисления находим, что $\mathbf{N}/\log d \leqslant C$, где C — некоторая константа.

§ 1. Верхняя оценка для вычета

Лемма 1. *Существует такая абсолютная константа c_1, что неравенство*

$$\varkappa(k) \leqslant c_1^N (1+\alpha)^N d_k^{1/2\alpha} \qquad (N = [k:\mathbf{Q}])$$

имеет место для всех числовых полей и всех $\alpha \geqslant 1$.

Доказательство. Пользуясь следствием 3 из теоремы 14 и теоремой 15 (гл. VII) и учитывая, что интегральные выражения для дзета-функции неотрицательны при вещественных s, получаем для $s > 1$ неравенство

$$(2^{-2r_2}\pi^{-N} d_k)^{s/2} \Gamma^{r_1}\left(\frac{s}{2}\right) \Gamma^{r_2}(s)\, \zeta_k(s) \geqslant \varkappa \frac{d_k^{1/2}(2\pi)^{-r_2}}{s(s-1)}.$$

Положим $s = 1 + \alpha^{-1}$. Множители Γ равномерно ограничены; члены c_1^N и $d_k^{1/2\alpha}$ получаются очевидным образом; из представления дзета-функции в виде произведения находим

$$\zeta_k\left(1+\frac{1}{\alpha}\right) \leqslant \zeta_{\mathbf{Q}}\left(1+\frac{1}{\alpha}\right)^N \leqslant (1+\alpha)^N.$$

Это дает требуемый результат.

Лемма 2. *Существует такая константа c_2, что для всех $k \neq \mathbf{Q}$ имеем*

$$\log(hR)/\log(d^{1/2}) \leqslant c_2.$$

Если k пробегает последовательность полей, для которой $N/\log d \to 0$, то

$$\overline{\lim}\left[\left(\frac{\log hR}{\log d^{1/2}} - 1\right)\frac{1}{N}\right] \leqslant 0.$$

Доказательство. Воспользуемся элементарной оценкой, согласно которой число w корней из единицы в числовом поле k не превосходит $c_3 N^2$, где c_3 — абсолютная константа. (Поле корней степени n из единицы

имеет над $\mathbf{Q}$ степень $\varphi(n)$; тогда, учитывая, что $\varphi(p^r)=(p-1)\,p^{r-1}$ и $\varphi(mn)=\varphi(m)\,\varphi(n)$ для взаимно простых m, n, получаем необходимую оценку для n в терминах $\varphi(n)$.)

Из леммы 1 и формулы для $\varkappa$ находим

$$\frac{\log hR}{\log d^{1/2}}-1\leqslant\frac{N}{\log d^{1/2}}\log(c_1(1+\alpha))+\frac{1}{\alpha}+\frac{N}{\log d^{1/2}}\log c_2.$$

Полагая $\alpha=1$, получаем первое утверждение. Зафиксируем α и рассмотрим нашу последовательность полей; если α достаточно велико, то для всех полей, кроме конечного числа их, левая часть не превосходит $\alpha^{-1}+\varepsilon$, где ε можно сделать сколь угодно малым.

§ 2. Нижняя оценка для вычета

Лемма 3. *Пусть s_0 — вещественное число, $0<s_0<1$. Предположим, что $\zeta(g_0, s_0)\leqslant 0$ (или, что то же самое, $\zeta_k(s_0)\leqslant 0$). Тогда*

$$\varkappa(k)\geqslant s_0(1-s_0)\,2^{-N}e^{-4\pi N}d_k^{(s_0-1)/2}.$$

Доказательство. В силу теоремы 15 гл. VII, § 8, имеем

$$\frac{\varkappa g_0(0)}{s_0(1-s_0)}\geqslant\int\limits_{\|a\|\geqslant 1}\hat{g}_0(a)\,\|a\|^{s_0}d^*a.$$

Уменьшим область интегрирования до $P=\prod P_v$, где P_v — множество единиц U_v для неархимедовых v и область

$$1\leqslant\|a_v d^{-1/2N}\|_v\leqslant 2$$

для архимедовых v. Значение интеграла при этом уменьшится; интеграл по P равен произведению локальных интегралов, которые мы сейчас вычислим.

Пусть v есть $\mathfrak{p}$-адическое нормирование. Тогда $g_{0,v}=d_{\mathfrak{p}}^{1/2}f_{0,v}$ и, значит, $\hat{g}_{0,v}=d_{\mathfrak{p}}^{1/2}\hat{f}_{0,v}$ есть $d_{\mathfrak{p}}$-кратная характеристическая функция множества $\mathfrak{a}_v$. Поэтому в этом случае интересующий нас локальный интеграл равен

$$\int\limits_{P_v}\hat{g}_{0,v}(a)\,d^*a=d_{\mathfrak{p}}^{1/2}.$$

Пусть теперь v — архимедово. Воспользуемся предложением 9 гл. VII, § 8, чтобы выразить $\hat{g}$ через $\hat{f}$. Замена переменной $z = a_v d^{-1/2N}$ превращает интеграл по P_v в

$$\| d^{1/2N} \|_v^{(s_0-1)} \int \hat{f}_{0,v}(z)\, d^*z,$$

где область интегрирования имеет вид $1 \leqslant \| z \|_v \leqslant 2$. Заменим $\hat{f}_{0,v}(z)$ нижней гранью этой функции в области интегрирования, именно числом $e^{-4\pi}$ в вещественном случае и $(1/2\pi)\, e^{-4\pi}$ — в комплексном. Мера области равна $\log 2$ и $2\pi \log 2$ соответственно. Это дает для интеграла оценку снизу вида

$$\| d^{1/2N} \|_v^{(s_0-1)} e^{-4\pi} \log 2.$$

Произведение по всем нормированиям приводит к неравенству

$$\varkappa d^{1/2} (2\pi)^{-r_2} \geqslant s_0 (1 - s_0)\, d^{1/2} d^{(s_0-1)/2} e^{-4\pi N} (\log 2)^N,$$

где мы пользуемся числом N вместо $r_1 + r_2$. Оценка в формулировке леммы является некоторым ослаблением этого неравенства.

Наша цель состоит в доказательстве следующей теоремы.

Теорема 1. *Пусть* $\varepsilon > 0$. *Существует такое число* $c_4(\varepsilon)$, *что для всех полей* k, *нормальных над* $\mathbf{Q}$, *имеет место неравенство*

$$\varkappa(k) \geqslant c_4(\varepsilon)^{-N} d_k^{-\varepsilon}.$$

Доказательство. Пользуясь гипотезой Римана, мы могли бы избавиться от условия нормальности. В самом деле, в рассуждениях приходится различать два случая.

Случай 1. Для всех нормальных полей k функция $\zeta_k(s)$ не обращается в нуль для вещественных s в интервале

$$1 - \varepsilon/N < s < 1.$$

Из интегрального представления тогда следует, что дзета-функция отрицательна вблизи от 1 слева. Следовательно, $\zeta_k(1 - \varepsilon/N) \leqslant 0$, и, полагая, $s_0 = 1 - \varepsilon/N$

в лемме 3, находим требуемое. Это же рассуждение проходит и для полей k, не являющихся нормальными.

Случай 2. Существует такое нормальное расширение k_0 поля $\mathbf{Q}$ степени N_0, что $\zeta_{k_0}(s_0)=0$ для некоторого вещественного значения s_0, удовлетворяющего неравенствам $1-\varepsilon/N_0<s_0<1$.

Чтобы справиться с этим случаем, нам придется предпринять обходной путь через теорию L-рядов. В следующем параграфе мы докажем такой результат.

Теорема 2. *Существует такая константа* c_5, *что для всех числовых полей* k *и нормальных расширений* K *поля* k *имеет место неравенство*

$$\varkappa(K)/\varkappa(k)\leqslant c_5^{N_K-N_k}(1+\alpha)^{N_K-N_k}(d_K/d_k)^{1/2\alpha}$$

для любых $\alpha\geqslant 1$.

Примем пока эту теорему. Нам понадобится еще следующая фундаментальная лемма Брауэра, доказательство которой приведено в приложении.

Лемма. *Пусть* G — *конечная группа*, χ_{reg} — *характер ее регулярного представления. Существуют такие циклические подгруппы* $H_j\neq 1$, *положительные рациональные числа* λ_j *и одномерные характеры* $\psi_j\neq 1$ *групп* H_j, *что*

$$\chi_{\mathrm{reg}}=\chi_0+\sum\lambda_j\psi_j^*,$$

где звездочка означает индуцированный характер.

Мы воспользуемся этой леммой несколько раз. Для начала отметим, что если поле K нормально над k и $\zeta_k(s_0)=0$ для некоторого s_0, то также $\zeta_K(s_0)=0$. (Для расширений, не являющихся нормальными, вопрос остается открытым. Конечно, ответ следовал бы из гипотез Артина.) Мы используем формулу Артина

$$\zeta_K(s)=\zeta_k(s)\prod L(s,\psi_j^*,K/k)^{\lambda_j};$$

входящие в нее L-ряды являются абелевыми L-рядами типа, изученного в гл. VII.

Теперь приступим к разбору второго случая. Число s_0, нуль дзета-функции между $1-\varepsilon/N_0$ и 1 и дискриминант поля k_0 можно считать функциями только от ε. Пусть k — нормальное расширение поля $\mathbf{Q}$. Положим $K=kk_0$. Тогда поле K нормально над k_0 и, следовательно, $\zeta_K(s_0)=0$.

По лемме 3,

$$\varkappa(K) \geqslant s_0(1-s_0)\,2^{-N_K} e^{2\pi N_K} d_K^{-(1-s_0)/2}.$$

Элементарная оценка дает

$$N_K \leqslant N_0 N_k, \qquad d_K \leqslant d_k^{N_0} d_0^{N_k},$$

откуда

$$d_K^{-(1-s_0)/2} \geqslant d_K^{-\varepsilon/2N_0} \geqslant d_k^{-\varepsilon/2} d_0^{-\varepsilon N_k/2N_0},$$

и мы получаем

$$\varkappa(K) \geqslant c_5(\varepsilon)^{-N_k} d_k^{-\varepsilon/2}.$$

В силу теоремы 2, связывающей вычеты в полях k и K, полагая $\alpha = N_0/\varepsilon$, получаем неравенство

$$\varkappa(k) \geqslant \varkappa(K)\, c_8(\varepsilon)^{-N_k} d_k^{-\varepsilon/2}.$$

Из последних двух неравенств следует теорема 1.

§ 3. Сравнение вычетов в нормальных расширениях

Нашей целью теперь является доказательство теоремы 2. Опять воспользуемся леммой Брауэра о представлениях групп и разложением дзета-функции:

$$\zeta_K(s) = \zeta_k(s) \prod L(s, \psi_j^*, K_j/k)^{\lambda_j}.$$

Всякий L-ряд в этом разложении имеет вид $L(s, \psi_j)$, где ψ_j — нетривиальный характер группы классов иделей поля K_j. Имеем

$$\varkappa(K)/\varkappa(k) = \prod L(1, \psi_j)^{\lambda_j}.$$

Множители справа конечны из-за нетривиальности характеров ψ_j.

Нам нужно оценить сверху величины $|L(1, \psi_j)|$. Отметим, что ψ_j — характеры конечного порядка.

Лемма 4. *Пусть k — числовое поле, $\psi \neq 1$ — характер конечного порядка группы C_k, $\alpha \geqslant 1$. Тогда*

$$|L(1, \psi)| \leqslant c_6^N (1+\alpha)^N d_\psi^{1/2\alpha}.$$

Доказательство. В обозначениях гл. VII, § 8, имеем

$$\zeta(g_\psi, \psi, 1) = \int\limits_{\|a\|\geqslant 1} g_\psi(a)\,\psi(a)\,\|a\|\,d^*a + \int\limits_{\|a\|\geqslant 1} \hat{g}_\psi(a)\,\bar{\psi}(a)\,d^*a.$$

Прямой подсчет показывает, что $|\hat{g}_\psi| \leqslant |g_\psi|$. Это дает верхнюю оценку

$$|\zeta(g_\psi, \psi, 1)| \leqslant 2 \int\limits_{\|a\|\geqslant 1} |g_\psi(a)|\,\|a\|^s d^*(a) \leqslant$$

$$\leqslant 2\zeta(|g_\psi|, \chi_0, s) \quad (s>1).$$

Наш характер неразветвлен относительно комплексных нормирований v. Пусть ν — число разветвленных вещественных нормирований, $\mu = r_1 - \nu$. Положим

$$\Gamma(s, \psi) = \Gamma\left(\frac{s+1}{2}\right)^\nu \Gamma\left(\frac{s}{2}\right)^\mu \Gamma(s)^{r_2}.$$

Несложная оценка локальных интегралов и представление дзета-функции в виде произведения локальных множителей дают неравенство

$$d_\psi^{1/2} 2^{-r_2} \pi^{-N/2}\,\Gamma(1, \psi)\,|L(1, \psi)| \leqslant$$

$$\leqslant 2\,(d_\psi^{1/2} 2^{-r_2} \pi^{-N/2})^s\,\Gamma(s, \psi)\,\zeta_k(s)$$

при $s>1$. Полагая $s = 1 + \alpha^{-1}$ и пользуясь той же тривиальной оценкой дзета-функции, что и в § 1, получаем неравенство леммы.

Положим

$$N_j = [K_j : \mathbf{Q}].$$

Применим лемму 4 к полям K_j и характерам ψ_j. Это дает

$$\varkappa(K)/\varkappa(k) \leqslant \Pi c_6^{N_j\lambda_j} (1+\alpha)^{N_j\lambda_j} d_{\psi_j}^{\lambda_j/2\alpha}.$$

Далее,

$$N_K = N_k + \sum N_j\lambda_j.$$

Это тождество получается, если умножить на $[k : \mathbf{Q}]$ значение характера регулярного представления $G(K/k)$

в единице. Отсюда и из формулы Артина для дискриминанта (см. [3]) сразу же получаем

$$d_K = d_k \Pi d_{\psi_j}^{\lambda_j}.$$

(Провести вычисление для дифференты, пользуясь ее мультипликативностью в башнях расширений.) Из этих разложений степени и дискриминанта немедленно следует требуемая оценка отношения вычетов.

Для удобства читателя приведем доказательство формулы разложения дискриминанта. Согласно формуле Артина, имеем

$$D_{K/k} = N_{K/k}(\mathfrak{D}_{K/k}) = \Pi N_{K_j/k}(\mathfrak{D}_{Kj/k} \mathfrak{f}_{\psi_j})^{\lambda_j}.$$

Умножим обе части этого равенства на

$$N_{K/k}(\mathfrak{D}_{k/\mathbf{Q}}) = \mathfrak{D}_{k/\mathbf{Q}}^{[K:k]}$$

и воспользуемся тождеством для степеней. Это дает

$$N_{K/k}(\mathfrak{D}_{K/\mathbf{Q}}) = \mathfrak{D}_{K/\mathbf{Q}} \Pi N_{K_j/k}(\mathfrak{D}_{K_j/\mathbf{Q}} \mathfrak{f}_{\psi_j})^{\lambda_j}.$$

Взяв норму $N_{k/\mathbf{Q}}$ от обеих частей этого равенства, получим требуемое.

§ 4. Окончание доказательства

Нижняя граница для вычета, полученная в § 2, приводит к неравенству вида

$$\log(hR) - \log d_k^{1/2} \geqslant -Nc_7(\varepsilon) - 2\varepsilon \log d_k^{1/2}.$$

Как мы уже отмечали, отношение $N/\log d$ ограничено на множестве всех числовых полей, отличных от $\mathbf{Q}$. Это позволяет следующим образом дополнить первое утверждение леммы 2.

Теорема 3. *Существует такая константа c_8, что для всех полей k, нормальных над $\mathbf{Q}$, имеет место неравенство*

$$|\log(hR)| \geqslant c_8 \log d^{1/2}.$$

Далее, если k пробегает некоторую последовательность полей, нормальных над $\mathbf{Q}$, для которой $N/\log d \to 0$, из предыдущего неравенства вытекает, что

$$\varliminf [\log (hR)/\log d^{1/2}] \geqslant 1 - 2\varepsilon.$$

Комбинируя этот результат с леммой 2, получаем:

Теорема 4. *Пусть k пробегает некоторую последовательность полей, нормальных над $\mathbf{Q}$, для которой $N/\log d \to 0$. Тогда*

$$\log (Rh) \sim \log d^{1/2}.$$

Нетрудно оценить дискриминант наименьшего нормального расширения k', содержащего данное числовое поле $k/\mathbf{Q}$:

$$d_{k'} \leqslant d_k^{N'/2},$$

где $N' = [k' : \mathbf{Q}]$. Применяя теорему 2 к полям k' и k и полагая $\alpha = \varepsilon/2$, $\varepsilon < 1/2$, находим

$$\varkappa (k) \geqslant \varkappa (k')\, c_9 (\varepsilon)^{-N'} d_{k'}^{-\varepsilon}.$$

С другой стороны, теорема 1 в применении к полю k' дает

$$\varkappa (k') \geqslant c_4 (\varepsilon)^{-N'} d_{k'}^{-\varepsilon},$$

так что

$$Rh/d^{1/2} \geqslant c_{10} (\varepsilon)^{-N'} d_{k'}^{-2}$$

и

$$\log (Rh) - \log d^{1/2} \geqslant -N' c_{10} (\varepsilon) - 2\varepsilon \log d_{k'}.$$

Оценивая $d_{k'}$ через d_k, как выше, получаем, наконец,

$$\left[\frac{\log (Rh)}{\log d^{1/2}} - 1\right] \frac{1}{N'} \geqslant -\frac{c_{10} (\varepsilon)}{\log d^{1/2}} - 2\varepsilon.$$

Число полей с ограниченным дискриминантом конечно. Левая часть последнего неравенства ограничена снизу и не имеет отрицательных предельных значений, когда k пробегает все числовые поля, отличные от $\mathbf{Q}$. Из леммы 2 следует наш основной результат.

Теорема 5. *Пусть k пробегает все числовые поля, отличные от $\mathbf{Q}$, N' — степень над $\mathbf{Q}$ наименьшего нор-*

мального поля k', содержащего k. Тогда множество значений величины

$$\left[\frac{\log(Rh)}{\log d^{1/2}} - 1\right]\frac{1}{N'}$$

ограничено и имеет своей единственной предельной точкой 0.

Следствие. *Пусть k пробегает числовые поля фиксированной степени N над полем* **Q**. *Тогда имеет место асимптотическая формула*

$$\log(hR) \sim \log d^{1/2}$$

при $d \to \infty$.

Доказательство. Очевидно, учитывая, что $d' \leqslant d!$.

Приложение — лемма Брауэра

В этом приложении мы докажем лемму о групповых характерах, которая неоднократно использовалась в этой главе. Нижеследующим изложением я обязан Серру (оно является переработкой рассуждений Брауэра).

Пусть G — конечная группа. Символом 1_G обозначим тривиальный характер, символом r_G — характер регулярного представления и положим $u_G = r_G - 1_G$. Для всякой подгруппы $H \subset G$ и всякого характера ψ группы H символом ψ^* обозначим индуцированный характер группы G.

Пусть A — циклическая группа порядка a. Определим функцию θ_A на A следующими условиями:

$$\theta_A(\sigma) = \begin{cases} a, & \text{если } \sigma \text{ — образующая группы } A, \\ 0 & \text{в противном случае.} \end{cases}$$

Положим $\lambda_A = \varphi(a) r_A - \theta_A$ (φ — функция Эйлера); $\lambda_A = 0$, если $a = 1$. Нужный нам результат содержится в двух предложениях.

Предложение 1. *Пусть G — конечная группа порядка g. Тогда*

$$u_G = \frac{1}{g}\sum \lambda_A^*,$$

где сумма взята по всем циклическим подгруппам группы G.

Доказательство. Для любых двух функций χ, ψ на G определено обычное скалярное произведение

$$\langle \psi, \chi\rangle_G = \frac{1}{g}\sum_{\sigma\in G}\psi(\sigma)\,\overline{\chi(\sigma)}.$$

Пусть ψ — произвольная функция на G. Тогда

$$\langle \psi, gu_G\rangle = \langle \psi, gr_G\rangle - \langle \psi, g1_G\rangle = g\psi(1) - \sum_{\sigma\in G}\psi(\sigma).$$

С другой стороны, пользуясь тем стандартным фактом, что оператор, переводящий характер подгруппы в индуцированный характер всей группы, сопряжен с оператором ограничения на подгруппу, получаем

$$\sum_A \langle \psi, \lambda_A^*\rangle = \sum_A \langle \psi \mid A, \lambda_A\rangle = \sum_A \langle \psi \mid A, \varphi(a) r_A - \theta_A\rangle =$$

$$= \sum_A \varphi(a)\psi(1) - \sum_A \frac{1}{a}\sum_{\sigma \text{ обр. } A} a\psi(\sigma) = g\psi(1) - \sum_{\sigma\in G}\psi(\sigma).$$

Следовательно, функции в обеих частях доказываемого равенства имеют одинаковые скалярные произведения с любой функцией и потому совпадают. Предложение доказано.

Предложение 2. *Если $A \neq \{1\}$, то функция λ_A является линейной комбинацией неприводимых нетривиальных характеров группы A с целыми положительными коэффициентами.*

Доказательство. Если порядок циклической группы A прост, то в силу предложения 1 имеем $\lambda_A = gu_A$, и требуемый результат следует из известной структуры регулярного представления.

Для доказательства утверждения в общем случае достаточно установить, что коэффициенты Фурье функции λ_A относительно любого характера первой степени являются неотрицательными целыми числами. Пусть ψ — характер первой степени. Вычисляя скалярное произведе-

ние относительно A, получаем

$$\langle \psi, \lambda_A \rangle = \varphi(a)\psi(1) - \sum_{\sigma \text{ обр.}} \psi(\sigma) =$$

$$= \varphi(a) - \sum_{\sigma \text{ обр.}} \psi(\sigma) = \sum_{\sigma \text{ обр.}} (1 - \psi(\sigma)).$$

Сумма $\sum \psi(\sigma)$, взятая по всем образующим группы A, является целым алгебраическим числом, которое к тому же рационально (по ряду элементарных соображений). Далее, если ψ нетривиален, вещественные части всех чисел $1 - \psi(\sigma)$ положительны, когда σ не есть единичный элемент, и равны нулю в противном случае. Тем самым рассматриваемая сумма является целым положительным числом. Для тривиального характера ψ она, очевидно, равна нулю. Предложение доказано.

Глава X

ЯВНЫЕ ФОРМУЛЫ

Мы следуем изложению Вейля [10]. Отметим, что логическая структура доказательств чрезвычайно проста. Используются только следующие результаты арифметического происхождения.

Ограниченность величины $|L(s)|$ в каждой полуплоскости $\mathrm{Re}(s) \geqslant 1 + a$, $a > 0$.

Функциональное уравнение для функции $\Lambda(s)$.

Ограниченность функции $\Lambda(s)$ в любой полосе $\sigma_0 \leqslant \sigma \leqslant \sigma_1$ с исключенными окрестностями полюсов. Это следует из обычных интегральных представлений.

Остальные рассуждения имеют аналитический характер. В частности, мы постоянно пользуемся формулой Стирлинга, описывающей асимптотическое поведение гамма-функции. Следует отметить, что нам приходится оценивать ряд преобразований Фурье и некоторые определенные интегралы.

Основной результат состоит в том, что сумма значений некоторой функции на степенях простых идеалов, по существу, совпадает с суммой значений ее преобразования Меллина в нулях дзета-функции. Точная формулировка содержится в § 3.

Одна часть доказательства основана на технике преобразований Фурье распределений. Я обязан Л. Шварцу за те соображения, которые используются в доказательстве предложения 4, § 5 (изложение Вейля в соответствующем месте настолько сжато, что его ход едва ли можно проследить).

Читателю, который захочет поупражняться, мы советуем обобщить теоремы из книги [12] на случай L-рядов с произвольным характером Гекке.

§ 1. Вейерштрассово разложение L-ряда

В этой главе мы будем постоянно пользоваться результатами гл. VII, § 8. Пусть k — числовое поле, χ — характер группы классов иделей, $d_\chi = \mathbf{N}(\mathfrak{D}\mathfrak{f}_\chi)$. Положим $A = 2^{-2r_2}\pi^{-N}d_\chi$ и

$$G_0(s, \chi) = A^{s/2} = G_0(s, \bar{\chi}),$$

$$G_v(s, \chi) = \Gamma(s_0/2) \text{ (для архимедовых } v),$$

где $s_v = s_v(\chi) = \frac{1}{2}(N_v(s + i\varphi_v) + |m_v|)$. Далее, символом $L(s, \chi)$ обозначается произведение обычных множителей по всем $\mathfrak{p}$, относительно которых χ неразветвлен.

Функция

$$\Lambda(s, \chi) = G_0(s, \chi)\,\Pi G_v(s, \chi)\,L(s, \chi) = \Lambda(s)$$

удовлетворяет функциональному уравнению вида

$$W(\chi)\Lambda(s, \chi) = \Lambda(1 - s, \bar{\chi})$$

или

$$\Lambda(\bar{s}) = \overline{\Lambda(1 - s)}\,u(\chi),$$

где числа $W(\chi)$ и $u(\chi)$ по абсолютной величине равны 1.

Как обычно, символ δ_χ означает 1 для $\chi = \chi_0$ и 0 — в остальных случаях.

Мы хотим доказать, что

$$[s(s-1)]^{\delta_\chi}\Lambda(s)$$

является целой функцией порядка 1 и потому, по стандартной общей теореме теории функций комплексной переменной, разлагается в произведение вида

$$\Lambda(s) = ae^{bs}[s(s-1)]^{-\delta_\chi}\prod_\omega\left(1 - \frac{s}{\omega}\right)e^{s/\omega},$$

где ω пробегает все нули функции $\Lambda(s)$ с их кратностями, а a и b — константы.

Нам придется оценивать гамма-множители с помощью формулы Стирлинга

$$\log\Gamma(s)=\left(s-\frac{1}{2}\right)\log s-s+\frac{1}{2}\log 2\pi+\int_0^\infty\frac{P_1(x)}{s+x}\,dx,$$

где

$$P_1(x)=[x]-x+\frac{1}{2}$$

— пилообразная функция. Интегральный член допускает оценку $O(1/|s|)$ равномерно в любом секторе вида

$$-\pi+\delta\leqslant\arg s\leqslant\pi-\delta,\qquad\delta>0.$$

Следовательно, для любого фиксированного комплексного числа a в таком секторе имеет место равномерная асимптотическая формула

$$\log\Gamma(s+a)=\left(s+a-\frac{1}{2}\right)\log s-s+\frac{1}{2}\log 2\pi+O(1/|s|).$$

В частности, если a вещественно, полагая $r=|s|$ и $\theta=\arg s$, находим, что

$$|\Gamma(s+a)|=r^{\sigma+a-1/2}e^{-t\theta}e^{-\sigma}(2\pi)^{1/2}e^{O(1/r)}$$

равномерно в описанном секторе. Аналогично для вещественных a и φ имеем

$$|\Gamma(s+a+i\varphi)|=r^{\sigma+a-1/2}e^{-t\theta-\varphi\theta}e^{-\sigma}(2\pi)^{1/2}e^{O(1/r)}.$$

Обозначим символом $G(s)$ произведение множителей G_v и G_0, т. е., по существу, гамма-множителей. Очевидно, что $|G(s)|=O(e^{|s|^{1+\varepsilon}})$ для любого $\varepsilon>0$ в полуплоскости $\sigma\geqslant 1$. Далее, из представления $L(s)$ в виде произведения ясно, что эта функция ограничена в полуплоскости $\sigma\geqslant 1+a$ при любом вещественном $a>0$. Следовательно, $\Lambda(s)=O(e^{|s|^{1+\varepsilon}})$ в такой полуплоскости.

Функциональное уравнение дает такую же оценку в полуплоскости $\sigma\leqslant -a$.

С другой стороны, представление $\Lambda(s)$ в виде суммы двух интегралов, сходящихся при всех s, и члена, описывающего полюсы в точках $s(s-1)$, показывает, что эта функция ограничена в каждой полосе $\sigma_0\leqslant\sigma\leqslant\sigma_1$, за исклю-

чением окрестностей полюсов $s=0$, 1, когда они имеются, т. е. при $\chi=\chi_0$. Мы покажем тем самым, что требуемая оценка имеет место при всех s, за исключением таких окрестностей, и, значит, порядок функции $\Lambda(s)$ равен 1.

§ 2. Оценка функции Λ'/Λ

Нам понадобятся две леммы из теории функций комплексной переменной.

Лемма 1. *Пусть функция $f(s)$ голоморфна в полуполосе $\sigma_0\leqslant\sigma\leqslant\sigma_1$, $t\geqslant t_1>0$. Пусть для нее при $t\to\infty$ в этой области справедлива оценка $O(e^{ct})$, где $c>0$ — некоторая константа, а на краях $\sigma=\sigma_0$ и $\sigma=\sigma_1$ — оценка $|f(s)|=O(t^M)$, где M — некоторое положительное целое число. Тогда оценка $f(s)=O(t^M)$ имеет место во всей области.*

Доказательство. Рассматривая функцию $f(s)/s^M$ вместо $f(s)$, мы можем считать, что f ограничена на краях полуполосы. Докажем, что тогда она ограничена во всей полуполосе. В самом деле, рассмотрим функцию $g(s)=f(s)e^{i\varepsilon s^\lambda}$ для некоторого $\lambda=1+\delta$, где $\delta>0$ достаточно мало. Тогда при больших t имеем

$$|g(s)|\leqslant Be^{ct-\varepsilon t^\lambda\sin\lambda\theta},$$

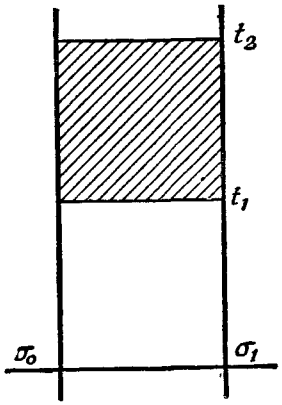
где B — некоторая константа, а $\theta=\arg s$. Следовательно, функция $g(s)$ ограничена константой B на горизонтальном отрезке $t=t_2$ (для достаточно больших t_2) между краями полуполосы $\sigma=\sigma_1$ и $\sigma=\sigma_2$.

На вертикальных сторонах прямоугольника, затененного на чертеже, функция $g(s)$ ограничена, потому что $f(s)$ ограничена и $e^{-\varepsilon t^\lambda\sin\lambda\theta}\leqslant 1$. Из ограниченности функции $g(s)$ на границе прямоугольника следует ее ограниченность во всем прямоугольнике; на самом деле оценка $|g(s)|\leqslant B$ годится и для внутренних точек. Поэтому, снова полагая $r=|s|$, имеем

$$|f(s)|\leqslant B|e^{-i\varepsilon s^\lambda}|\leqslant Be^{\varepsilon r^\lambda\sin\lambda\theta}$$

внутри прямоугольника. Так как эта оценка годится при всех $\varepsilon > 0$, то $|f(s)| \leqslant B$ внутри прямоугольника, что и дает требуемое.

Доказанная лемма известна под названием теоремы Фрагмена — Линделефа.



Лемма 2. *Пусть функция $f(z)$ голоморфна в круге $|z-z_0| \leqslant R$ и имеет по крайней мере n нулей в круге $|z-z_0| \leqslant r < R$ (считая каждый нуль столько раз, какова его кратность).*

Пусть, кроме того, $f(z_0) \neq 0$. Тогда

$$[(R-r)/r]^n \leqslant B/|f(z_0)|,$$

где B — максимум модуля $|f(z)|$ в большом круге.

Доказательство. Можно считать, что $z_0 = 0$. Пусть

$$f(z) = \prod_{i=1}^{n} (z-a_i)\,\varphi(z),$$

где a_i — нули функции f в меньшем круге. Тогда в большом круге, очевидно,

$$|\varphi(z)| \leqslant |f(z)|/(R-r)^n \leqslant B/(R-r)^n.$$

Так как $|a_i| \leqslant r$ при всех i, то требуемое неравенство получается отсюда, если положить $z = 0$.

Вернемся к L-рядам. Положим

$$L_1(s) = s(s-1)L(s).$$

Рассмотрим полосу $\sigma_0 < 0 < 1 < \sigma_1$. *Мы утверждаем, что для некоторого целого числа M в этой полосе имеет место оценка* $L_1(s) = O(|t|^M)$.

Для доказательства заметим, что

$$|L_1(s)| = |s(s-1)L(s)| = |s(s-1)G(s)^{-1}G(1-\bar{s})L(1-\bar{s})|$$

в силу функционального уравнения. Внутри полосы функция $\Lambda(s)$ ограничена, это следует из ее интегрального представления. С помощью асимптотики для гамма-функции отсюда следует, что внутри полосы $L_1(s) = O(e^{c|t|})$, где c — некоторая константа. Далее, при $\sigma = \sigma_1$ функция $L(s)$ ограничена; это видно из ее представления в виде произведения. То же верно для $L(1-\bar{s})$ при $\sigma = \sigma_0$ в силу функционального уравнения. Пусть a, b — фиксированные комплексные числа; из результатов § 1 следует, что $|\Gamma(s+a)/\Gamma(b-\bar{s})| = O(|t|^M)$ (для некоторого M, зависящего от a, b) внутри полосы (ибо множители вида $e^{-t\theta}$ сокращаются). Собирая вместе все эти оценки, получаем, что $L_1(s) = O(|t|^M)$ на краях $\sigma = \sigma_0$ и $\sigma = \sigma_1$, если M достаточно велико. Требуемый результат теперь следует из леммы 1.

Применяя лемму 2 к паре кругов постоянных радиусов с центром $1+a+it$ при фиксированном $a > 0$, получаем

Предложение 1. *Число нулей функции $\Lambda(s)$ (совпадающее с числом нулей функции $L(s)$) в прямоугольнике $0 \leqslant \sigma \leqslant 1$ и $T \leqslant |t| \leqslant T+1$ оценивается как $O(\log T)$.*

Следствие. *Существуют такое число α и такая последовательность чисел T_m, $m < T_m < m+1$, $|m| \geqslant 2$, что у функции $\Lambda(s)$ нет нулей ни в одной горизонтальной полосе вида*

$$|t - T_m| \leqslant \frac{\alpha}{\log|m|}.$$

Вернемся к разложению Вейерштрасса. Вычисляя разность его логарифмических производных в двух точках

s, s_0, находим

$$\Lambda'/\Lambda(s)-\Lambda'/\Lambda(s_0)=$$
$$=\sum_{\omega}\left(\frac{1}{s-\omega}-\frac{1}{s_0-\omega}\right)-\delta_\chi\left(\frac{1}{s}+\frac{1}{s-1}-\frac{1}{s_0}-\frac{1}{s_0-1}\right).$$

Предложение 2. *Пусть* $0<a\leqslant 1$, m — *целое число*, $|m|\geqslant 2$. *Пусть* $s=\sigma+iT_m$, *где* $-a\leqslant\sigma\leqslant 1+a$, *а число* T_m *выбрано, как выше. Тогда*

$$|\Lambda'/\Lambda(s)|\leqslant B(\log|m|)^2,$$

где константа B *зависит от* a, *но не зависит от* m *и* σ.

Доказательство. Положим $s_0=1+a+iT_m$ и $\omega=\beta+i\gamma$.

Имеем

$$|\Lambda'/\Lambda(s)-\Lambda'/\Lambda(s_0)|\leqslant\sum_{\omega}\left|\frac{s_0-s}{(s-\omega)(s_0-\omega)}\right|+B_1,$$

где B_1 — константа, оценивающая выражение справа от символа δ_χ. Сумма оценивается так:

$$\sum_{\omega}\left|\frac{s_0-s}{(s-\omega)(s_0-\omega)}\right|\leqslant(a+1-\sigma)\sum_{\omega}\frac{1}{|(s-\omega)(s_0-\omega)|}.$$

При наших предположениях

$$|s_0-\omega|^2=(1+a-\beta)^2+(T_m-\gamma)^2\geqslant a^2+(T_m-\gamma)^2.$$

С другой стороны, полагая $b=a/\log|m|$ (можно считать, что $b\leqslant 1$), находим

$$|s-\omega|^2\geqslant(T_m-\gamma)^2\geqslant\frac{1}{2}(T_m-\gamma)^2+\frac{1}{2}b^2\geqslant$$
$$\geqslant\frac{1}{2}b^2[a^2+(T_m-\gamma)^2],$$

потому что $0<a\leqslant 1$. Следовательно,

$$|\Lambda'/\Lambda(s)-\Lambda'/\Lambda(s_0)|\leqslant B_1+\frac{2(a+1-\sigma)}{b}\sum_{\omega}\frac{1}{a^2+(T_m-\gamma)^2}.$$

Кроме того,

$$\sum_{\omega} \frac{1}{a^2+(T_m-\gamma)^2} \leqslant \frac{(a+1)^2}{a^2} \sum_{\omega} \frac{1}{(a+1)^2+(T_m-\gamma)^2}.$$

Мы сравним это выражение с оценкой для $\mathrm{Re}\,(\Lambda'/\Lambda(s_0))$ и учтем, что $\mathrm{Re}\,(\Lambda'/\Lambda(s_0)) \leqslant |\Lambda'/\Lambda(s_0)|$.

Имеем

$$\Lambda'/\Lambda(s_0) = b + \sum_{\omega} \left[\frac{1}{s_0-\omega} + \frac{1}{\omega}\right] - \delta_\chi \left(\frac{1}{s_0} + \frac{1}{s_0-1}\right).$$

Вещественная часть средней суммы равна

$$\sum_{\omega} \left[\frac{1+a-\beta}{(1+a-\beta)^2+(T_m-\gamma)^2} + \frac{\beta}{\beta^2+\gamma^2}\right],$$

и потому она не меньше

$$\sum_{\omega} \frac{a}{(1+a)^2+(T_m-\gamma)^2}.$$

Из этой оценки требуемый результат получается немедленно с помощью следующего утверждения.

Предложение 3. *Пусть* $a>0$. *Функция* $L'/L(s)$ *ограничена на прямой* $\mathrm{Re}\,(s) = 1+a$; *кроме того,*

$$\Gamma'/\Gamma(s) = \log s + O(1/|s|^2),$$

когда $\mathrm{Re}\,(s) = 1+a$ *и* $|s| \to \infty$.

Доказательство. Первое утверждение следует из представления L-функции в виде произведения, а второе — из формулы Стирлинга (производная от интеграла дает остаточный член).

§ 3. Основная сумма

Пусть $F(x)$ — комплекснозначная функция на вещественной прямой, для которой существует такая константа $a'>0$, что функция

$$F(x)\, e^{(1/2+a')|x|}$$

принадлежит пространству $\mathfrak{L}_1$. Тогда преобразование Меллина

$$\Phi(s)=\int_{-\infty}^{+\infty} F(x)\, e^{(s-1/2)x}\, dx$$

представляет собой функцию, голоморфную в любой полосе $-a\leqslant\sigma\leqslant 1+a$, где $0<a<a'$. Для начала мы предположим, кроме того, что в каждой такой полосе имеет место равномерная оценка $\Phi(s)=o\,(1/(\log|t|)^2$ (позже мы усилим требования). 74

Пусть $T>2$. Количество нулей функции $\Lambda(s)$, мнимая часть которых лежит между T и ближайшим числом T_m (см. предыдущий параграф), оценивается как $O(\log T)$; то же относится к количеству нулей между $-T$ и ближайшим числом T_l. Сумма $\Sigma\Phi(\omega)$ по этим нулям стремится к нулю, когда $T\to\infty$.

Рассмотрим интеграл от функции $\Phi(s)\,d\log\Lambda(s)$ по прямоугольнику, ограниченному прямыми $\sigma=-a$, $\sigma=1+a$, $t=T_m$, $t=T_l$. В силу предложения 2 интеграл по горизонтальным сторонам стремится к нулю при $T\to\infty$, это следует из условий, наложенных на Φ. Обозначая через $o(1)$ аддитивную группу функций от T, стремящихся к нулю, когда $1/T\to 0$, в силу формулы вычетов получаем следующие сравнения $\bmod o(1)$:

$$-\delta_\chi[\Phi(0)+\Phi(1)]+\sum_{-T<\gamma<T}\Phi(\omega)\equiv$$

$$\equiv\frac{1}{2\pi i}\int\limits_{\substack{\text{граница}\\ \text{прямоугольника}}}\Phi(s)\,d\log\Lambda(s)\equiv$$

$$\equiv\frac{1}{2\pi i}\int_{1+a+iT_l}^{1+a+iT_m}\Phi(s)\,d\log\Lambda(s)-\frac{1}{2\pi i}\int_{-a+iT_l}^{-a+iT_m}\Phi(s)\,d\log\Lambda(s)\equiv$$

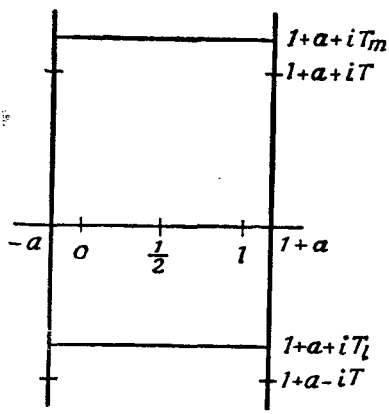
$$\equiv\frac{1}{2\pi i}\int_{1+a+iT_l}^{1+a+iT_m}\Phi(s)\,d\log\Lambda(s)-$$

$$-\frac{1}{2\pi i}\int_{-a+iT_l}^{-a+iT_m}\Phi(s)\,d\log\Lambda(1-s,\ \chi^{-1})\equiv$$

$$\equiv \frac{1}{2\pi i}\int_{1+a-iT}^{1+a+iT} \Phi(s)\, d\log \Lambda(s) +$$

$$+ \frac{1}{2\pi i}\int_{-a+iT}^{-a-iT} \Phi(s)\, d\log \Lambda(1-s,\ \chi^{-1}).$$

На последнем шаге мы пользуемся оценкой предложения 3, из которой следует, что интегралы по $(T_m,\ T)$ и $(T_l,\ -T)$ стремятся к нулю при $T \to \infty$.



Чтобы оценить получившиеся интегралы, мы воспользуемся представлением Λ в виде произведения. Получатся три типа интегралов, соответствующих множителям G_0, G_v и L. Далее, мы примем, что функция F удовлетворяет следующим дополнительным условиям:

(A) F непрерывна вместе со своей производной всюду, кроме конечного числа точек α_i, где $F(x)$ и производная $F'(x)$ имеют разрывы только первого рода, причем

$$F(\alpha_i) = \frac{1}{2}[F(\alpha_i + 0) + F(\alpha_i - 0)].$$

(Б) Для некоторого числа $b>0$ имеют место оценки вида

$$F(x)=O(e^{-(1/2+b)|x|}),$$
$$F'(x)=O(e^{-(1/2+b)|x|})$$

при $|x|\to\infty$.

Из этих условий следует, что $\Phi(s)=O(|t|^{-1})$ равномерно в полосе $-a'\leqslant\sigma\leqslant 1+a'$, если $0<a'<b$. Поэтому приведенный выше подсчет применим, если $0<a<a'<b$ и $a\leqslant 1$.

Интегралы по прямым $\sigma=1+a$ и $\sigma=-a$ мы сведем к интегралам по прямой $\sigma=1/2$. Нашим окончательным результатом будет следующая

Явная формула. *Пусть функция $F(x)$ удовлетворяет условиям* (А) *и* (Б); *пусть Φ — преобразование Мелина функции F. Сумма $\sum\Phi(\omega)$, распространенная на все нули $\omega=\beta+i\gamma$ функции $L(s)$, удовлетворяющие условиям $0\leqslant\beta\leqslant 1$ и $|\gamma|<T$, стремится к некоторому пределу при $T\to\infty$, и этот предел равен*

$$\lim_{T\to\infty}\sum_{|\gamma|<T}\Phi(\omega)=\delta_\chi\int_{-\infty}^{\infty}F(x)(e^{x/2}+e^{-x/2})\,dx+F(0)\log A-$$
$$-\sum_{\mathfrak{p},\,n}\frac{\log N\mathfrak{p}}{N\mathfrak{p}^{n/2}}[\chi(\mathfrak{p})^n F(\log N\mathfrak{p}^n)+\chi(\mathfrak{p})^{-n}F(\log N\mathfrak{p}^{-n})]+$$
$$+\sum_{v\in S_\infty}\frac{N_v}{2\pi}\hat{\Psi}_v(F_v),$$

где $F_v(x)=F(x)e^{-i\varphi_v x}$, а $\hat{\Psi}_v$ — функционал, который будет описан в § 5.

Если в качестве F взять функцию

$$F(x)=\begin{cases}0 & \text{при } x<0 \text{ и } x>\log y,\\ e^{x/2} & \text{при } 0<x<\log y,\end{cases}$$

где $y>1$ — некоторое фиксированное число, получится классическая формула ([12], гл. IV). Точную формулировку результата оставляем читателю. Отметим, что условия (А) и (Б) в этом случае, очевидно, удовлетворяются, а в сумме по $\mathfrak{p},n$ остаются только члены с положительными n.

§ 4. Вычисление суммы: первая часть

В нашей явной формуле интеграл (с множителем δ_χ) появляется очевидным образом как сумма $\Phi(0)+\Phi(1)$.

Для того чтобы получить остальные слагаемые, воспользуемся тождеством

$$d\log\Lambda = d\log G_0 + d\log L + \sum_{v\in S_\infty} d\log G_v$$

и вычислим соответствующие интегралы отдельно для каждого из трех слагаемых.

Начнем с G_0. Имеем

$$\frac{d}{ds}\log G_0(s) = \frac{1}{2}\log A, \quad \frac{d}{ds}\log G_0(1-s) = -\frac{1}{2}\log A.$$

Поскольку мы интегрируем голоморфную функцию, контур интегрирования можно сдвинуть на прямую $\sigma = 1/2$ и объединить оба интеграла в один

$$\frac{\log A}{2\pi i}\int_{1/2-iT}^{1/2+iT}\Phi(s)\,ds.$$

Сделаем подстановку $s = 1/2+it$, $ds = idt$ и перейдем к пределу при $T\to\infty$. Формула обращения Фурье применима в данном случае, поэтому пределом будет величина $F(0)\log A$, что и требовалось.

Теперь проинтегрируем $d\log L$. Начнем с интеграла по прямой $\sigma = 1+a$. Тривиальный подсчет приводит к выражению

$$\frac{-1}{2\pi}\int_{-T}^{+T} dt \sum{}' \int_{-\infty}^{\infty} H^+_{\mathfrak{p},\,n}(u)\,e^{itu}du,$$

где

$$H^+_{\mathfrak{p},\,n}(u) = \frac{\log \mathbf{N}\mathfrak{p}}{\mathbf{N}\mathfrak{p}^{n/2}}\chi(\mathfrak{p})^n F(u+\log \mathbf{N}\mathfrak{p}^n)\,e^{(1/2+a)u}.$$

Пользуясь существованием такой константы C, что

$$|F(x)| \leqslant Ce^{-(1/2+b)|x|},$$

находим

$$|H^+_{\mathfrak{p},\,n}(u)| \leqslant \frac{2C\log \mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^{n(1+a)}}.$$

Эта оценка показывает, что ряд $\sum H^+_{\mathfrak{p},\,n}(u)$ сходится абсолютно и равномерно и определяет некоторую функцию $H^+(u)$, принадлежащую пространству $\mathfrak{L}_1$.

Подобное же вычисление для интеграла по прямой $\sigma=-a$ и оценка для функции

$$H^-_{\mathfrak{p},\,n}(u) = \frac{\log \mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^{n/2}}\,\chi(\mathfrak{p})^{-n}F(u-\log \mathrm{N}\mathfrak{p}^n)\,e^{-(1/2+a)u}$$

приводят к аналогичному ряду. Положим $H_{\mathfrak{p},\,n}(u) = H^+_{\mathfrak{p},\,n}(u)+H^-_{\mathfrak{p},\,n}(u)$. Меняя местами суммирование и интегрирование, находим, что сумма интегралов от $d\log L$ равна

$$\frac{-1}{2\pi}\int_{-T}^{+T} dt \int_{-\infty}^{\infty} H(u)\,e^{it\,u}\,du.$$

Функция $H(u)$ непрерывна вместе со своей производной всюду, кроме точек $\alpha_i \pm \log \mathrm{N}\mathfrak{p}^n$, где у нее и у ее производной имеются разрывы первого рода (напомним, что количество таких чисел α_i конечно). Так как, кроме того, в точках разрыва значение функции $H(u)$ равно полусумме ее предельных значений, то можно применить формулу обращения Фурье, так что при $T\to\infty$ наш интеграл стремится к пределу $-H(0)$. Так появляется сумма по $\mathfrak{p},n$ в правой части явной формулы.

§ 5. Вычисление суммы: вторая часть

Переходим к последнему члену. Для каждого v мы должны вычислить интеграл от $d\log G_v$. Отметим, что у функции G_v'/G_v нет полюсов в полуплоскости $\sigma>0$ и что для нее имеет место оценка $O(\log|t|)$ в любой полосе с вырезанными окрестностями полюсов. Следовательно, интеграл от $1+a-iT$ до $1+a+iT$ отличается от интеграла от $1/2-iT$ до $1/2+iT$ на $o(1)$. Подобным же рассуждением, заменяя s на $1-s$, мы можем превратить

интеграл по прямой $\sigma = -a$ в интеграл по прямой $\sigma = 1/2$. Получаем

$$(1)\quad \frac{1}{2\pi i}\int_{1/2-iT}^{1/2+iT} \Phi(s)\,[d\log G_v(s,\ \chi) - d\log G_v(1-s,\ \chi^{-1})].$$

Подставляя сюда формулы, определяющие G_v, находим, что интеграл (1) равен

$$\frac{N_v/2}{2\pi i}\int_{1/2-iT}^{1/2+iT} \Phi(s)\left[\Gamma'/\Gamma\left(\frac{N_v(s+i\varphi_v)+|m_v|}{2}\right)+\right.$$
$$\left.+\Gamma'/\Gamma\left(\frac{N_v(1-s-i\varphi_v)+|m_v|}{2}\right)\right]ds.$$

Произведем замену переменных: полагая $s = 1/2 + it - i\varphi_v$, $ds = idt$, получаем

$$(2)\quad \frac{N_v/2}{2\pi i}\int_{-T}^{+T} \Phi\left(\frac{1}{2}+it-i\varphi_v\right)[\Gamma'/\Gamma(z)+\Gamma'/\Gamma(\bar{z})]\,dt,$$

где $z = (N_v(1/2+it)+|m_v|)/2$.

Положим

$$\psi_v(t) = \Phi\left(\frac{1}{2}+it-i\varphi_v\right)$$

и

$$F_v(x) = F(x)\,e^{-i\varphi_v x}.$$

С помощью обычной замены переменной находим

$$\psi_v(t) = \int_{-\infty}^{\infty} F_v(x)\,e^{itx}dx,$$

причем функция F_v удовлетворяет условиям (А) и (Б). Определим функцию

$$\text{Ч}(t) = \operatorname{Re}\Gamma'/\Gamma\left(\frac{N_v\left(\frac{1}{2}+it\right)+|m_v|}{2}\right).$$

Последний интеграл (2) можно тогда представить в виде

$$(3)\quad \frac{N_v}{2\pi}\int_{-T}^{T} \psi_0(t)\,\text{Ч}_v(t)\,dt.$$

Функция $\psi_v(t)$ при $|t| \to \infty$ допускает оценку $O(1/|t|)$, поэтому она принадлежит пространству $\mathfrak{L}_2$. Из формулы Стирлинга следует, что

$$\text{Ч}_v(t) = \log|t| + g_v(t),$$

где $g_v \in \mathfrak{L}_2$. Следовательно, мы не можем ни непосредственно применить формулу Планшереля, ни рассмотреть интеграл от $-\infty$ до $+\infty$ без специального доказательства сходимости. Поэтому наша задача состоит в оправдании обобщенной формулы Планшереля в интересующем нас случае.

В конце концов мы докажем существование предела

$$\lim_{T\to\infty} \int_{-T}^{T} \psi_v(t)\, \text{Ч}_v(t)\, dt.$$

Для этого нам понадобятся некоторые результаты из функционального анализа.

Условимся на будущее, что

$$\int_{-\infty}^{\infty} = \lim_{T\to\infty} \int_{-T}^{+T}.$$

Мы будем впредь ссылаться на книгу Шварца [13].

Рассмотрим линейное пространство тех функций на вещественной прямой, которые ограничены, непрерывны и удовлетворяют некоторому условию Липшица равномерно на всяком компактном подмножестве. Это пространство мы назовем пространством ОНЛ-функций.

Линейное пространство, порожденное этими функциями и характеристическими функциями всевозможных интервалов, концы которых отличны от 0, назовем пространством *почти* ОНЛ-функций. Все такие функции непрерывны в нуле.

Определим функционал W на пространстве почти ОНЛ-функций, полагая

$$W(\beta) = \lim_{\lambda\to\infty} \left[\int_{-\infty}^{\infty} \frac{1 - e^{-\lambda|x|}}{|e^{x/2} - e^{-x/2}|} \beta(x)\, dx - 2\beta(0) \log \lambda \right].$$

Разумеется, мы должны оправдать это определение.

Лемма 3. *На пространстве почти* ОНЛ-*функций описанный предел существует.*

Доказательство. В окрестности нуля знаменатель

$$|e^{x/2} - e^{-x/2}|$$

ведет себя, как $|x| \pmod{x^2}$. Поэтому достаточно доказать наше утверждение, заменив этот знаменатель на $|x|$, а β — на функцию, быстро стремящуюся к нулю при $x \to \infty$.

Начнем с рассмотрения характеристической функции интервала. Если точка 0 не лежит в этом интервале, то предел, очевидно, существует. В противном случае мы приходим к необходимости рассмотреть интеграл вида

$$\varphi(\lambda) = \int_0^b \frac{1 - e^{-\lambda x}}{x}\, dx, \quad b > 0, \quad \lambda \geqslant 1.$$

Мы можем дифференцировать под знаком интеграла; считая для простоты, что $b = 1$, имеем

$$\varphi'(\lambda) = \frac{1}{\lambda} - \frac{e^{-\lambda}}{\lambda}.$$

Поэтому $\varphi(\lambda) = \log \lambda +$ интеграл, сходящийся к некоторому пределу при $\lambda \to \infty$. Отсюда следует, что член $2\beta(0) \log \lambda$ уничтожает расходимость.

Пусть теперь β — ОНЛ-функция, быстро стремящаяся к нулю на бесконечности. Она представляется в виде суммы четной и нечетной функций; можно ограничиться рассмотрением четных функций, которые в нуле обращаются в нуль (достаточно вычесть характеристическую функцию интервала с центром в нуле). Тогда функция $\beta(x)/|x|$ ограничена в некоторой окрестности начала, так что интеграл

$$\int_{-\infty}^{\infty} (1 - e^{-\lambda |x|}) \frac{\beta(x)}{|x|}\, dx$$

стремится к некоторому пределу при $\lambda \to \infty$. Далее, член $2\beta(0) \log \lambda$ равен нулю, так что наше утверждение в этом случае справедливо.

Пусть теперь β — произвольная ОНЛ-функция. Имеем

$$\beta(x) = \beta(x) - \beta(0) + \beta(0),$$

откуда по линейности получаем

$$W(\beta) = \beta(0)\, W(1) + \int_{-\infty}^{\infty} \frac{\beta(x) - \beta(0)}{|e^{x/2} + e^{-x/2}|}\, dx.$$

Сходимость последнего интеграла очевидна. Остюда следует

Лемма 4. *Для любой* ОНЛ-*функции* β *имеем*

$$|W(\beta)| \leqslant C(|\beta| + \operatorname{lip}_1 \beta),$$

где C — *фиксированная константа, а* $\operatorname{lip}_1 \beta$ — *константа Липшица для некоторого компактного интервала, содержащего нуль.*

Пользуясь этой леммой, мы можем установить некоторое свойство непрерывности функционала W.

Лемма 5. *Пусть* $\{\beta_n\}$ — *последовательность* ОНЛ-*функций, сходящаяся к некоторой* ОНЛ-*функции* β. *Предположим, что функции* $\{\beta_n\}$ *равномерно ограничены и что на каждом компактном множестве сходимость равномерна, а константы Липшица функций* β_n *равномерно ограничены. Тогда* $W(\beta_n)$ *сходится к* $W(\beta)$.

Доказательство. Для каждого n имеем

$$\beta_n(x) = \beta_n(x) - \beta_n(0) + \beta_n(0).$$

Последовательность $\beta_n(0)$ сходится к $\beta(0)$. Доказательство тем самым сводится к рассмотрению суммы интегралов

$$\int \frac{\beta_n(x) - \beta_n(0)}{|e^{x/2} - e^{-x/2}|}\, dx$$

по отрезкам

$$A \leqslant |x|,$$

$$\varepsilon \leqslant |x| \leqslant A,$$

$$|x| \leqslant \varepsilon,$$

где $\varepsilon > 0$ достаточно мало, а A велико. При больших A первый интеграл мал из-за экспоненты в знаменателе. При малых ε последний интеграл мал из-за существования равномерной оценки для констант Липшица. Средний интеграл тогда близок к соответствующему интегралу от функции $\beta(x) - \beta(0)$. Лемма доказана.

Для любой ОНЛ-функции β и для любого числа y обозначим символом β_y функцию $\beta_y(x) = \beta(x+y)$. Из вышесказанного следует, что $W(\beta_y)$ как функция от y непрерывна.

Пусть $\{\varrho_n\}$ — некоторая последовательность регуляризующих функций, т. е. бесконечно дифференцируемых неотрицательных функций с компактным носителем, стягивающимся к нулю; интеграл от каждой функции равен 1. Легко проверяется, что последовательность сверток $\{\beta * \varrho_n\}$ сходится к β и условия леммы 5 выполнены.

Для любой функции β символом β^- обозначим функцию

$$\beta^-(y) = \beta(-y).$$

Имеет место

Лемма 6. *Пусть $\{\varrho_n\}$ — некоторое регуляризующее семейство. Тогда последовательность функций $W((\beta * \varrho_n)^-_x)$ сходится к $W(\beta^-_x)$ равномерно на всяком компактном множестве.*

Отсюда вытекает

Лемма 7. *Функционал W является распределением. Пусть β — некоторая ОНЛ-функция. Свертка W и T_β (распределение, представленное функцией β) представляется функцией, значение которой в точке x равно $W(\beta^-_x)$; в символической записи*

$$(W * T_\beta)(x) = W(\beta^-_x).$$

Эта функция непрерывна.

Доказательство. Пусть T — распределение, представленное вне некоторого компактного множества функцией, которая экспоненциально стремится к нулю на бесконечности, а α — некоторая ограниченная C^∞-функция. Теория распределений устанавливает, что в этом случае распределение

$$T * T_\alpha$$

представлено функцией $T(\alpha_{\bar{x}})$. Этот результат можно применить к функциям $\beta * \varrho_n$, что доказывает нашу лемму (см. [13], теорема XI гл. VI, § 4, и формула (VI, 1; 2)).

Теперь сформулируем аналог леммы 7 для почти ОНЛ-функций.

Лемма 8. *Пусть χ — характеристическая функция интервала, ни один из концов которого не является нулем. Тогда распределение $W * T_\chi$ представлено некоторой C^∞-функцией в окрестности каждой точки, за исключением концов интервала. Значение этой функции в такой точке x равно $W(\chi_{\bar{x}})$.*

Доказательство. Это следует из общих свойств свертки распределений (см., например, [13], гл. VI, теорема III, § 3, и теорема XI, § 4).

Следствие. *Пусть F — почти* ОНЛ-*функция, непрерывная в нуле. Тогда распределение $W * T_F$ представлено некоторой C^∞-функцией в окрестности любой точки непрерывности функции F; ее значение в нуле равно*

$$W(F^-).$$

Перейдем теперь к рассмотрению некоторых специальных свойств гамма-функции.

Из ее вейерштрассова разложения следует формула

$$\Gamma'/\Gamma(z) = -\frac{1}{z} - \gamma + \sum_{n=1}^{\infty} \left[\frac{1}{n} - \frac{1}{n+z} \right]$$

(см. любой учебник). Положим $z = 1/2 + it$ и рассмотрим вещественные части, учитывая, что

$$\gamma = \lim_{M \to \infty} \left(1 + \ldots + \frac{1}{M} - \log M \right).$$

Отсюда получаем

$$\text{Ч}(t) = \lim_{M \to \infty} \left[\log M - \sum_{n=0}^{M} \frac{n + \frac{1}{2}}{\left(n + \frac{1}{2}\right)^2 + t^2} \right] = \lim_{M \to \infty} \text{Ч}_M(t),$$

где символом Ч_M обозначена функция в квадратных скобках.

Лемма 9. *Сходимость к предельной функции равномерна на каждом компактном множестве. Кроме того,*

$$|\text{Ч}_M(t)| \leqslant C \log |t|$$

при всех $|t| \geqslant 2$, *где* C — *некоторая константа, не зависящая от* M.

Доказательство. Первое утверждение очевидно. Для доказательства второго заметим, что общий член суммы в выражении для Ч_M ограничен снизу величиной

$$\frac{n+\frac{1}{2}}{\left(n+\frac{1}{2}\right)^2+t^2} \leqslant \frac{1}{n+\frac{1}{2}}.$$

Пусть $t > 0$. При $M \leqslant t$ функция Ч_M ограничена величиной $\log M \leqslant \log t$. При $M \geqslant t$ имеем

$$\sum_{n=0}^{M} \geqslant \sum_{n=t}^{M} \geqslant \log M - \log t - \text{const}.$$

Это снова дает требуемое.

С этого места и до конца параграфа условимся нормализовать преобразование Фурье следующим образом. Для подходящего класса функций f положим

$$\hat{f}(t) = \int_{-\infty}^{+\infty} f(x)\, e^{-itx}\, dx.$$

Символом $\langle\, ,\, \rangle$ условимся обозначать аналогичный интеграл от произведения функций, стоящих в скобках, когда он имеет смысл. Тогда *формулу Планшереля* для некоторого класса функций f, g можно записать в виде

$$\langle \hat{f}^-, g\rangle = \langle f, \hat{g}\rangle,$$

а формулу обращения Фурье —

$$\hat{\hat{f}} = 2\pi f^-.$$

Преобразованием Фурье функции f мы впредь называем функцию $\hat{f}$.

Преобразование Фурье функции

$$\frac{a}{a^2+t^2}$$

легко вычислить, интегрируя по полуокружности (верхней при $x<0$ и нижней при $x>0$). Поэтому, полагая

$$\text{Ч}_M = \log M + g_M,$$

находим

$$\hat{g}_M(x) = -\pi \frac{1-e^{-M|x|}}{|e^{x/2}-e^{-x/2}|}.$$

Преобразование Фурье постоянной функции 1 представляет собой распределение

$$\hat{1} = 2\pi\delta,$$

где δ — функционал $\delta(f) = f(0)$. Отсюда следует

Лемма 10. *Имеем*

$$T_{\text{Ч}} = \hat{\text{Ч}} = -\pi W$$

в смысле теории распределений.

Доказательство. Из условия ограниченности леммы 9 следует, что предел преобразований Фурье равен преобразованию Фурье предела (воспользоваться [13], пример 3 из гл. VII, § 7).

Нашей целью является доказательство следующего утверждения.

Предложение 4. *Пусть F — функция, удовлетворяющая условиям* (А) *и* (Б). *Положим*

$$\psi = \hat{F}^{-}.$$

Тогда число $\langle \psi, \text{Ч} \rangle$ *существует и равно*

$$\langle \psi, \text{Ч} \rangle = \lim_{M\to\infty} \langle F, \hat{\text{Ч}}_M \rangle,$$

т. е. в силу леммы 10 $\langle \psi, \text{Ч} \rangle = -\pi W(F)$.

Доказательство. Представление функции F в виде суммы четной и нечетной функций

$$F(x)=\frac{F(x)+F(-x)}{2}+\frac{F(x)-F(-x)}{2}$$

определяет подобное же представление преобразования Фурье. Поэтому достаточно проверить наше утверждение отдельно для четных и нечетных функций. Функция $Ч(t)$ четна; поэтому для нечетных F интеграл $\langle\psi, Ч\rangle$ обращается в нуль. Предел справа тоже равен нулю, потому что каждый член равен нулю, так что наше утверждение в этом случае тривиально.

Будем считать теперь, что F — четная функция; в частности, она непрерывна в нуле.

Мы докажем предложение 4 для более широкого класса функций. Именно, пусть функция F удовлетворяет следующим условиям:

(1) F — четная почти ОНЛ-функция;

(2) F принадлежит пространству $\mathfrak{L}_2$, дифференцируема всюду, кроме точек разрыва, и ее производная тоже принадлежит $\mathfrak{L}_2$.

Всякая четная функция, удовлетворяющая условиям (А) и (Б), удовлетворяет также условиям (1) и (2).

Лемма 11. *Пусть, как обычно, T_f — распределение, представленное функцией f. Тогда*

$$\hat{T}_{\psi Ч}=\hat{T}_{Ч}*T_F.$$

Доказательство. Это следует из теории распределений и условий (1) и (2), потому что W — быстро убывающая функция, а T_f — умеренное распределение ([13], теорема XV гл. VII, § 8).

Согласно леммам 7 и 8, распределение $W*T_F$ представлено некоторой функцией, непрерывной всюду, кроме точек разрыва функции F.

Представим F в виде суммы ОНЛ-функции β и характеристических функций интервалов $F=\beta+\sum\chi_t$.

Из условия (2) тогда следует, что ψ имеет вид

$$\psi(t) = \sum_{\nu} c_\nu \frac{\sin a_\nu t}{t} + \frac{h(t)}{t},$$

где c_ν, a_ν — константы, $a_\nu \neq 0$ и $h \in \mathfrak{L}_2$.

Так как произведение двух функций из $\mathfrak{L}_2$ принадлежит $\mathfrak{L}_1$, отсюда вытекает, что

$$\psi(t) * \chi(t) = \sum_{\nu} c_\nu \frac{\sin a_\nu t}{t} \log|t| + k(t),$$

где $k(t) \in \mathfrak{L}_1$.

Функции

$$\frac{\sin a_\nu t}{t} \log|t|$$

при $t > 0$ осциллируют при $t \to \infty$. Отсюда следует, что интеграл

$$\lim_{T\to\infty} \int_{-T}^{+T} \psi(t) * \chi(t)\, dt$$

сходится, подобно тому как сходится знакопеременный ряд, члены которого по абсолютной величине монотонно стремятся к нулю.

Преобразование Фурье функции $\psi * \chi$

$$\int_{-\infty}^{+\infty} \psi(t) * \chi(t)\, e^{-itx}\, dt$$

можно вычислить, интегрируя отдельно $k(t)$ и члены вида

$$\frac{\sin a_\nu t}{t} \log|t|$$

при условии, что $x \neq \pm a_\nu$ при любом ν (этим обеспечивается равномерная сходимость интеграла Фурье в некоторой окрестности точки x). Тем самым это преобразование Фурье представляет собой непрерывную функцию, определенную вне точек $\pm a_\nu$.

Функция ψЧ представляет распределение $T_{\psi Ч}$, преобразование Фурье которого (как распределения) определяется леммой 11. Кроме того, имеет место

Лемма 12. *Пусть* $f = \psi Ч$. *Всюду, за исключением точек* $\pm a_\nu$, *распределение* $\hat{T}_f$ *представлено непрерывной функцией*

$$\int_{-\infty}^{+\infty} f(t)\, e^{-itx}\, dt.$$

Доказательство. Пусть A — компактный отрезок $-T \leqslant t \leqslant T$, и пусть f_A — произведение функции f на характеристическую функцию этого отрезка. Наше утверждение справедливо для f_A вместо f. Тем самым T_{f_A} стремится к T_f как умеренное распределение, а $\hat{T}_{f_A}$ стремится к $\hat{T}_f$ как умеренное распределение и, стало быть, как распределение в окрестности каждой точки $x \neq \pm a_\nu$. Но интеграл, определяющий $\hat{T}_{f_A}$, сходится к

$$\int_{-\infty}^{+\infty} f(t)\, e^{-itx}\, dt$$

равномерно (и значит, как распределение) на каждом компактном множестве, не содержащем точек $\pm a_\nu$. Следовательно, распределение $\hat{T}_f$ представлено этим интегралом в соответствующей области.

Распределения $\hat{T}_{\psi Ч}$, $\hat{T}_Ч * \hat{T}_F$ совпадают (лемма 11), и каждое из них представлено непрерывной функцией, заданной интегралом, всюду, кроме конечного числа точек. Тем самым соответствующие функции должны совпадать почти всюду и, значит, всюду. В частности, их значения в точке нуль равны. Пользуясь следствием из леммы 8, получаем доказательство предложения 4.

Рассуждения, проведенные выше для функции $Ч(t)$, можно провести для функции $Ч_\nu$ с параметрами N_ν, $|m_\nu|$.

С этой целью рассмотрим функционал

$$W_v(\beta) = \lim_{\lambda\to\infty}\left[\int_{-\infty}^{+\infty}(1-e^{-\lambda|x|})K_v(x)\beta(x)\,dx - 2\beta(0)\log\lambda\right],$$

где $K_v(x)$ определяется формулами

$$K_v(x) = \frac{e^{(1/2-|m_v|)|x|}}{|e^x - e^{-x}|} \quad \text{при } N_v = 1,$$

$$K_v(x) = \frac{e^{-1/2|m_v x|}}{|e^{x/2} - e^{-x/2}|} \quad \text{при } N_v = 2.$$

Подобно тому как мы вычислили преобразование Фурье функции $\text{Ч}(t)$, можно вычислить преобразование Фурье функции Ч_v. Результат получается следующий.

Лемма 13. *Преобразование Фурье функции* Ч_v *равно*

$$\hat{\text{Ч}}_v = -\frac{2\pi}{N_v} W_v.$$

Собирая все слагаемые воедино, получаем

Предложение 5. *Последняя сумма в явной формуле имеет вид*

$$\sum_{v\in S_\infty} \frac{N_v}{2\pi}\hat{\text{Ч}}_v(F_v) = -\sum_{v\in S_\infty} W_v(F_v).$$

ЛИТЕРАТУРА

1. Artin E., Algebraic numbers and algebraic functions, Lecture Notes by I. Adamson, Princeton and New York Universities, 1951.
2. Artin E., Theory of algebraic numbers, Notes by G. Wurges, Göttingen, 1956.
3. Artin E., Tate J., Class field theory, Princeton notes, 1951, distributed by Harvard University.
4. Bourbaki N., Commutative algebra, Hermann, Paris, 1962.
5. Brauer R., On the zeta-functions of algebraic number fields II, *Amer. J. Math.*, 72, № 4 (1950), 739—746.
6. Hilbert D., Die Theorie der algebraischen Zahlkörper, *Jahresber. Dtsch. Math. Ver.*, 4 (1897), 175—546.
7. Lang S., Diophantine Geometry, Interscience, New York, 1962.
8. Serre J. P., Corps locaux, Hermann, Paris, 1963.
9. Tate J., Fourier analysis in number fields and Hecke's zeta-function, Thesis, Princeton, 1950.
10. Weil A., Sur les «formules explicites» de la théorie des nombres premiers, Comm. Séminaire Math. Université de Lund (dédié à M. Riesz), 1952, 252—265.
11*. Голод Е., Шафаревич И., О башне полей классов, *Изв. АН СССР*, сер. мат., 1964.
12. Инграм А. Е., Распределение простых чисел, М. — Л., ОНТИ, 1936.
13. Schwartz L., Theorie des Distributions, Paris, 1948.

УКАЗАТЕЛЬ ТЕРМИНОВ

Адель VI, 1
Артина символ IV,3
Архимедово нормирование II,1

Ведущий идеал VII,2
Величина (дивизора) V,1
Вещественное нормирование II,1
Вполне разветвленное расширение II,5
— распадающийся идеал I.7
Выпуклое множество V,3

Гекке характер VII,7
Гензеля лемма I,6; II,2
Главный дробный идеал I,6
— идель VI,3

Дедекиндово кольцо I,6
Дивизор V,1
Дискретно нормированное кольцо I,7
Дискриминант III,3
Дифферента III,1
Дробный идеал I,6

Единицы V,1; II,7

Идеалов класс I,7
Иделей класс VI,3
Идель VI,1
Индекс ветвления I,7
Инерции группа I,5

Равномерное распределение VIII,5
Разложения групп I,5
— поля I,5
Регулятор VII,7

Симметричное тело V,3
Слабо разветвленное расширение II,5
Степень поля классов вычетов I,7

Каноническая система нормирований II,1
Квазихарактер VII,2; VII,5
Комплексное нормирование II,1
Круговое расширение IV,1

Линейная эквивалентность идеалов I,6
Локальная дифферента III,1
Локальное поле VII,1
— кольцо I,1

Мультипликативное подмножество I,1
Мультипликативность дифференты III,1

Неразветвленный идеал II,4
— характер VII,2
Норма идеала I,7
— иделя VI,1
Нормирование II,1
Нуль I,6

Ограниченное прямое произведение VI,1

Параллелотоп V,2
Полюс I,6
Пополнение II,1
Порядок идеала I,6; II,2
— элемента I,6

Формальный идеал II,2
Фробениуса автоморфизм IV,3
Фундаментальная область V,2
Фундаментальные единицы VII,7

Целое алгебраическое число I,2
Целозамкнутое кольцо I,2
Целый элемент I,2
Числовое поле I,2

ОГЛАВЛЕНИЕ

Предисловие 5
Предварительные требования 7
От переводчика 8

Глава I **Целые алгебраические числа** 9

§ 1. Локализация 9
§ 2. Целое замыкание 10
§ 3. Простые идеалы 15
§ 4. Китайская теорема об остатках 18
§ 5. Расширения Галуа 19
§ 6. Дедекиндовы кольца 25
§ 7. Дискретно нормированные кольца 31

Глава II. **Пополнения** 39

§ 1. Определения и пополнения 39
§ 2. Многочлены над полными полями 48
§ 3. Некоторые фильтрации 53
§ 4. Неразветвленные расширения 56
§ 5. Слабо разветвленные расширения 59

Глава III. **Дифферента и дискриминант** 65

§ 1. Дополнительные модули 65
§ 2. Дифферента и ветвление 71
§ 3. Дискриминант 74

Глава IV. **Круговые поля** 78

§ 1. Корни из единицы 78
§ 2. Квадратичные поля 84

§ 3. Символ Артина 86
§ 4. Лемма Артина 87

Глава V. **Параллелотопы** 91

§ 1. Формула произведения 91
§ 2. Точки решетки в параллелотопах 102
§ 3. Вычисление одного объема 110
§ 4. Константа Минковского 113

Глава VI. **Идели и адели** 118

§ 1. Ограниченные прямые произведения 118
§ 2. Адели 121
§ 3. Идели 123

Глава VII. **Функциональное уравнение** 130

§ 1. Локальная аддитивная двойственность 131
§ 2. Локальная мультипликативная теория 134
§ 3. Локальное функциональное уравнение 137
§ 4. Локальные вычисления 139
§ 5. Ограниченные прямые произведения 145
§ 6. Глобальная аддитивная двойственность. Теорема Римана — Роха 149
§ 7. Глобальное функциональное уравнение 153
§ 8. Глобальные вычисления 159

Глава VIII. **Плотность простых идеалов и тауберова теорема** 164
§ 1. Интеграл Дирихле 165
§ 2. Тауберова теорема Икеара 167
§ 3. Тауберова теорема для рядов Дирихле 173
§ 4. Некоторые теоремы о сходимости 175
§ 5. Плотности 179

Глава IX. **Теорема Брауэра — Зигеля** 184

§ 1. Верхняя оценка для вычета 185
§ 2. Нижняя оценка для вычета 186
§ 3. Сравнение вычетов в нормальных расширениях . 189
§ 4. Окончание доказательства 191
Приложение — лемма Брауэра 193

Глава X. **Явные формулы** 196
§ 1. Вейерштрассово разложение L-ряда 197
§ 2. Оценка функции Λ'/Λ 199
§ 3. Основная сумма 203
§ 4. Вычисление суммы: первая часть 207
§ 5. Вычисление суммы: вторая часть 208

Литература 221
Указатель терминов 222

С. Ленг
АЛГЕБРАИЧЕСКИЕ ЧИСЛА

Редактор *Л. Б. Штейнпресс*
Художественный редактор *В. И. Шаповалов*
Технический редактор *Н. А. Иовлева*

Сдано в производство 31/VIII 1965 г. Подписано к печати 3/XII 1965 г.
Бумага 84×108$^1/_{32}$=3,56 бум. л. 11,97 печ. л. Уч-изд. л. 9,21
Изд. № 1/3393. Цена 64 к. Заказ 1254
(Темплан 1966 г. изд-ва «МИР», пор. № 23)

ИЗДАТЕЛЬСТВО «МИР»
Москва, 1-й Рижский пер., 2
Московская типография № 16
Главполиграфпрома Комитета по печати
при Совете Министров СССР.
Москва, Трехпрудный пер., 9