Э. ГЕККЕ

ЛЕКЦИИ ПО ТЕОРИИ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

Перевод с немецкого
Г. И. ОЛЬШАНСКОГО и Д. А. РАЙКОВА

ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ТЕХНИКО-ТЕОРЕТИЧЕСКОЙ ЛИТЕРАТУРЫ
Москва 1940 Ленинград

Редактор *Л. Е. Садовский.* Тех. редактор *В. Ф. Зазульская.*

Индекс Т 23-5-4 (2). Печ. л. 16¼.
Прот. ТКК № 20. Учетно-автор. листов 19,3.
Сдано в производство 1/II 1939 г. Учетный № 4616.
Подписано к печати 16/VII 1939 г. Заказ № 1386.
Тираж 4.000 экз. Уполномоченный Главлита № А-11986.
Формат бумаги 60×92¼₁₆. Бумага Окуловской ф-ки. Тип. зн. в 1 бум. л. 102400.

4-я типография ОГИЗ'а РСФСР треста „Полиграфкнига" имени Евг. Соколовой.
Ленинград, пр. Красных Командиров, 29

ИЗ ПРЕДИСЛОВИЯ АВТОРА

Предлагаемая книга, составленная на основе лекций, которые я многократно читал в Базеле, Геттингене и Гамбурге, имеет своей целью, не предполагая у читателя никаких предварительных сведений из теории чисел, подвести его к пониманию вопросов, стоящих в центре внимания современной теории алгебраических числовых полей. Первые семь глав по материалу не содержат ничего нового. Что же касается формы изложения, то при выборе ее я исходил из современного развития математики и особенно арифметики и прежде всего всюду использовал способы выражения и методы теории групп, что дало возможность получить существенные формальные и идейные упрощения; необходимые для этого теоремы о конечных и бесконечных абелевых группах изложены во второй главе. Все же и специалист, быть может, найдет кое-что интересное в деталях, как, например, доказательство фундаментальной теоремы об абелевых группах (§ 8), изложение теории относительных дискриминантов, при котором я следую первоначальному методу Дедекинда (§§ 36, 38), и определение числа классов без помощи дзета-функции (§ 50).

Последняя, восьмая, глава ведет читателя к вершинам современной теории. В ней дается новое доказательство самых общих квадратичных законов взаимности в произвольных алгебраических числовых полях, проводимое с помощью тэта-функций и значительно более короткое, чем все известные до сих пор доказательства. Хотя этот метод и не поддается обобщению, он все же имеет то преимущество, что начинающий читатель очень быстро входит в круг новых понятий, встречающихся при изучении степенных вычетов в алгебраических числовых полях, и в силу этого легче сможет перейти к изучению высших законов взаимности. Книга заканчивается доказательством существования поля классов относительной степени 2, получающимся здесь как следствие законов взаимности.

В качестве предварительных сведений от читателя требуется лишь знание элементов дифференциального и интегрального исчислений и алгебры, а для последней главы — также элементов теории аналитических функций комплексного переменного.

Гамбург, Математический семинар, март 1923.

Э. Гекке.

ОТ ИЗДАТЕЛЬСТВА

Перевод первых 26 параграфов и половины § 27 сделан Г. И. Ольшанским. Этот перевод проредактирован Д. А. Райковым. Остальную часть книги перевел Д. А. Райков.

ОГЛАВЛЕНИЕ

ГЛАВА I

ЭЛЕМЕНТЫ ТЕОРИИ ЦЕЛЫХ РАЦИОНАЛЬНЫХ ЧИСЕЛ

§ 1. Делимость. Наибольший общий делитель. Модули. Простые числа. Основная теорема теории чисел

Предметом арифметики являются в первую очередь целые числа: $0, \pm 1, \pm 2, \ldots$; применение к ним операций сложения, вычитания, умножения и (в некоторых случаях) деления снова приводит к целым числам. Высшая арифметика подвергает подобному же исследованию также и другие классы вещественных или комплексных чисел, причем для получения своих предложений она употребляет аналитические средства, принадлежащие другим областям математики, как исчисление бесконечно малых и теория функций комплексного переменного. Так как в последних частях этой книги будет итти речь также и об этих отделах арифметики, то мы здесь предполагаем известной совокупность вещественных и (обыкновенных) комплексных чисел — числовую область, в которой четыре действия (за исключением деления на 0) неограниченно выполнимы, как это подробно устанавливается обычно в элементах алгебры или диференциального исчисления. В этой широкой области чисел выделяется одно число — единица, 1, — обладающее тем свойством, что уравнение

$$1 \cdot a = a$$

удовлетворяется при каждом a. Из числа 1 с помощью процессов сложения и вычитания получаются последовательно все *целые числа*, а если затем выполнить над ними процесс деления, то получится множество *рациональных чисел* как совокупность частных от деления целых чисел. Лишь далее, начиная с § 21, понятие „целое число“ подвергается существенному обобщению.

В этой вводной части мы кратко изложим основные предложения арифметики, касающиеся свойств делимости обыкновенных целых чисел.

В то время как при целых рациональных a, b выражения $a+b$, $a-b$, ab всегда дают опять целые числа, число $\frac{a}{b}$ — не обязательно целое. Если же оно целое, то мы имеем дело с особым свойством чисел a и b, которое мы выразим знаком

$$b \mid a$$

или словами: b делит a, или: b содержится в a, или: b есть *делитель* a, или: a есть *кратное* b. Каждое целое число $a(\neq 0)$ имеет тривиальные делители $\pm a$, ± 1; a и $-a$ имеют одни и те же делители; единственными числами, являющимися делителями каждого числа, являются обе „единицы": 1 и -1. Отличное от нуля целое число a имеет всегда только конечное число делителей, так как эти последние по абсолютной величине не могут превосходить $|a|$; число же 0 делится на каждое другое целое число.

Если b отлично от нуля и целое, то среди кратных b, не превосходящих определенного целого числа a, существует точно одно наибольшее, скажем, qb, и потому $a-qb=r$ есть неотрицательное целое число, меньшее чем $|b|$. Это целое число r, однозначно определенное для чисел a и b условиями

$$a=qb+r,\ q \text{ целое},\ 0\leqslant r<|b|,$$

называется остатком от деления a на b или *вычетом a по модулю b*. Утверждение $b\mid a$ равнозначно, таким образом, утверждению $r=0$.

Обращаясь теперь к общим делителям c двух целых чисел a, b, т. е. к числам c, для которых имеет место одновременно $c\mid a$ и $c\mid b$, отметим, прежде всего, что среди них имеется один однозначно определенный *наибольший общий делитель*; мы его обозначим через $(a,b)=d$. Согласно этому определению, всегда $d\geqslant 1$. Обратимся к нахождению свойств числа $d=(a,b)$. Заметим прежде всего, что для любых целых x и y имеем $d\mid ax+by$. Рассмотрим совокупность чисел $L(x,y)=ax+by$, получающуюся, когда x и y пробегают все целые числа. Очевидно, что d есть также наибольший общий делитель всех $L(x,y)$. В самом деле, d есть делитель всех $L(x,y)$, и не существует никакого большего числа, которое обладало бы этим свойством, так как никакое большее число не может содержаться одновременно в $a=L(1,0)$ и в $b=L(0,1)$. Пусть $d_0=L(x_0,y_0)$ будет наименьшее положительное среди чисел $L(x,y)$, так что

$$\text{из } L(x,y)>0 \text{ следует } L(x,y)\geqslant d_0. \tag{1}$$

Мы покажем теперь, что каждое число $n=L(x,y)$ есть кратное d_0 и что $d=d_0$. В самом деле, рассмотрим вычет r числа n по модулю d_0,

$$r=n-qd_0=L(x-qx_0,\ y-qy_0),\quad 0\leqslant r<d_0.$$

Если бы было $r>0$, то из (1) следовало бы $r\geqslant d_0$, поэтому возможно только $r=0$, т. е. $n=qd_0$. Таким образом совокупность чисел $L(x,y)$ содержит только кратные числа d_0, и она совпадает с совокупностью всех кратных числа d_0, так как каждое такое кратное $qd_0=L(qx_0,qy_0)$ действительно содержится среди чисел $L(x,y)$. Поэтому d_0 также есть наибольший общий делитель всех $L(x,y)$ и, следовательно, совпадает с d. В частности, отсюда получается следующая теорема:

Теорема 1. *Если* $(a, b) = d$, *то уравнение*

$$n = ax + by$$

разрешимо в целых числах x, y *тогда и только тогда, когда* $d \mid n$.

Из этого вытекает, далее, что каждый общий делитель чисел a и b, содержась во всех числах $L(x, y)$, содержится в наибольшем общем делителе чисел a и b.

Для нахождения наибольшего общего делителя пользуются, как известно, приемом, идущим еще от Евклида, — так называемым *алгоритмом Евклида*. Смысл его заключается в сведении вычисления (a, b) к вычислению наибольшего общего делителя двух меньших чисел. Именно, из $a = qb + r$ следует, что общие делители чисел a и b совпадают с общими делителями чисел b и r, а потому и $(a, b) = (b, r)$. Примем для удобства $a > 0$, $b > 0$ и, положив для симметрии $a = a_1$, $b = a_2$, обозначим через a_3 вычет a_1 по модулю a_2 и вообще через a_{i+2} вычет a_i по модулю a_{i+1}, для $i = 1, 2, \ldots$, до тех пор пока этот вычет можно определить, т. е. пока $a_{i+1} > 0$. Пусть при этом

$$a_i = q_i a_{i+1} + a_{i+2}, \quad 0 \leqslant a_{i+2} < a_{i+1}.$$

Так как числа a_i для $i > 2$ образуют монотонно убывающую последовательность целых положительных чисел, то процесс должен закончиться после конечного числа шагов, что возможно только тогда, когда получится остаток, равный нулю. Пусть, например, $a_{k+2} = 0$. В силу соотношений

$$(a_1, a_2) = (a_2, a_3) = \ldots = (a_k, a_{k+1}) = (a_{k+1}, a_{k+2}) = (a_{k+1}, 0) = a_{k+1}$$

последний не равный нулю остаток a_{k+1} есть искомый наибольший общий делитель чисел a и b.

При доказательстве теоремы 1 мы воспользовались только одним свойством числового множества $L(x, y)$, а именно тем, что оно есть модуль.

Определение. Система S целых чисел называется *модулем*, если она содержит хоть одно число, отличное от нуля, и если вместе с числами m, n к S принадлежит всегда также $m - n$.

Таким образом, если m принадлежит к S, то к S принадлежит также $m - m = 0$, далее, $0 - m = -m$, $m - (-m) = 2m$, $2m - (-m) = 3m$ и т. д., а также $-m - m = -2m$, $-2m - m = -3m$ и т. д.; вообще, если m принадлежит к S, то к S принадлежит и mx при любом целом x, а следовательно, вместе с m и n к S принадлежит также $mx + ny$ при любых целых x и y.

Мы можем теперь, отправляясь от доказательства теоремы 1, доказать относительно модулей следующую очень общую теорему:

Теорема 2. *Совокупность чисел каждого модуля* S *совпадает с совокупностью кратных некоторого определенного числа* d. *Модулем* S *число* d *определяется с точностью до множителя* ± 1.

Для доказательства заметим, что S во всяком случае содержит положительные числа. Пусть d — наименьшее из них. Если n при-

надлежит S, то, как уже было прежде указано, S принадлежит также $n - qd$ при любом целом q, в частности, — также остаток от деления n на d; но он неотрицателен и меньше d, а следовательно, должен быть равен нулю. Таким образом каждое n из S есть кратное d, и так как d принадлежит S, то и все кратные d принадлежат S. Если, наконец, d' есть другое число, также обладающее тем свойством, что S состоит из всех его кратных, то d должно быть кратным d', и обратно, т. е. $d' = \pm d$.

Если мы в произвольной линейной форме $a_1x_1 + \ldots + a_nx_n$ с целыми коэфициентами $a_1, \ldots, a_n$ заставим $x_1, \ldots, x_n$ пробегать все целые числа, то полученная таким образом совокупность значений формы, очевидно, составит модуль. Поэтому мы получаем следующую теорему:

Теорема 3. *Совокупность значений линейной формы от n переменных с целыми коэфициентами, которые не все равны нулю, совпадает с совокупностью значений некоторой формы от одной переменной, dx. При этом d есть наибольший общий делитель коэфициентов первоначальной формы.*

Таким образом, для того чтобы уравнение

$$k = a_1x_1 + \ldots + a_nx_n$$

(так называемое диофантово уравнение) было разрешимо в целых числах $x_1, \ldots, x_n$, необходимо и достаточно, чтобы наибольший общий делитель чисел $a_1, \ldots, a_n$ был делителем k.

Если $(a, b) = 1$, то мы называем a и b *взаимно простыми*. По теореме 1, для того чтобы $(a, b) = 1$, необходимо и достаточно, чтобы уравнение

$$ax + by = 1$$

было разрешимо в целых числах x, y.

Важнейшее правило для вычисления символа (a, b) формулируется следующей теоремой:

Теорема 4. *Для любых трех целых чисел a, b, c, где $c > 0$, имеет место соотношение*

$$(a, b)\, c = (ac, bc). \tag{2}$$

Действительно, если $(a, b) = d$, то из равенства $ax + by = d$, которое, согласно теореме 1, наверное выполняется при некоторых целых x, y, следует $acx + bcy = cd$, а потому cd есть кратное (ac, bc), опять-таки по теореме 1; но, с другой стороны, cd, очевидно, есть общий делитель ac и bc, а потому необходимо равно (ac, bc).

Отметим еще понятие *наименьшего общего кратного* двух чисел a, b. Это есть наименьшее положительное число v, которое делится как на a, так и на b. Наименьшее общее кратное v связано с наибольшим общим делителем $d = (a, b)$ соотношением

$$v = \frac{|ab|}{d}. \tag{3}$$

В самом деле, согласно (2), имеем

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1, \quad v = \left(\frac{a}{d}v, \frac{b}{d}v\right).$$

Но $\frac{ab}{d}$ есть общий делитель $\frac{a}{d}v$ и $\frac{b}{d}v$, а следовательно, является делителем v, т. е. $v \geqslant \frac{|ab|}{d}$; с другой стороны, $\frac{ab}{d}$ есть число, делящееся как на a так и на b, а потому по абсолютной величине $\geqslant v$. Поэтому $\frac{ab}{d} = \pm v$.

Так как числа, делящиеся на a и b, образуют модуль и v есть наименьшее положительное встречающееся в нем число, то каждое число, делящееся на a и b, должно быть кратным v.

Мы обратимся теперь к разложению чисел на множители. Если не существует другого разложения числа a на целочисленные множители, кроме тривиального, при котором один из множителей есть ± 1, а другой $\pm a$, то a называется *простым числом*. Такие числа существуют, например ± 2, ± 3, ± 5, ... Единицы ± 1 не причисляются к простым числам. Ограничимся для простоты разложением положительных чисел a на положительные множители. Прежде всего мы заметим, что каждое $a > 1$ делится по крайней мере на одно положительное простое число; действительно, наименьший положительный и превосходящий единицу множитель числа a, очевидно, может быть только простым числом. Выделим из положительного числа a при помощи разложения $a = p_1 a_1$ простой множитель p_1; далее, в случае если $a_1 > 1$, выделим из a_1 дальнейший простой множитель p_2, и т. д. Процесс этот должен будет через конечное число шагов закончиться, так как $a_1, a_2, \ldots$ образуют убывающую последовательность целых положительных чисел; иначе говоря, некоторое a_k необходимо должно будет стать равным единице. Этим способом a будет представлено в виде произведения $p_1 p_2 \ldots p_k$ из простых чисел. Таким образом простые числа являются теми простейшими элементами, из которых можно при помощи умножения построить каждое целое число. При этом имеет место следующая *основная теорема арифметики*:

Теорема 5. *Каждое положительное целое число, превосходящее единицу, можно одним и — отвлекаясь от порядка множителей — только одним способом представить в виде произведения положительных простых множителей.*

Покажем прежде всего, что простое число p только тогда может делить произведение ab двух целых чисел, если оно делит по крайней мере один из сомножителей. Это следует из теоремы 4. В самом деле, если простое число p не есть делитель a, то, как простое число, оно вообще не может иметь общих делителей с a, так что $(a, p) = 1$. Тогда, по теореме 4, для каждого положительного целого числа b

$$(ab, pb) = b.$$

Отсюда следует, что если $p \mid ab$, то и $p \mid b$, так что простое число p должно быть делителем второго множителя произведения ab. Эта теорема сразу переносится на произведения нескольких множителей.

Чтобы доказать теперь теорему 5, рассмотрим два представления положительного числа a в виде произведения степеней различных положительных простых чисел p_i, q_i:

$$p_1^{a_1} p_2^{a_2} \dots p_r^{a_r} = q_1^{b_1} q_2^{b_2} \dots q_k^{b_k}.$$

По только что доказанному, каждое простое число q входит делителем по крайней мере в один простой множитель левой части, а потому совпадает с некоторым p_i. Таким образом числа $q_1, \dots, q_k$ (быть может расположенные в другом порядке) совпадают с числами $p_1, \dots, p_r$, и обратно, так что и $k = r$. Выберем нумерацию так, чтобы $p_i = q_i$. Если бы теперь соответственные показатели степеней не оказались равными, например, $a_1 > b_1$, то после деления обеих частей равенства на $q_1^{b_1}$ мы получили бы, что левая часть имеет еще множитель $p_1 = q_1$, в то время как правая часть его уже не имеет; но это противоречит только что доказанному. Таким образом $a_1 = b_1$ и вообще $a_i = b_i$, $i = 1, \dots, k$.

Этой теоремой об *однозначной* разложимости каждого числа на простые множители дан существенно новый метод для разрешения рассмотренных выше вопросов, например, о том, является ли данное число b делителем другого числа a, о том, как найти наибольший общий делитель или наименьшее общее кратное чисел a и b, и т. д. В самом деле, представим себе a и b разложенными на их простые множители:

$$a = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}, \quad b = p_1^{b_1} p_2^{b_2} \dots p_r^{b_r},$$

где в качестве показателей a_i, b_i допускаются также нули. Очевидно, $b \mid a$ тогда и только тогда, если постоянно $a_i \geqslant b_i$. Далее,

$$(a, b) = p_1^{d_1} p_2^{d_2} \dots p_r^{d_r}, \quad \text{где} \quad d_i = \min(a_i, b_i), \quad i = 1, \dots, r,$$

$$v = p_1^{c_1} p_2^{c_2} \dots p_r^{c_r}, \quad \text{где} \quad c_i = \max(a_i, b_i), \quad i = 1, \dots, r.$$

Что *существует бесчисленное множество простых чисел*, доказывается следующим, принадлежащим Евклиду, рассуждением:

$$z = p_1 p_2 \dots p_n + 1$$

есть число, не делящееся ни на одно из простых чисел $p_1, p_2, \dots, p_n$. Поэтому z делится по крайней мере на одно простое число, отличное от $p_1, \dots, p_n$, а следовательно, если существует n простых чисел, то их существует и $n + 1$.

§ 2. Сравнения и классы вычетов

Всяким целым числом $n \neq 0$ определяется распределение всех целых чисел соответственно остаткам, которые они дают при делении на n. Два целых числа a и b, которые при делении на n дают один

и тот же остаток, мы относим к одному *классу вычетов по модулю* n или просто к одному классу $\bmod n$, и пишем $a \equiv b \pmod n$ (читается: a сравнимо с b по модулю n или modulo n); соотношение $a \equiv b \pmod n$ равносильно, таким образом, с $n \mid (a-b)$. Если a не сравнимо с b по модулю n, то мы пишем $a \not\equiv b \pmod n$. $a \equiv 0 \pmod n$ означает, что a делится на n. Каждое целое число называется *представителем* своего класса. Так как различными остатками при делении на n являются числа $0, 1, 2, \ldots, |n|-1$, то количество всех различных классов по модулю n равно $|n|$.

Для вычислений со сравнениями имеют место следующие легко устанавливаемые правила: Если a, b, c, d, n — целые числа и $n \neq 0$, то

I. $a \equiv a \pmod n$.

II. Из $a \equiv b \pmod n$ следует $b \equiv a \pmod n$.

III. Из $a \equiv b \pmod n$ и $b \equiv c \pmod n$ следует $a \equiv c \pmod n$.

IV. Из $a \equiv b \pmod n$ и $c \equiv d \pmod n$ следует $a \pm c \equiv b \pm d \pmod n$.

V. Из $a \equiv b \pmod n$ следует $ac \equiv bc \pmod n$.

Вообще из $a \equiv b \pmod n$ и $c \equiv d \pmod n$ следует также $ac \equiv bd \pmod n$. В частности, из $a \equiv b \pmod n$ следует $a^k \equiv b^k \pmod n$ при каждом целом и положительном k.

При помощи повторного применения правил IV и V мы получаем: Если $a \equiv b \pmod n$ и $f(x)$ есть целая рациональная функция от x (полином относительно x) с целочисленными коэфициентами, то $f(a) \equiv f(b) \pmod n$.

Таким образом, поскольку это касается целых рациональных операций (сложения, вычитания, умножения), можно, коротко говоря, производить вычисления со сравнениями по одному и тому же модулю точно так же, как и с уравнениями. Иначе обстоит дело с делением. Из $ca \equiv cb \pmod n$ не следует $a \equiv b \pmod n$. В самом деле, $ca \equiv cb \pmod n$ означает, что $n \mid c(a-b)$. Если теперь $(n, c) = d$, то имеем далее

$$\left(\frac{n}{d}, \frac{c}{d}\right) = 1, \quad \frac{n}{d} \mid \frac{c}{d}(a-b),$$

а следовательно, по теореме 4, мы можем лишь утверждать, что

$$\frac{n}{d} \mid (a-b), \quad \text{т. е.} \quad a \equiv b \pmod{\frac{n}{d}}.$$

Например, из $5 \cdot 4 \equiv 5 \cdot 1 \pmod{15}$ не следует, что $4 \equiv 1 \pmod{15}$, а следует только, что $4 \equiv 1 \pmod{\frac{15}{5} = 3}$. Таким образом имеет место следующая теорема:

Теорема 6. *Если* $(c, n) = d$, *то из* $ca \equiv cb \pmod n$ *следует* $a \equiv b \pmod{\frac{n}{d}}$, *и обратно.*

Именно этим обусловливается то обстоятельство, что *произведение двух целых чисел может быть сравнимо с нулем даже тогда, когда*

ни один из сомножителей этим свойством не обладает. Например, $2 \cdot 3 \equiv 0 \pmod 6$, но ни 2, ни 3 не сравнимы с нулем по модулю 6.

Что касается связи между сравнениями *по различным модулям*, то мы видим непосредственно из определения, что если некоторое сравнение выполняется по модулю n, то оно справедливо также и для каждого делителя n, в частности, и для $-n$. Далее если

$$a \equiv b \pmod{n_1} \text{ и } a \equiv b \pmod{n_2},$$

то

$$a \equiv b \pmod{v},$$

где v есть наименьшее общее кратное n_1 и n_2.

Так как классы вычетов по модулям n и $-n$ совпадают, то достаточно исследовать классы вычетов по положительному модулю n.

Систему целых чисел мы называем *полной системой вычетов по модулю* n, если она содержит точно по одному представителю от каждого класса вычетов по модулю n. Так как такая система состоит из $|n|$ различных чисел, то $|n|$ попарно несравнимых по модулю n чисел всегда образуют полную систему вычетов $\bmod n$. Такими являются, например, числа $0, 1, 2, \ldots, |n|-1$.

Теорема 7. *Если числа* $x_1, \ldots, x_n$ *образуют полную систему вычетов по модулю* n $(n > 0)$, *то и числа* $ax_1 + b, \ldots, ax_n + b$ *образуют такую систему, если только* a, b — *целые числа и* $(a, n) = 1$.

В самом деле, n чисел $ax_i + b$ $(i = 1, \ldots, n)$, согласно теореме 6, также все не сравнимы между собой по модулю n.

Нижеследующая теорема дает полезное часто представление системы вычетов по составному модулю.

Теорема 8. *Пусть* $a_1, a_2, \ldots, a_n$ — *целые попарно взаимно простые числа и* $A = a_1 a_2 \ldots a_n$. *Если в выражении*

$$L(x_1, \ldots, x_n) = \frac{A}{a_1} c_1 x_1 + \ldots + \frac{A}{a_n} c_n x_n,$$

где c_i — *любые числа, взаимно простые соответственно с* a_i $(i = 1, \ldots, n)$, *заставить числа* x_i *пробегать независимо друг от друга соответственно полные системы вычетов по модулям* a_i $(i = 1, \ldots, n)$, *то полученная система чисел будет составлять полную систему вычетов по модулю* A.

В самом деле, количество получаемых чисел L равно $|A|$, так что нужно лишь доказать, что все они не сравнимы между собой по модулю A. Но из справедливости сравнения

$$L(x_1, \ldots, x_n) \equiv L(x_1', \ldots, x_n') \pmod A$$

следует справедливость каждого из сравнений

$$L(x_1, \ldots, x_n) \equiv L(x_1', \ldots, x_n') \pmod{a_i}$$

($i = 1, \ldots, n$). Так как, однако,

$$\frac{A}{a_k} \equiv 0 \pmod{a_i} \text{ для всех } k \neq i,$$

то мы получаем, что

$$c_i \frac{A}{a_i} x_i \equiv c_i \frac{A}{a_i} x_i' \pmod{a_i}$$

($i = 1, \ldots, n$); в силу условий $(c_i, a_i) = 1$ и $\left(\frac{A}{a_i}, a_i\right) = 1$ и теоремы 6, отсюда следует, что $x_i \equiv x_i' \pmod{a_i}$ ($i = 1, \ldots, n$). Таким образом фигурирующие в теореме 8 числа L все попарно не сравнимы между собой по модулю A.

Характеристикой каждого класса вычетов по модулю n может служить наибольший общий делитель, который произвольное число этого класса имеет с числом n. Этот наибольший общий делитель, действительно, зависит только от класса, так как из $a \equiv b \pmod{n}$ следует, что $a = b + qn$, где q—целое, а потому каждый общий делитель чисел a и n есть также общий делитель чисел b и n, и обратно. Мы можем поэтому говорить о *наибольшем общем делителе класса вычетов по модулю n с n*.

Мы поставим в первую очередь вопрос *о числе классов по модулю n, взаимно простых с n*. Это число есть *эйлерова функция* $\varphi(n)$. $\varphi(n)$ легко определяется для случая, когда n есть степень положительного простого числа p, $n = p^k$. В самом деле, $\varphi(p^k)$ есть число тех из чисел $1, \ldots, p^k$, которые не делятся на p. Но число тех из чисел $1, \ldots, p^k$, которые делятся на p, есть число кратных p на отрезке от 1 до p^k, т. е. равно p^{k-1}. Поэтому

$$\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right).$$

Чтобы найти $\varphi(n)$ для составного n, мы докажем следующую лемму:

Лемма. $\varphi(ab) = \varphi(a)\varphi(b)$, *если* $(a, b) = 1$.

В самом деле, по теореме 8 мы получим полную систему вычетов по модулю ab, если в форме $ax + by$ заставим x пробежать полную систему вычетов по модулю b, а y — полную систему вычетов по модулю a. Но для того чтобы такое число было взаимно простым с ab, т. е. как с a, так и с b, необходимо и достаточно, чтобы $(ax, b) = 1$ и $(by, a) = 1$, т. е., в силу условия $(a, b) = 1$, чтобы $(x, b) = 1$ и $(y, a) = 1$. Таким образом те из чисел $ax + by$, которые взаимно просты с ab, мы получим, если заставим x пробежать классы вычетов, взаимно простые с b, а y — соответственно классы вычетов, взаимно простые с a. Этим наша лемма доказана. Повторно применяя ее, в предположении, что n разложено на положительные простые

множители, мы получим следующий результат: Если $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$, то

$$\varphi(n) = \varphi(p_1^{a_1})\varphi(p_2^{a_2})\dots\varphi(p_r^{a_r}) = n \prod_{p|n}\left(1 - \frac{1}{p}\right), \tag{4}$$

где p в произведении пробегает все различные положительные простые множители, входящие в n.

Полная система тех классов по модулю n, которые взаимно просты с n, называется *приведенной системой классов вычетов по модулю n*. Она содержит $\varphi(n)$ классов, и система представителей по одному из каждого из этих классов называется *полной приведенной системой вычетов по модулю n*.

Аналогично тому как в теореме 7, доказывается следующее предложение: Если $x_1, \dots, x_h$ есть полная приведенная система вычетов по модулю n и $(a, n) = 1$, то и $ax_1, \dots, ax_h$ есть такая система. Отсюда получается одно чрезвычайно важное следствие. Так как, согласно сказанному выше, каждое из чисел $ax_1, \dots, ax_h$ сравнимо по модулю n точно с одним из чисел $x_1, \dots, x_h$, то произведение чисел $ax_1, \dots, ax_h$ сравнимо с произведением чисел $x_1, \dots, x_h$, т. е.

$$a^h x_1 \dots x_h \equiv x_1 \dots x_h \pmod{n};$$

но каждое x_i взаимно просто с n, поэтому, по теореме 6, можно сократить обе части сравнения на $x_1 \dots x_h$, и мы получаем

$$a^h \equiv 1 \pmod{n}.$$

Так как $h = \varphi(n)$, то мы доказали следующую теорему, называемую *малой теоремой Ферма*:

Теорема 9. *Каждое число a, взаимно простое с n, удовлетворяет сравнению*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

В частности, если n есть простое число p (> 0), то $\varphi(p) = p - 1$, и умножением на a мы получаем сравнение, справедливое уже для каждого целого числа a:

$$a^p \equiv a \pmod{p}. \tag{5}$$

Значение этой теоремы и сущность ее доказательства вполне выяснятся лишь во второй главе, когда мы свяжем эти исследования с общим понятием группы. Эта теорема содержит высказывание относительно решений сравнения $x^p - x \equiv 0 \pmod{p}$ и образует основу для теории сравнений высших степеней.

§ 3. Целочисленные полиномы. Функциональные сравнения. Делимость по модулю p

Руководствуясь при дальнейшем развитии изложенных до сих пор идей аналогиями из алгебры, мы ближайшей своей целью поставим исследование полиномов $f(x)$ с целыми коэфициентами в смысле их

поведения относительно модуля n и затем исследование вопроса о разрешимости сравнения $f(x) \equiv 0 \pmod{n}$ в целых числах x.

Под *целочисленным полиномом* $f(x) = a_0 + a_1 x + \ldots + a_k x^k$ мы понимаем такой полином, в котором коэфициенты $a_0, a_1, \ldots, a_k$ суть целые числа. Два целочисленных полинома $f(x) = a_0 + a_1 x + \ldots + a_k x^k$ и $g(x) = b_0 + b_1 x + \ldots + b_k x^k$ называются *сравнимыми по модулю* n,

$$f(x) \equiv g(x) \pmod{n},$$

если

$$a_i \equiv b_i \pmod{n} \text{ для } i = 0, 1, \ldots, k.$$

(Для констант, т. е. полиномов нулевой степени, это определение сравнения совпадает с прежним.) Это определение характеризует, таким образом, взаимоотношение полиномов $f(x)$ и $g(x)$ тождественно относительно переменной x, а не только для специальных численных значений x. Если даже для всех целочисленных знечений x постоянно

$$f(x) \equiv g(x) \pmod{n},$$

то из этого все же еще не вытекает, что $f(x)$ и $g(x)$ должны быть сравнимыми в определенном выше смысле. Чтобы убедиться в этом, достаточно рассмотреть пример

$$x^p \equiv x \pmod{p}$$

(p — простое положительное число). По теореме Ферма это *числовое сравнение* выполняется для каждого целого числа x; однако *полиномы* x^p и x не сравнимы между собой.

Для определенных нами функциональных сравнений имеют место точно те же правила I — V, которые указаны на стр. 13 для числовых сравнений. Доказательство столь же просто, и поэтому мы на нем не будем останавливаться.

Определение. Говорят, что целочисленный полином $f(x)$ *делится по модулю* n на целочисленный полином $g(x)$, если существует такой целочисленный же полином $g_1(x)$, что

$$f(x) \equiv g(x)\, g_1(x) \pmod{n}.$$

Далее, всякое целое число a, удовлетворяющее сравнению

$$f(a) \equiv 0 \pmod{n},$$

называется *корнем* $f(x)$ *по модулю* n.

Если a есть корень $f(x)$ по модулю n и $a \equiv b \pmod{n}$, то, очевидно, b также есть корень $f(x)$ по модулю n.

Связь между корнями по модулю n и делимостью по модулю n устанавливается следующим предложением:

Теорема 10. *Если a есть корень целочисленного полинома $f(x)$ по модулю n, то $f(x)$ делится на $x - a$ по модулю n, и обратно.*

В самом деле, так как $f(a) \equiv 0 \pmod{n}$, то

$$f(x) \equiv f(x) - f(a) \pmod{n}.$$

Но $\frac{f(x)-f(a)}{x-a}$ есть целочисленный полином $g(x)$, так как для каждого положительного m

$$\frac{x^m-a^m}{x-a}=x^{m-1}+ax^{m-2}+\ldots+a^{m-2}x+a^{m-1}$$

есть целочисленный полином и $f(x)-f(a)$ есть целочисленная комбинация выражений x^m-a^m. Поэтому

$$f(x)\equiv(x-a)g(x) \pmod n.$$

Обратное предложение тривиально.

Если f, g, g_1 — целочисленные полиномы и $f(x)\equiv g(x)g_1(x) \pmod n$, то отсюда еще не следует, как это можно было бы предположить по аналогии с алгеброй, что корень a полинома $f(x)$ по модулю n есть также корень $g(x)$ или $g_1(x)$ по модулю n. Например,

$$x^2\equiv(x-2)(x-2) \pmod 4,$$

но 4, будучи корнем x^2 по модулю 4, не есть корень $x-2$ по модулю 4. Только для простых модулей, как показывает нижеследующая теорема, имеет место предполагаемое свойство.

Теорема 11. *Если* $f(x)\equiv g(x)g_1(x) \pmod p$, *где* p *есть простое число, то каждый корень* $f(x)$ *по модулю* p *есть корень по крайней мере одного из полиномов* $g(x)$, $g_1(x)$ *по модулю* p.

Действительно, если для целого числа a

$$f(a)\equiv 0 \pmod p,$$

то

$$g(a)g_1(a)\equiv f(a)\equiv 0 \pmod p;$$

но тогда простое число p, деля произведение $g(a)g_1(a)$, должно делить по крайней мере одного из сомножителей.

Теорема 12. *Целочисленный полином* $f(x)$ *степени* k *может иметь по простому модулю* p *не больше* k *несравнимых корней, за исключением случая, когда* $f(x)\equiv 0 \pmod p$, *т. е. когда все коэффициенты полинома* $f(x)$ *делятся на* p.

Теорема справедлива для полиномов нулевой степени, т. е. констант. В самом деле, если $f(x)$ не зависит от x, $f(x)=c_0$, то сравнение $f(x)\equiv 0 \pmod p$ имеет либо 0 решений, если p не есть делитель c_0, либо бесконечное множество решений, — а именно, все целые числа, — если c_0 делится на p, т. е. $f(x)\equiv 0 \pmod p$. Пусть теперь наша теорема доказана для всех полиномов степени $\leqslant k-1$. Докажем, что тогда она справедлива также и для полиномов степени k. Если a есть корень $f(x)$ по модулю p, то, согласно теореме 10, мы можем положить

$$f(x)\equiv(x-a)f_1(x) \pmod p,$$

где степень $f_1(x)$ не выше $k-1$. По теореме 11 каждый корень $f(x)$ по модулю p есть либо корень $f_1(x)$, либо корень $x-a$ (либо корень

обоих) по модулю p. Но сравнение $x-a\equiv 0 \pmod p$ имеет только одно решение, а сравнение $f_1(x)\equiv 0 \pmod p$ имеет, по предположению, либо не больше $k-1$ несравнимых решений, — и тогда $f(x)$ имеет не больше $k-1+1=k$ решений — либо $f_1(x)\equiv 0 \pmod p$, а тогда и $f(x)\equiv 0 \pmod p$. Таким образом наша теорема с помощью полной индукции доказана.

Аналогичная теорема для составных модулей несправедлива, как показывает рассмотрение корней полинома x^2-1 по модулю 8. Этот полином второй степени имеет по модулю 8 четыре несравнимых корня, а именно $x=1, 3, 5, 7$.

Теорема 13. *Если для двух целочисленных полиномов $f(x)$ и $g(x)$ имеет место соотношение*

$$f(x)\,g(x)\equiv 0 \pmod p,$$

где p — простое число, тогда имеет место по крайней мере одно из соотношений $f(x)\equiv 0 \pmod p$, $g(x)\equiv 0 \pmod p$.

Допустим, что теорема неверна, т. е. $f(x)\not\equiv 0 \pmod p$ и $g(x)\not\equiv 0 \pmod p$. Опустим тогда в $f(x)$ и в $g(x)$ все члены, делящиеся на p. Мы получим два отличных от нуля полинома $f_1(x)$, $g_1(x)$, все коэфициенты которых не делятся на p, и в то же самое время $f(x)\equiv f_1(x) \pmod p$, $g(x)\equiv g_1(x) \pmod p$, так что $f_1(x)g_1(x)\equiv 0 \pmod p$. Таким образом старший коэфициент в $f_1(x)g_1(x)$ должен, с одной стороны, быть $\equiv 0 \pmod p$, а с другой стороны, он равен произведению старших коэфициентов $f_1(x)$ и $g_1(x)$. Но так как p есть простое число и все коэфициенты $f_1(x)$ и $g_1(x)$ не делятся на p, то и произведение двух таких коэфициентов не может делиться на p. Таким образом наше допущение неверно и теорема доказана.

Определение. Целочисленный полином $f(x)$ называется *примитивным*, если его коэфициенты взаимно просты, так что для каждого простого числа p всегда $f(x)\not\equiv 0 \pmod p$.

Теорему 13 можно теперь, очевидно, сформулировать так:

Теорема 13а. *Произведение двух примитивных полиномов есть примитивный полином. (Теорема Гаусса.)*

§ 4. Сравнения первой степени

Полиномы первой степени и их корни по модулю n легко исследовать. Это ведет к теории линейных сравнений с одной или многими неизвестными.

Пусть даны целые числа a, b, n $(n>0)$. Спрашивается, что можно утверждать относительно решений в целых числах сравнения

$$ax+b\equiv 0 \pmod n. \tag{6}$$

Так как решениями, если таковые существуют, являются одновременно все числа некоторого класса по модулю n, то вопрос ставится только

относительно решений, несравнимых по модулю n. Ответ на этот вопрос дает следующая теорема:

Теорема 14. *Если* $(a, n) = 1$, *то сравнение* (6) *имеет одно и только одно решение по модулю* n.

В самом деле, по теореме 7 $ax + b$ точно один раз попадает в класс вычетов 0, когда x пробегает полную систему вычетов по модулю n, чем теорема 14 и доказана.

Если $(a, n) = d$ и сравнение (6) разрешимо, то оно справедливо также и по модулю d, и мы получаем для b условие

$$b \equiv 0 \pmod{d}.$$

По теореме 6 сравнение (6) равносильно тогда с

$$\frac{a}{d}x + \frac{b}{d} \equiv 0 \pmod{\frac{n}{d}},$$

а это последнее по теореме 14 имеет по модулю $\frac{n}{d}$ одно вполне определенное решение x_0. Все решения сравнения (6) даются, следовательно, числами

$$x = x_0 + \frac{n}{d}y$$

с целыми y, а среди них имеется точно d различных по модулю n. Мы их получим, если заставим y пробежать полную систему вычетов по модулю d.

Таким образом, *если* $(a, n) = d > 1$, *то сравнение* (6) *разрешимо только тогда, когда* $d \mid b$. *В этом случае число несравнимых по модулю* n *решений равно* d.

Сравнение (6) равносильно уравнению $ax + b = nz$, где z — целое, т. е. разрешение сравнения (6) эквивалентно разрешению линейного диофантова уравнения $ax - nz = -b$. Применение к этому уравнению теоремы 1 также приводит, конечно, к только что полученному результату. В частности, если $(a, n) = 1$, то сравнение

$$aa' \equiv 1 \pmod{n}$$

всегда имеет одно определенное решение a' по модулю n, и решение более общего сравнения $ax + b \equiv 0 \pmod{n}$ мы, умножая обе части этого сравнения на a', получим в форме

$$x \equiv -a'b \pmod{n}.$$

Согласно теореме 9, мы в качестве a' можем взять, в частности, число $a^{\varphi(n)-1}$.

Если дано несколько сравнений с одной неизвестной x, но по различным модулям, то мы можем предположить, что они приведены к форме

$$x \equiv a_1 \pmod{n_1}, \ldots, \quad x \equiv a_k \pmod{n_k}. \tag{7}$$

Если x и y — два числа, удовлетворяющих этой системе, то $x - y$ делится на каждое n_i, а значит, и на наименьшее общее кратное v

чисел $n_1, \ldots, n_k$, т. е. $x \equiv y \pmod{v}$. Обратно, если x есть решение системы (7) и $x \equiv y \pmod{v}$, то y также есть решение этой системы. Таким образом решения системы (7), если они существуют, однозначно определены по модулю v. Мы здесь займемся только наиболее важным случаем.

Теорема 15. *k сравнений (7) имеют точно одно определенное решение по модулю $n_1 n_2 \ldots n_k$, если модули $n_1, \ldots, n_k$ попарно взаимно просты.*

В самом деле, принимая во внимание теорему 8, мы положим

$$x = \frac{v}{n_1} x_1 + \ldots + \frac{v}{n_k} x_k \quad (v = n_1 \ldots n_k),$$

и определим числа x_i из сравнений

$$\frac{v}{n_i} x_i \equiv a_i \pmod{n_i} \quad (i = 1, \ldots, k),$$

что по теореме 14 всегда возможно при нашем предположении. Полученное таким образом x, очевидно, будет решением системы (7). Единственность решения по модулю $n_1 \ldots n_k$ вытекает из замечаний, предшествовавших теореме 15.

Исследование корней полиномов высших степеней по модулю n приводит к сравнениям высших степеней с одной неизвестной. Чтобы иметь возможность охватить даже только элементы этой гораздо более сложной теории, мы должны глубже изучить оперирование с классами вычетов. Основные моменты имеющих здесь место соотношений будут еще многократно встречаться нам впоследствии в самых различных формах, так что является целесообразным извлечь то понятие, которое поддается столь многообразным осуществлениям, и сделать его объектом самостоятельного исследования. Этим понятием является *понятие группы*. Ему посвящена следующая глава.

ГЛАВА II

АБЕЛЕВЫ ГРУППЫ

§ 5. Общее понятие о группе. Операции над элементами группы

Определение группы. Система S каких-либо элементов $A, B, C, \ldots$ называется *группой*, если выполнены следующие условия:

I. Дан способ (правило композиции), согласно которому из элемента A и элемента B системы S всегда однозначным образом получается снова некоторый элемент C из S. Символически мы записываем это соотношение так:

$$AB = C \quad \text{или} \quad C = AB.$$

Эта композиция не обязательно должна быть коммутативной относительно элементов A и B, т. е. AB может быть отлично от BA.

II. Для композиции должен иметь место ассоциативный закон: для любых трех элементов A, B и C всегда

$$A(BC) = (AB)C.$$

III. Если A, A' и B — три каких-нибудь элемента из S, то
из $AB = A'B$ следует $A = A'$,
из $BA = BA'$ следует $A = A'$.

IV. Для любых двух элементов A, B из S существует в S такой элемент X, что $AX = B$, и такой элемент Y, что $YA = B$.

Если система S содержит только конечное число различных элементов, — пусть это число будет h, — то условие IV выполняется само собой как следствие условий I и III. В самом деле, пусть в AX элемент X пробегает все h различных элементов $X_1, \ldots, X_h$ группы. Согласно условию I, AX представляет собой всегда элемент группы, и полученные таким образом h элементов, согласно условию III, все различны между собой, так что каждый элемент группы встречается среди них точно один раз, в частности, среди них имеется также элемент B, следовательно, существует такое X, что $AX = B$. Аналогичным рассуждением доказывается вторая часть условия IV.

Если группа содержит бесконечное множество элементов, то она называется *бесконечной*; в противном случае она называется *конечной группой порядка* h, где h есть число ее элементов.

Свойство образовывать группу присуще системе S не абсолютно, а лишь в связи с определенным способом композиции. При одном способе композиции S может быть группой, в то время как при другом способе композиции те же самые элементы могут не образовывать группы.

Примерами групп являются: система всех целых чисел, если за композицию принимается сложение, и система всех положительных рациональных чисел, если за композицию принимается умножение. Система же положительных целых чисел при композиции путем умножения не образует группы, так как требование IV не выполняется.

Если, далее, мы будем два целых числа считать равными, когда они сравнимы по определенному модулю n, то система вычетов по модулю n образует при композиции путем сложения конечную группу порядка n.

Точно так же система вычетов по модулю n, взаимно простых с n, образует при композиции путем умножения конечную группу порядка $\varphi(n)$. Во всех этих случаях композиция коммутативна. Примером некоммутативной группы может служить система всех вращений вокруг центра некоторого правильного тела, например куба, приводящих это тело к совпадению с самим собой. При этом результатом AB композиции вращений A и B называется то вращение, которое получится, если выполнить сначала B, потом A.

Совокупность перестановок из n цифр также образует конечную группу. За результат композиции перестановки A с перестановкой B принимается здесь перестановка AB, которая получится, если выполнить сначала B, а затем A. Эта группа также некоммутативна.

Если даны две группы $\mathfrak{G}_1$ и $\mathfrak{G}_2$, элементы которых отмечены соответственно индексами 1 и 2, и если между элементами групп $\mathfrak{G}_1$ и $\mathfrak{G}_2$ можно установить такое взаимно однозначное соответствие (обозначаемое символом $\rightarrow$), что всегда

$$\text{из } A_1 \rightarrow A_2 \text{ и } B_1 \rightarrow B_2 \text{ следует } A_1 B_1 \rightarrow A_2 B_2,$$

то группы $\mathfrak{G}_1$ и $\mathfrak{G}_2$ называются *изоморфными*. Две изоморфных группы отличаются, таким образом, только обозначением элементов и связывающей их операции. Поэтому все свойства, присущие какой-либо группе, присущи также и каждой изоморфной с ней группе, если только эти свойства могут быть получены с помощью одних только групповых аксиом I — IV. Таким образом в теоретико-групповых исследованиях изоморфные группы не следует рассматривать как различные.

Пусть теперь $\mathfrak{G}$ — группа. Ее элементы мы в дальнейшем будем обозначать большими латинскими буквами. Согласно условию, определено „произведение“ (т. е. результат композиции) двух элементов из $\mathfrak{G}$. С помощью полной индукции мы определяем теперь произведение k элементов:

Определение. Пусть уже определено, какие элементы из $\mathfrak{G}$ следует понимать под произведениями $A_1 A_2 \ldots A_n$ произвольных n элементов $A_1, A_2, \ldots, A_n$ из $\mathfrak{G}$. Мы определяем тогда произведение

любых $n+1$ элементов $A_1, \ldots, A_n, A_{n+1}$ из $\mathfrak{G}$ с помощью равенства

$$A_1 \ldots A_n A_{n+1} = (A_1 \ldots A_n) A_{n+1}.$$

Докажем теперь следующую лемму:

Лемма. *Для каждого целого* $k \geqslant 3$ *имеет место равенство*

$$A_1 A_2 \ldots A_k = A_1 (A_2 \ldots A_k).$$

Для $k = 3$ это равенство, очевидно, справедливо, в силу ассоциативного закона II. Но если лемма справедлива для $k = n$, то она справедлива и для $k = n+1$, как это видно из равенств

$$A_1 A_2 \ldots A_n A_{n+1} = (A_1 A_2 \ldots A_n) A_{n+1} =$$
$$= A_1 (A_2 \ldots A_n) A_{n+1} = A_1 (A_2 \ldots A_n A_{n+1}).$$

Таким образом лемма доказана.

Из этой леммы следует, что

$$(A_1 \ldots A_{l-1} A_l)(A_{l+1} \ldots A_k) = [(A_1 \ldots A_{l-1}) A_l](A_{l+1} \ldots A_k) =$$
$$= (A_1 \ldots A_{l-1})[A_l (A_{l+1} \ldots A_k)] =$$
$$= (A_1 \ldots A_{l-1})(A_l A_{l+1} \ldots A_k),$$

т. е. в первоначальном произведении можно, не меняя результата, перенести внутренние скобки на одно место влево. Следовательно, их можно перенести вообще на сколько угодно мест вправо или влево, и потому произведение

$$(A_1 \ldots A_l)(A_{l+1} \ldots A_k) = A_1 \ldots A_k$$

совершенно не зависит от места, где стоят скобки. Таким образом в произведении, состоящем из двух выражений, находящихся в скобках, можно, не меняя результата, опустить эти скобки. При помощи полной индукции эта теорема легко обобщается на случай произведения любого числа выражений:

Теорема 16. *Произведение из* $r+1$ *заключенных в скобки выражений*

$$(A_1 \ldots A_{n_1})(A_{n_1+1} \ldots A_{n_2})(A_{n_2+1} \ldots A_{n_3}) \ldots (A_{n_r-1} \ldots A_k)$$

не меняется, если эти скобки опустить, и равно поэтому, независимо от того, где стоят скобки, произведению

$$A_1 \ldots A_k.$$

Продолжим исследование свойств групп.

Теорема 17. *В каждой группе существует точно один элемент* E, *обладающий тем свойством, что*

$$AE = EA = A$$

для каждого элемента A *группы.* E *называется единичным элементом.*

В самом деле, согласно IV, для A существует такое E, что

$$AE = A,$$ а значит, и $$YAE = YA.$$

Если теперь Y пробегает все элементы группы, то, согласно IV это же будет иметь место и для $YA = B$, так что $BE = B$ для каждого B, и E не зависит от B.

Далее, таким же образом убеждаемся в существовании такого E', что для каждого A

$$E'A = A.$$

Для $A = E$ имеем тогда

$$E'E = E,$$

а из $AE = A$ следует при $A = E'$, что

$$E'E = E'.$$

Следовательно,

$$E = E',$$

что и доказывает теорему.

Единичный элемент E играет, следовательно, роль числа 1 в обыкновенном умножении; он иногда и обозначается через 1.

Согласно условию IV, для каждого A существуют такие X и Y, что

$$AX = E, \quad YA = E.$$

Отсюда при композиции с Y получаем

$$YAX = YE, \text{ т. е. } EX = YE,$$

или

$$X = Y.$$

Этот, однозначно определяемый элементом A, элемент X называется элементом, *обратным элементу* A, и обозначается через A^{-1}. Он определен равенствами

$$AA^{-1} = A^{-1}A = E.$$

Теперь мы можем ввести понятие степени элемента A. Под A^m мы при положительном целом m понимаем произведение m элементов, каждый из которых равен A. По теореме 16 для любых целых положительных m, n имеет тогда место равенство

$$A^{m+n} = A^m A^n = A^n A^m.$$

Далее, пользуясь теоремой 16, получаем

$$A^m (A^{-1})^m = E,$$

т. е. $(A^{-1})^m$ есть обратный элемент для A^m и равен, следовательно, $(A^m)^{-1}$. Мы обозначаем этот элемент через

$$A^{-m} = (A^{-1})^m = (A^m)^{-1}.$$

Наконец, для любого A полагаем

$$A^0 = E.$$

Точно так же как в элементарной алгебре, для определенных нами степеней с любыми целыми показателями доказывается следующая теорема:

Теорема 18. *Для любых целых чисел m, n имеют место равенства*

$$A^m A^n = A^n A^m = A^{m+n},$$

$$(A^m)^n = (A^n)^m = A^{nm}.$$

С помощью обратных элементов можно разрешить уравнение относительно элементов группы с одним неизвестным: умножая обе части уравнения $AX = B$ на A^{-1}, мы получаем

$$X = A^{-1}B;$$

таким же образом из

$$YA = B$$

получаем

$$Y = BA^{-1}.$$

§ 6. Подгруппы.

Разложение группы на смежные классы по данной подгруппе.

Пусть теперь часть элементов из $\mathfrak{G}$ уже сама образует группу относительно того же правила композиции. Такая часть называется *делителем* или *подгруппой* группы $\mathfrak{G}$. Пусть $\mathfrak{U}$ — некоторая подгруппа и $U_1, U_2, \ldots$ — элементы этой подгруппы (в конечном или бесконечном числе). Если A есть произвольный элемент из $\mathfrak{G}$, то мы будем через

$$A\mathfrak{U} = (AU_1, AU_2, \ldots)$$

обозначать совокупность элементов AU_i $(i = 1, 2, \ldots)$. Элементы группы $\mathfrak{G}$ можно теперь расположить в ряды вида $A\mathfrak{U}$, называемые *смежными классами по подгруппе* $\mathfrak{U}$ [1]). При этом имеет место следующее предложение:

Лемма. *Если два смежных класса $A\mathfrak{U}$ и $B\mathfrak{U}$ имеют общий элемент, то все их элементы общие, т. е., с точностью до порядка элементов, оба смежных класса вообще совпадают.*

В самом деле, если $AU_a = BU_b$ есть общий элемент, то $B = AU_aU_b^{-1}$, так что

$$B\mathfrak{U} = (AU_aU_b^{-1}U_1, AU_aU_b^{-1}U_2, \ldots).$$

Но в силу свойства IV, $U_aU_b^{-1}U_i$ при $i = 1, 2, \ldots$ пробегает все элементы группы $\mathfrak{U}$, следовательно, $A\mathfrak{U}$ и $B\mathfrak{U}$ действительно совпадают.

Число различных элементов, находящихся в каком-либо смежном классе $A\mathfrak{U}$, очевидно, не зависит от выбора A и равно порядку подгруппы $\mathfrak{U}$. Пусть этот порядок есть N, причем, значит, допускается и

---

[1]) Иногда их называют „смежными группами“, хотя только в классе $E\mathfrak{U} = \mathfrak{U}$ элементы образуют группу.

$N=\infty$. Каждый элемент A из $\mathfrak{G}$ действительно встречается в одном из смежных классов по подгруппе $\mathfrak{U}$; например, A имеется в $A\mathfrak{U}$, так как в $\mathfrak{U}$, как в группе, наверное имеется единичный элемент E, а $AE=A$. Мы получим, таким образом, каждый элемент из $\mathfrak{G}$ точно один раз, если пробежим все элементы во всех различных смежных классах $A\mathfrak{U}$. Мы это выражаем символически равенством

$$\mathfrak{G}=A_1\mathfrak{U}+A_2\mathfrak{U}+\ldots,$$

где $A_1\mathfrak{U}$, $A_2\mathfrak{U}$, ... означают все различные существующие смежные классы по подгруппе $\mathfrak{U}$.

Если теперь $\mathfrak{G}$ есть *конечная* группа порядка h, то и порядок N подгруппы $\mathfrak{U}$ конечен и число различных смежных классов по подгруппе $\mathfrak{U}$ тогда также конечно и равно, скажем, j. Так как каждый элемент из $\mathfrak{G}$ встречается точно в одном смежном классе и в каждом смежном классе содержится точно N различных элементов, то

$$h=jN.$$

Этим доказана следующая теорема:

Теорема 19. *В конечной группе $\mathfrak{G}$ порядка h порядок N каждой подгруппы $\mathfrak{U}$ есть делитель числа h.*

Частное $\frac{h}{N}=j$ называется *индексом* подгруппы $\mathfrak{U}$ относительно группы $\mathfrak{G}$.

Если $\mathfrak{G}$ есть *бесконечная* группа, то как порядок подгруппы $\mathfrak{U}$, так и число различных смежных классов по этой подгруппе могут быть бесконечно велики, и очевидно, что по крайней мере одно из этих обстоятельств наверное должно иметь место. Число различных смежных классов по подгруппе $\mathfrak{A}$ и в этом случае называется индексом этой подгруппы, так что индекс подгруппы может быть как конечным, так и бесконечным.

Наши дальнейшие исследования будут относиться пока только к конечным группам.

Система $S=(U_1, U_2, \ldots)$ элементов, принадлежащих какой-либо конечной группе $\mathfrak{G}$, образует подгруппу этой группы, если только известно, что произведение каждых двух элементов из S тоже принадлежит S. В самом деле, групповые аксиомы II и III выполняются сами собой, I имеет место по предположению, а требование IV, как было ранее показано, для конечных групп есть следствие остальных.

Таким образом, например, все степени какого-либо элемента из $\mathfrak{G}$ с положительными показателями всегда образуют подгруппу группы $\mathfrak{G}$. Эти степени не могут быть все различны, так как $\mathfrak{G}$ содержит только конечное число элементов. Но из $A^m=A^n$ следует $A^{m-n}=E$. Поэтому некоторая степень A с отличным от нуля показателем всегда равна E.

Чтобы получить представление о тех показателях q, для которых $A^q=E$, заметим, что эти показатели, очевидно, образуют модуль. В самом деле, из $A^q=E$ и $A^r=E$ следует $A^{q\pm r}=E$. Следовательно, по теореме 1 совокупность этих q совпадает с совокупностью всех

кратных некоторого целого числа $a(>0)$. Этот однозначно определенный элементом A показатель a называется *порядком элемента* A. Он обладает следующим свойством: $A^r = E$ тогда и только тогда, когда $r \equiv 0 \pmod a$. Единственный элемент, имеющий порядок 1, есть E. Очевидно, имеет место следующая более общая теорема:

ТЕОРЕМА 20. *Если a есть порядок элемента A, то $A^m = A^n$ тогда и только тогда, когда $m \equiv n \pmod a$.*

Таким образом среди степеней элемента A имеется только a различных между собой, например $A^0 = E, A^1, \ldots, A^{a-1}$, и они, согласно предыдущему, образуют подгруппу порядка a группы $\mathfrak{G}$. Из теоремы 19 вытекает поэтому далее

ТЕОРЕМА 21. *Порядок a всякого элемента группы $\mathfrak{G}$ есть делитель порядка h группы $\mathfrak{G}$, и потому*

$$A^h = E$$

для каждого элемента A группы $\mathfrak{G}$.

§ 7. Абелевы группы. Произведение двух абелевых групп

В теории чисел встречаются почти исключительно группы, закон композиции которых *коммутативен*: $AB = BA$ для всех элементов группы. Группы такого рода называются *абелевыми*. В этом и в ближайшем параграфе мы займемся более точным исследованием структуры произвольной конечной абелевой группы. $\mathfrak{G}$ *будет означать в дальнейшем конечную абелеву группу порядка* h.

ТЕОРЕМА 22. *Если простое число p делит порядок h группы $\mathfrak{G}$, то в $\mathfrak{G}$ существует элемент порядка p.*

В самом деле, пусть $C_1, \ldots, C_h$ будут h элементов группы $\mathfrak{G}$ и $c_1, \ldots, c_h$ — соответственно их порядки. Образуем всевозможные произведения

$$C_1^{x_1} \ldots C_h^{x_h}, \tag{8}$$

где каждое x_i пробегает соответственно полную систему вычетов по модулю c_i. Тогда мы получим $c_1 \ldots c_h$ формально различных произведений, охватывающих в совокупности все элементы группы $\mathfrak{G}$. Из того, что любая пара различных представлений одного и того же элемента приводит к некоторому представлению единичного элемента, следует, что в (8) все элементы фигурируют одинаково часто, скажем, по Q раз. Следовательно,

$$c_1 \ldots c_h = hQ.$$

Простое число p, входящее в h, должно поэтому быть делителем хоть одного из c_i, например, c_1. Тогда элемент

$$A = C_1^{\frac{c_1}{p}}$$

есть элемент порядка p.

Теорема 23. *Пусть $h = a_1 \dots a_r$ и целые числа $a_1, \dots, a_r$ попарно взаимно просты. Тогда каждый элемент C из $\mathfrak{G}$ можно одним и только одним способом представить в виде*

$$C = A_1 \dots A_r,$$

где

$$A_1^{a_1} = A_2^{a_2} = \dots = A_r^{a_r} = E.$$

В самом деле, определим r целых чисел $n_1, \dots, n_r$ так, чтобы

$$\frac{h}{a_1} n_1 + \dots + \frac{h}{a_r} n_r = 1,$$

что, в силу нашего предположения относительно a_i, всегда возможно по теореме 3. Если мы теперь положим

$$A_i = C^{\frac{h}{a_i} n_i} \quad (i = 1, \dots, r),$$

то по теореме 21

$$A_i^{a_i} = C^{h n_i} = E,$$

и, таким образом, C представлено в требуемом виде:

$$C = A_1 \dots A_r.$$

Чтобы убедиться в однозначности этого представления, допустим, что $C = B_1 \dots B_r$ есть другое представление требуемого вида. Тогда

$$(B_1 \dots B_r)^{\frac{h}{a_1}} = (A_1 \dots A_r)^{\frac{h}{a_1}}. \tag{9}$$

Но так как композиция коммутативна (что мы лишь теперь впервые используем), то из (9) следует

$$B_1^{\frac{h}{a_1}} \dots B_r^{\frac{h}{a_1}} = A_1^{\frac{h}{a_1}} \dots A_r^{\frac{h}{a_1}}.$$

Так как $\frac{h}{a_1}$ делится на каждое из чисел $a_2, \dots, a_r$, то, по предположенному относительно A_i, B_i, множители с индексами $2, 3, \dots, r$ должны быть равны E, и, следовательно,

$$B_1^{\frac{h}{a_1}} = A_1^{\frac{h}{a_1}}$$

Но $\left(a_1, \frac{h}{a_1}\right) = 1$, поэтому существуют такие целые числа x и y, что $a_1 x + \frac{h}{a_1} y = 1$. Принимая теперь во внимание, что

$$E = B_1^{a_1} = A_1^{a_1},$$

мы получим

$$B_1 = B_1^{a_1 x + \frac{h}{a_1} y} = A_1^{a_1 x + \frac{h}{a_1} y} = A_1.$$

Аналогично получаем $A_i = B_i$ для всех i, и однозначность рассматриваемого представления доказана.

Пусть a_i' есть число различных элементов A, обладающих тем свойством, что

$$A^{a_i} = E;$$

очевидно, что совокупность этих элементов образует подгруппу порядка a_i' группы $\mathfrak{G}$, так как произведение двух таких элементов опять обладает тем же свойством. Из теоремы 23 вытекает, что

$$h = a_1' \ldots a_r' = a_1 \ldots a_r. \tag{10}$$

Покажем, что

$$a_i' = a_i \quad (i = 1, \ldots, r).$$

В самом деле, если p есть простое число и $p \mid a_i'$, то по теореме 22 среди элементов A, обладающих свойством $A^{a_i} = E$, существует элемент порядка p, а следовательно, $p \mid a_i$. Поэтому a_i' не содержит никаких простых делителей, не входящих в a_i. В силу равенства (10), а также того, что числа a_i попарно взаимно просты, отсюда следует, что $a_i' = a_i$, $i = 1, \ldots, r$.

Тем самым мы доказали следующую теорему:

Теорема 24. *Если* $c \mid h$ *и* $\left(\frac{h}{c}, c\right) = 1$ $(c > 0)$, *то совокупность элементов группы* $\mathfrak{G}$, *обладающих свойством*

$$A^c = E,$$

образует подгруппу порядка c.

Теорема 23 приводит к мысли ввести специальное название для отношения группы $\mathfrak{G}$ к r подгруппам, к которым принадлежат соответственно $A_1, \ldots, A_r$ и из которых, согласно этой теореме, может быть построена группа $\mathfrak{G}$. Можно назвать $\mathfrak{G}$ „произведением“ этих подгрупп. Однако, если хотят, исходя из двух групп $\mathfrak{G}_1$ и $\mathfrak{G}_2$, лишь определить группу $\mathfrak{G}$, которая содержала бы $\mathfrak{G}_1$ и $\mathfrak{G}_2$ в качестве подгрупп и могла бы быть названа произведением этих подгрупп, то надо принять во внимание, что заранее „произведение“ какого-либо элемента из $\mathfrak{G}_1$ и какого-либо элемента из $\mathfrak{G}_2$ еще не имеет смысла.

Мы поступим поэтому следующим образом. Элементы абелевой группы $\mathfrak{G}_i$ $(i = 1, 2)$ мы будем отмечать индексом i. Определим теперь новую группу, элементами которой являются *пары* (A_1, A_2), следующими условиями:

1. $(A_1, A_2) = (B_1, B_2)$ означает, что $A_1 = B_1$ и $A_2 = B_2$.
2. Правилом композиции для пар (A_1, A_2), (B_1, B_2) является

$$(A_1, A_2)(B_1, B_2) = (A_1 B_1, A_2 B_2).$$

Этими условиями h_1h_2 новых элементов (где h_i есть порядок группы $\mathfrak{G}_i$) объединены в абелеву группу $\mathfrak{G}$. Ее единичным элементом служит (E_1, E_2), где E_i означает единичный элемент группы $\mathfrak{G}_i$. h_i элементов (A_1, E_2), где A_1 пробегает группу $\mathfrak{G}_1$, очевидно, образуют подгруппу группы $\mathfrak{G}$, изоморфную с $\mathfrak{G}_1$; таким же образом группа элементов (E_1, A_2) изоморфна с $\mathfrak{G}_2$. Обе подгруппы имеют только один общий элемент (E_1, E_2). Каждый элемент из $\mathfrak{G}$ можно одним и только одним способом представить в виде произведения из двух элементов обеих подгрупп:

$$(A_1, A_2) = (A_1, E_2)(E_1, A_2).$$

Наконец, мы полагаем, по определению,

3. $(A_1, E_2) = A_1$, $(E_1, A_2) = A_2$, в частности, следовательно, $E_1 = E_2$.

Эти определения соотношений равенств правомерны, так как между элементами групп $\mathfrak{G}$, $\mathfrak{G}_1$ и $\mathfrak{G}_2$ соотношение равенства еще не было определено, и при композиции элементов, определяемых здесь как равные, получаются и в результате равные элементы. Определенную, таким образом, условиями 1, 2 и 3 группу $\mathfrak{G}$ с h_1h_2 элементами A_1A_2 мы называем *произведением* групп $\mathfrak{G}_1$ и $\mathfrak{G}_2$ и пишем

$$\mathfrak{G} = \mathfrak{G}_1\mathfrak{G}_2 = \mathfrak{G}_2\mathfrak{G}_1.$$

Пользуясь этой терминологией, мы, в силу ассоциативности определенного сейчас произведения групп, получаем из теоремы 23 следующую теорему:

Теорема 25. *Каждая конечная абелева группа может быть представлена в виде произведения абелевых групп, порядками которых являются степени простых чисел.*

§ 8. Базис абелевой группы

Мы теперь можем доказать следующую теорему, дающую полное представление о структуре самой общей конечной абелевой группы

Теорема 26. (*Основная теорема теории абелевых групп.*) *В каждой конечной абелевой группе $\mathfrak{G}$ порядка h (>1) существуют такие элементы $B_1, \ldots, B_r$, соответственно, порядков $h_1, \ldots, h_r$ $(h_i > 1)$, что каждый элемент из $\mathfrak{G}$ одним и только одним способом представляется в виде*

$$C = B_1^{x_1} \ldots B_r^{x_r},$$

когда x_i, независимо друг от друга, пробегают полные системы вычетов соответственно по модулям h_i. Далее, h_i являются степенями простых чисел, $h_i = p_i^{k_i}$, и $h = h_1 \ldots h_r$.

r элементов такого рода называются *базисом* группы $\mathfrak{G}$.

Согласно теореме 25, справедливость этой теоремы будет доказана для абелевых групп любого порядка h, если она будет установлена для абелевых групп, порядки которых суть степени простых чисел.

Пусть, следовательно, теперь порядок h группы $\mathfrak{G}$ равен p^k, где p есть простое число и k — целое $\geqslant 1$. Порядок каждого элемента из $\mathfrak{G}$ равен тогда p^α, где $0 \leqslant \alpha \leqslant k$, α — целое.

Систему из m элементов $A_1, \ldots, A_m$, соответственно, порядков $a_1, \ldots, a_m$ мы будем называть *независимой*, если из $A_1^{x_1} \ldots A_m^{x_m} = E$ следует $x_i \equiv 0 \pmod{a_i}$ для $i = 1, \ldots, m$. Например, каждый элемент A сам по себе есть независимый элемент, так что независимые системы существуют. Всевозможные произведения степеней m независимых элементов A_i, соответственно, порядков a_i, очевидно, образуют группу, содержащую точно $a_1 \ldots a_m$ различных элементов. Вместе с $A_1, \ldots, A_m$ также $m+1$ элементов $A_1, \ldots, A_m, E$ всегда независимы, и обратно. Мы условимся теперь всегда нумеровать независимые элементы так, чтобы их порядки образовывали убывающий ряд:

$$a_1 \geqslant a_2 \geqslant \ldots \geqslant a_m \geqslant 1.$$

Систему чисел $a_1, a_2, \ldots, a_m$ мы будем называть системой ранговых чисел для $A_1, \ldots, A_m$ или рангом R системы $A_1, \ldots, A_m$. Введем теперь определенное расположение среди систем R. Пусть заданы две независимые системы:

$$A_i \text{ порядка } a_i = p^{\alpha_i} \quad (i = 1, \ldots, m)$$

и

$$B_q \text{ порядка } b_q = p^{\beta_q} \quad (q = 1, \ldots, n).$$

В случае если $m \neq n$ и, скажем, $m > n$, мы положим $\beta_{n-1} = \beta_{n+2} = \ldots = \beta_m = 0$. Заданные системы мы будем называть системами равного ранга, если $\alpha_i = \beta_i$ для $i = 1, \ldots, m$. В противном случае мы будем говорить, что ранг системы $(A_1, \ldots, A_m)$ выше или ниже ранга системы $(B_1, \ldots, B_n)$, в зависимости от того, будет ли первая не равная нулю разность $\alpha_i - \beta_i$ положительна или отрицательна. Опускание или присоединение элементов E не меняет, таким образом, расположения ранга данной системы относительно рангов других систем. Если ранг системы $(A_1, \ldots)$ выше ранга системы $(B_1, \ldots)$, а последний выше ранга системы $(C_1, \ldots)$, то ранг системы $(A_1, \ldots)$ выше также ранга системы $(C_1, \ldots)$. Очевидно, что для рангов систем независимых и отличных от E элементов группы $\mathfrak{G}$ порядка h может представиться не больше h^h возможностей, следовательно, существуют системы независимых элементов с наивысшим возможным рангом; такие системы мы коротко будем называть максимальными системами. Пусть будет $(B_1, \ldots, B_r)$ максимальная система, в которой ни один элемент не равен E. *Мы покажем, что* $B_1, \ldots, B_r$ *есть система базисных элементов.* Для этого мы должны лишь показать, что каждый элемент из $\mathfrak{G}$ может быть представлен в виде произведения степеней элементов B_i. Докажем предварительно следующие три леммы:

Лемма а). *Среди элементов* $B_1, \ldots, B_r$ *ни один не может быть* p*-й степенью элемента из* $\mathfrak{G}$.

В самом деле, если бы, например, $B_m = C^p$, то система, полученная из $B_1, \ldots, B_r$ путем замены B_m на C и возможного изменения

нумерации, также была бы независимой, но, очевидно, более высокого ранга, чем система $B_1, \ldots, B_r$, что невозможно.

Лемма b). *Если в системе* $B_1, \ldots, B_r$ *один из элементов, например* B_m, *заменить на*

$$A = B_m^u B_{m+1}^{x_{m+1}} \ldots B_r^{x_r},$$

где $u \not\equiv 0 \pmod p$, *а* x_i — *произвольные целые числа, то ранг не изменится, и новая система также будет максимальной.*

В самом деле, A имеет тот же порядок, что и B_m, так как порядки элементов $B_{m+1}, \ldots, B_r$ не больше порядка элемента B_m и, значит, являются его делителями. Далее, каждое произведение степеней элементов $A, B_{m+1}, \ldots, B_r$ может быть также представлено в виде произведения степеней элементов $B_m, B_{m+1}, \ldots, B_r$, и обратно. Поэтому новая система также независима, а следовательно, есть максимальная система.

Лемма c). *Если элемент* C^p *может быть представлен в виде произведения степеней* B_i, *то то же самое имеет место и для* C.

В самом деле, если

$$C^p = B_1^{x_1} \ldots B_r^{x_r}, \tag{11}$$

то все $x_i \equiv 0 \pmod p$. Действительно, если бы $x_m = u$ был первый показатель, не делящийся на p, то в системе элементов B_i мы бы заменили B_m на

$$A = B_m^u B_{m+1}^{x_{m+1}} \ldots B_r^{x_r} = C^p B_1^{-x_1} \ldots B_{m-1}^{-x_{m-1}}$$

Эта новая система была бы, согласно лемме b), опять максимальной системой, но содержала бы элемент A, являющийся p-й степенью некоторого элемента, что противоречит лемме a). Таким образом в (11) можно положить $x_i = py_i$, где y_i — целые, а потому

$$(C^{-1} B_1^{y_1} \ldots B_r^{y_r})^p = E.$$

Если бы теперь элемент C не мог быть представлен в виде произведения степеней элементов B_i, то то же самое имело бы место для всех C^n при $n \not\equiv 0 \pmod p$, и стоящее выше в скобках выражение

$$C' = C^{-1} B_1^{y_1} \ldots B_r^{y_r},$$

отличное от E, было бы, следовательно, элементом порядка p. Поэтому $r+1$ элементов

$$B_1, \ldots, B_r, C'$$

были бы также независимы и правильно расположены по убывающим порядкам (так как порядок B_r больше единицы и поэтому $\geqslant p$) и представляли бы собой систему высшего ранга, чем система $B_1, \ldots, B_r$, что невозможно. Следовательно, наше предположение неправильно, и лемма c) доказана.

Но повторным применением леммы c) мы убеждаемся в возможности представления каждого элемента A из $\mathfrak{G}$ с помощью элементов B_i. В самом деле, если A имеет порядок p^m, то

$$A^{p^m} = E$$

во всяком случае может быть представлено при помощи элементов B_i, а потому, согласно лемме c), при помощи элементов B_i может быть представлено и $A^{p^{m-1}}$, а значит, и $A^{p^{m-2}}$, если $m > 1$, и т. д., пока мы не придем к $A^{p^0} = A$.

Итак, мы показали, что элементы $B_1, \ldots, B_r$ максимальной системы образуют базис группы $\mathfrak{G}$. Тем самым доказана и теорема 26.

Элементы базиса абелевой группы $\mathfrak{G}$ не определяются этой группой однозначно. Однако некоторые свойства базиса характеристичны для самой группы $\mathfrak{G}$. Важнейшей константой, определяемой лишь самой группой $\mathfrak{G}$, является число $e = e(p)$ тех элементов базиса, порядки которых делятся на простое число p; мы называем *e базисным числом, принадлежащим p*. Независимость этого числа от выбора базисных элементов устанавливается следующей теоремой:

Теорема 27. *Если p есть простое число, то количество различных элементов группы* $\mathfrak{G}$, *обладающих свойством*

$$A^p = E,$$

равно p^e, *где e есть базисное число, принадлежащее p.*

Доказательство этой теоремы проводится следующим образом. Пусть $B_1, \ldots, B_e$ — те базисные элементы, порядки которых являются степенями p. Из соотношений

$$A = B_1^{x_1} \ldots B_e^{x_e} B_{e+1}^{x_{e+1}} \ldots B_r^{x_r} \quad \text{и} \quad A^p = E$$

вытекает ряд сравнений

$$px_i \equiv 0 \pmod{h_i} \quad (i = 1, \ldots, r),$$

где h_i — порядок элемента B_i. Следовательно, для $i = e+1, \ldots, r$, в силу равенства $(h_i, p) = 1$, имеем $x_i \equiv 0 \pmod{h_i}$, а для $i = 1, \ldots, e$ в силу равенств $h_i = p^{k_i}$, будет $x_i \equiv 0 \pmod{\frac{h_i}{p}}$. И обратно, эти сравнения имеют своим следствием равенство $A^p = E$. Количество не сравнимых между собой по соответствующему модулю h_i решений каждого из этих сравнений есть 1 для $i = e+1, \ldots, r$ и p для $i = 1, \ldots, e$. Поэтому число систем несравнимых решений есть p^e.

Доказанное предложение справедливо также и в том случае, когда p не входит в порядок h группы, так как тогда $e = 0$.

Простейшие абелевы группы получаются путем возведения в степень одного элемента. Если все элементы абелевой группы являются степенями одного элемента A, то группа называется *циклической* и A называется *образующим элементом* группы. Здесь имеет место следующая теорема:

Теорема 28. *Абелева группа* $\mathfrak{G}$ *порядка* h *будет циклической тогда и только тогда, когда для каждого простого числа* p, *являющегося делителем* h, *число элементов* A, *для которых* $A^p = E$, *равно* p.

Согласно предыдущей теореме, это условие равносильно такому: базисное число, принадлежащее p, должно быть равно 1.

Это условие необходимо для цикличности группы. В самом деле, если

$$C;\ C^2, \ldots, C^{h-1},\ C^h = E$$

— h элементов группы $\mathfrak{G}$, то из $A^p = E$ следует при $A = C^x$

$$px \equiv 0 \pmod{h}$$

или

$$x \equiv 0 \pmod{\frac{h}{p}},$$

т. е. x имеет по модулю h одно из p значений $\frac{h}{p}, 2\frac{h}{p}, \ldots, p\frac{h}{p}$; и обратно, мы таким путем получаем p различных элементов A с $A^p = E$.

Но это условие также и достаточно. В самом деле, если разложение h на различные простые множители есть $h = p_1^{k_1} \ldots p_r^{k_r}$, то, по предположению, каждому p_i принадлежит только один базисный элемент; таким образом каждый элемент группы $\mathfrak{G}$ имеет вид

$$A = B_1^{x_1} \ldots B_r^{x_r},$$

где

$$B_i^{h_i} = E \quad \text{и} \quad h_i = p_i^{k_i}.$$

Но мы получим тогда h различных элементов, а значит, — все элементы группы $\mathfrak{G}$, если образуем, например, последовательные степени элемента

$$C = B_1 \ldots B_r.$$

В самом деле, если u есть порядок C, то в силу того, что элементы B_i образуют базис,

$$u \equiv 0 \pmod{h_i} \quad \text{для} \quad i = 1, \ldots, r,$$

и так как числа h_i попарно взаимно просты, то u делится на $h_1 \ldots h_r = h$, а потому $u = h$, так как u не может быть больше h.

§ 9. Композиция смежных классов. Факторгруппы

Пусть $\mathfrak{U}$ — подгруппа абелевой группы $\mathfrak{G}$ порядка h. С ее помощью можно образовать новую группу следующим образом. Вместе с $\mathfrak{U}$ однозначно определены, согласно сказанному в § 6, также смежные классы $A\mathfrak{U}$. Их число есть $\frac{h}{N}$, где N — порядок подгруппы $\mathfrak{U}$; мы их обозначим через $R_1, R_2, \ldots$ Эти смежные классы R_i обладают

следующим свойством: Если A_1 и A_1' — элементы из R_1, A_2 и A_2' — элементы из R_2, то A_1A_2 и $A_1'A_2'$ принадлежат одному и тому же смежному классу R_3. В самом деле,

$$A_1' = A_1U_1, \quad A_2' = A_2U_2,$$

где U_1 и U_2 — элементы из $\mathfrak{U}$; таким образом $A_1'A_2' = A_1A_2U_1U_2$ (здесь мы опираемся на то, что композиция элементов в $\mathfrak{G}$ коммутативна). Так как A_1A_2 и $A_1'A_2'$ отличаются только множителем из $\mathfrak{U}$, то они принадлежат одному и тому же смежному классу R_3. Таким образом смежные классы R_1 и R_2 однозначно определяют смежный класс R_3, который можно рассматривать как получающийся в результате их композиции и обозначать в виде

$$R_3 = R_1R_2.$$

При этом способе композиции смежных классов R групповые аксиомы I — III выполняются. Кроме того, очевидно, что эта композиция также коммутативна. Поэтому классы смежности R образуют абелеву группу $\mathfrak{R}$ порядка $\frac{h}{N}$.

Определение. Определенная таким образом группа $\mathfrak{R}$ называется *факторгруппой группы* $\mathfrak{G}$ *по подгруппе* $\mathfrak{U}$ и обозначается так:

$$\mathfrak{R} = \mathfrak{G}/\mathfrak{U}.$$

Ее порядок равен индексу подгруппы $\mathfrak{U}$.

Мы можем описать группу $\mathfrak{R}$ также следующим образом: она получается из $\mathfrak{G}$, если два элемента из $\mathfrak{G}$, отличающиеся друг от друга только множителем, принадлежащим $\mathfrak{U}$, рассматривать как неразличные и если в остальном сохранить правило композиции, установленное в $\mathfrak{G}$.

В дальнейшем мы будем пользоваться введенным только что понятием преимущественно в том случае, когда $\mathfrak{U}$ есть группа тех элементов из $\mathfrak{G}$, которые могут быть представлены как p-е степени элементов из $\mathfrak{G}$, где p есть простое число, входящее в порядок h группы $\mathfrak{G}$. Эту подгруппу $\mathfrak{U}$ мы теперь обозначим через $\mathfrak{U}_p$. Имеет место следующая теорема:

Теорема 29. *Порядок факторгруппы* $\mathfrak{G}/\mathfrak{U}_p$ *есть* p^e, *где* e *есть базисное число, принадлежащее в* $\mathfrak{G}$ *простому числу* p. *Группа* $\mathfrak{G}/\mathfrak{U}_p$ *изоморфна группе тех элементов* C *из* $\mathfrak{G}$, *для которых* $C^p = E$.

В самом деле, нетрудно видеть, что каждый элемент группы $\mathfrak{G}$, порядок которого не содержит простого числа p, есть p-я степень некоторого элемента из $\mathfrak{G}$ (именно, некоторой своей степени). Поэтому теорема 26 показывает, что каждый элемент X из $\mathfrak{G}$ может быть представлен в виде

$$X = B_1^{x_1} \dots B_e^{x_e} A^p,$$

где $B_1, \ldots, B_e$ суть e базисных элементов, принадлежащих простому числу p, причем e чисел $x_1, \ldots, x_e$ элементом X однозначно определены по модулю p, а A^p есть соответственным образом выбранная p-я степень, т. е. элемент из $\mathfrak{U}_p$. Из единственности разложения по степеням базисных элементов явствует, что X есть p-я степень тогда и только тогда, когда все $x_i \equiv 0 \pmod p$. Следовательно, количество различных классов смежности, определяемых подгруппой $\mathfrak{U}_p$, равно количеству систем x_i, различных по модулю p, т. е. равно p^e. p-я степень каждого смежного класса совпадает с самой подгруппой $\mathfrak{U}_p$, т. е. в группе $\mathfrak{G}/\mathfrak{U}_p$ порядка p^e каждый элемент, отличный от единичного, имеет порядок p. Поэтому, в силу теоремы 27, $\mathfrak{G}/\mathfrak{U}_p$ необходимо содержит точно e базисных элементов, каждый порядка p. Такую же структуру имеет по теореме 27 также группа элементов C из $\mathfrak{G}$ с $C^p = E$. Кроме того, нетрудно видеть, что в факторгруппе систему базисных элементов образуют e смежных классов

$$B_i\mathfrak{U} \qquad (i = 1, \ldots, e),$$

а в группе элементов C из $\mathfrak{G}$ с $C^p = E$ базис образуют e элементов

$$B_i^{\frac{h_i}{p}} \qquad (i = 1, \ldots, e).$$

Обе группы поэтому изоморфны.

§ 10. Характеры абелевых групп

Так как композиция в абелевой группе коммутативна, как обыкновенное умножение, то в силу символического равенства $A^h = 1$, элементы этой группы формально ведут себя, как корни h-й степени из единицы, т. е. как известные числа, и естественным является вопрос, нельзя ли вообще свести исследование абелевой группы к некоторым вопросам теории чисел, например, тем способом, что каждому элементу A данной абелевой группы $\mathfrak{G}$ будет отнесено число, — обозначим его через $\chi(A)$, — и притом так, чтобы для каждых двух элементов A, B из $\mathfrak{G}$ всегда имело место равенство

$$\chi(A)\chi(B) = \chi(AB), \tag{12}$$

т. е. чтобы композиции элементов отвечало умножение соответствующих чисел.

Все отвечающие этим требованиям „функции“ $\chi(A)$ можно, в силу основной теоремы теории абелевых групп (см. теорему 26), найти следующим образом.

Тривиальное решение „$\chi(A) = 0$ для всех A“ мы оставим в стороне.

Прежде всего для единичного элемента должно быть

$$\chi(E) = 1.$$

В самом деле, для каждого A

$$\chi(A)\chi(E) = \chi(AE) = \chi(A).$$

Пусть, далее, $B_1, \ldots, B_r$ — базис группы $\mathfrak{G}$ и

$$A = B_1^{x_1} \ldots B_r^{x_r}$$

Повторным применением равенства (12) получаем

$$\chi(A) = \chi(B_1)^{x_1} \ldots \chi(B_r)^{x_r}. \tag{13}$$

Таким образом $\chi(A)$ известно для каждого элемента A, если оно известно для r базисных элементов B_i. Однако значения $\chi(B_i)$ не произвольны, а должны быть выбраны так, чтобы все системы показателей x_i, которые приводят к одному и тому же A, давали бы в (13) для $\chi(A)$ одно и то же значение. Это значит, что $\chi(B_i)$ должно быть таким числом, чтобы $\chi(B_i)^{x_i}$ зависело только от значения x_i по модулю h_i. Теперь, в силу равенств

$$1 = \chi(E) = \chi(B_i^{h_i}) = \chi(B_i)^{h_i},$$

$\chi(B_i)$ отлично от нуля и есть корень h_i-й степени из единицы. Но это условие также достаточно. В самом деле, пусть будут

$$\chi(B_m) = \zeta_m \quad (m = 1, \ldots, r)$$

— какие-нибудь корни соответственно h_m-х степеней из единицы,

$$\zeta_m = e^{\frac{2\pi i}{h_m} a_m} \quad (a_m \text{ — произвольное целое число, } m = 1, \ldots, r).$$

Тогда для $A = B_1^{x_1} \ldots B_r^{x_r}$ положим

$$\chi(A) = \zeta_1^{x_1} \ldots \zeta_r^{x_r}. \tag{14}$$

Так как выражение $\chi(A)$ зависит только от того, какому классу по модулю h_m принадлежат числа x_m, и так как эти классы однозначно определяются элементом A, то $\chi(A)$ таким образом однозначно определено и удовлетворяет также требованию (12). Но корней h_m-й степени из 1 существует точно h_m, соответственно значениям $a_m = 1, \ldots, h_m$. Следовательно, существует точно $h = h_1 \ldots h_r$ формально различных функций $\chi(A)$, причем никакие две из них, действительно, не совпадают для всех элементов, так как они различны по крайней мере для одного базисного элемента. Этим доказана следующая теорема:

Теорема 30. *Для каждой абелевой группы $\mathfrak{G}$ порядка h существует точно h различных функций $\chi(A)$, обладающих тем свойством, что $\chi(AB) = \chi(A)\chi(B)$ и $\chi(A)$ отлично от нуля для всех элементов A из $\mathfrak{G}$. Каждое χ есть корень h-й степени из единицы.*

Каждая такая функция $\chi(A)$ называется *групповым характером* или *характером* группы $\mathfrak{G}$.

Среди характеров $\chi(A)$ один равен единице для всех A из $\mathfrak{G}$; он называется *главным характером*. Обратно, существует точно один

элемент группы $\mathfrak{G}$, а именно E, такой, что $\chi(E)=1$ для каждого характера этой группы.

Самые характеры также можно объединить в абелеву группу порядка h. В самом деле, если $\chi_1(A)$ и $\chi_2(A)$ — характеры, то $f(A)=\chi_1(A)\chi_2(A)$ также удовлетворяет условиям, определяющим характер, и, значит, также есть характер группы $\mathfrak{G}$. Если $\chi(A)$ пробегает все характеры группы $\mathfrak{G}$, а $\chi_1(A)$ есть какой-нибудь определенный фиксированный характер этой группы, то $\chi(A)\chi_1(A)$ также пробегает все характеры группы $\mathfrak{G}$. Будем под $\sum_A$ понимать сумму, распространенную на все h элементов A из $\mathfrak{G}$, а под $\sum_\chi$ — сумму, распространенную на все h характеров χ. Имеет место следующая теорема:

ТЕОРЕМА 31.

$$\sum_A \chi(A)=\begin{cases} h, & \text{если } \chi \text{ есть главный характер},\\ 0, & \text{если } \chi \text{ не есть главный характер}.\end{cases}$$

$$\sum_\chi \chi(A)=\begin{cases} h, & \text{если } A=E,\\ 0, & \text{если } A\neq E.\end{cases}$$

Первая половина каждого из этих утверждений тривиальна, так как в этом случае каждое из слагаемых равно единице. Пусть теперь B — произвольный элемент группы $\mathfrak{G}$. Тогда вместе с A также AB пробегает все элементы из $\mathfrak{G}$, следовательно,

$$\sum_A \chi(A)=\sum_A \chi(AB)=\chi(B)\sum_A \chi(A),$$

и, значит,

$$(1-\chi(B))\sum_A \chi(A)=0.$$

Но если χ не есть главный характер, то $\chi(B)\neq 1$ по крайней мере для одного B, а потому $\sum_A \chi(A)=0$.

Точно так же, пусть χ_1 — произвольный характер группы $\mathfrak{G}$, тогда

$$\sum_\chi \chi(A)=\sum_\chi \chi_1(A)\chi(A)=\chi_1(A)\sum_\chi \chi(A),$$

и, значит,

$$(1-\chi_1(A))\sum_\chi \chi(A)=0.$$

Если $A\neq E$, то $\chi_1(A)\neq 1$ по крайней мере для одного характера χ_1, а потому $\sum_\chi \chi(A)=0$.

Пусть $\chi_1,\ldots,\chi_h$ будут h характеров группы $\mathfrak{G}$. Каждый элемент A группы $\mathfrak{G}$ однозначно определяется h числами $\chi_n(A)$. В самом деле, если бы какой-нибудь другой элемент B имел те же самые значения

$\chi_n(B)=\chi_n(A)$, то $\chi_n(AB^{-1})$ было бы равно единице для всех n, и, в силу теоремы 31, AB^{-1} было бы единичным элементом, так что $B=A$.

Однако h чисел $\chi_n(A)$ не произвольны, а именно, имеет место следующая теорема:

Теорема 32. *Если A есть элемент порядка f, то $\chi_n(A)$ есть корень f-й степени из единицы для всех характеров χ_n. Среди h чисел $\chi_n(A)$, $n=1,\ldots,h$, все корни f-й степени из единицы встречаются одинаково часто, а именно, по $\frac{h}{f}$ раз.*

Действительно, так как $A^f=E$, то

$$(\chi_n(A))^f=\chi_n(A^f)=\chi_n(E)=1,$$

следовательно, первая часть теоремы доказана. Пусть теперь ζ — произвольный корень f-й степени из единицы. Рассмотрим сумму

$$\sum_{n=1}^{h}\{\zeta^{-1}\chi_n(A)+\zeta^{-2}\chi_n(A^2)+\ldots+\zeta^{-f}\chi_n(A^f)\}=S.$$

Так как, по предположению, A^m не есть единичный элемент при $1\leqslant m\leqslant f$ (исключая тривиальный случай $f=1$, т. е. $A=E$), то, разбивая сумму S на f отдельных сумм, заключаем из теоремы 31, что $S=h$.

С другой стороны, выражение в каждой скобке равно $\varepsilon+\varepsilon^2+\ldots+\varepsilon^f$, где

$$\varepsilon=\zeta^{-1}\chi_n(A),\quad \varepsilon^f=1,$$

а потому равно 0 или f, в зависимости от того, будет ли $\varepsilon\neq 1$ или $=1$, т. е. будет ли $\chi_n(A)\neq\zeta$ или $=\zeta$. Отсюда следует, что $S=kf$, где k означает число тех характеров $\chi_n(A)$, для которых $\chi_n(A)=\zeta$, а потому, в связи с прежним результатом,

$$kf=h,\quad k=\frac{h}{f},$$

независимо от ζ, что и требовалось доказать.

Покажем, что *группа характеров группы $\mathfrak{G}$ изоморфна с самой группой $\mathfrak{G}$*. Отнесем каждому из базисных элементов B_q какой-либо первообразный корень h_q-й степени из единицы, скажем,

$$\zeta_q=e^{\frac{2\pi i}{h_q}},$$

и определим характер χ_q условиями $\chi_q(B_q)=\zeta_q$, $\chi_q(B_p)=1$ при $p\neq q$. Этими условиями характер χ_q действительно определяется: для любого элемента $A=B_1^{x_1}\ldots B_r^{x_r}$ из $\mathfrak{G}$ имеем $\chi_q(A)=\zeta_q^{x_q}=\chi_q(B_q^{x_q})$, и так как число χ_q определено по модулю h_q, то условие $\chi_q(AB)=\chi_q(A)\chi_q(B)$, очевидно, удовлетворяется. Теперь, характеры χ_q, $q=1,\ldots,h$, могут служить базисными элементами в группе харак-

теров группы $\mathfrak{G}$. Действительно, пусть χ — произвольный характер группы $\mathfrak{G}$. Так как $\chi(B_q)$ — корень h_q-й степени из единицы и $\zeta_q = \chi_q(B_q)$ — первообразный корень h_q-й степени из единицы, то $\chi(B_q) = \chi_q^{y_q}(B_q)$, где целое число y_q однозначно определено по модулю h_q характером χ. Тогда для любого $A = B_1^{x_1} \dots B_r^{x_r}$ из $\mathfrak{G}$ имеем

$$\chi(A) = \chi(B_1^{x_1}) \dots \chi(B_r^{x_r}) = \chi_1^{y_1}(B_1^{x_1}) \dots \chi_r^{y_r}(B_r^{x_r}) = \\ = \chi_1^{y_1}(A) \dots \chi_r^{y_r}(A),$$

причем числа y_q однозначно определены характером χ соответственно по модулям h_q и не зависят от A. Если мы теперь отнесем характеру

$$\chi = \chi_1^{y_1} \dots \chi_r^{y_r}$$

элемент

$$L_1^{y_1} \dots B_r^{y_r},$$

то этим, очевидно, будет установлен изоморфизм между группой характеров группы $\mathfrak{G}$ и самой группой $\mathfrak{G}$.

С помощью характеров абелевой группы можно задать каждую ее подгруппу. Если мы возьмем какие-нибудь k различных характеров $\chi_1, \dots, \chi_k$ группы $\mathfrak{G}$, то совокупность элементов U, для которых $\chi_1(U) = \chi_2(U) = \dots = \chi_k(U) = 1$, очевидно, образует подгруппу $\mathfrak{U}$ группы $\mathfrak{G}$, так как вместе с элементами U_1, U_2 также и их произведение $U_1 U_2$ обладает указанным свойством.

В том, что каждая подгруппа $\mathfrak{U}$ группы $\mathfrak{G}$ может быть получена этим способом, можно убедиться следующим образом. Пусть $\mathfrak{U}$ — произвольная подгруппа группы $\mathfrak{G}$ и j — ее индекс. Факторгруппа $\mathfrak{G}/\mathfrak{U}$, элементами которой являются различные смежные классы $A\mathfrak{U}$, есть абелева группа порядка j и соответственно с этим имеет точно j характеров, которые мы обозначим через $\lambda_1(A\mathfrak{U}), \dots, \lambda_j(A\mathfrak{U})$. С их помощью мы определим характер $\chi_k(A)$, положив

$$\chi_k(A) = \lambda_k(A\mathfrak{U}) \quad (k = 1, \dots, j).$$

Это определение однозначно, так как каждый элемент A принадлежит только одному смежному классу. Далее, для любых двух элементов A, B из $\mathfrak{G}$ всегда

$$\chi_k(A)\chi_k(B) = \lambda_k(A\mathfrak{U})\lambda_k(B\mathfrak{U}) = \lambda_k(AB\mathfrak{U}) = \chi_k(AB).$$

Таким образом $\chi_k(A)$ действительно есть характер группы $\mathfrak{G}$. Все характеры $\lambda_k(A\mathfrak{U})$, $k = 1, \dots, j$, одновременно принимают значение 1 только для единичного элемента группы $\mathfrak{G}/\mathfrak{U}$, т. е. для того смежного класса, который совпадает с самой подгруппой $\mathfrak{U}$. Поэтому все j характеров $\chi_k(A)$ одновременно принимают значение 1 для тех и только для тех элементов A, которые принадлежат подгруппе $\mathfrak{U}$. Иначе говоря, подгруппа $\mathfrak{U}$ может быть охарактеризована как совокупность тех элементов A, для которых выполняется j условий

$$\chi_k(A) = 1, \quad k = 1, \dots, j. \tag{15}$$

Однако эти j условий, которым должен удовлетворять каждый элемент A из $\mathfrak{U}$, не независимы между собой, так как вместе с χ_1 и χ_2 среди χ_k имеется также $\chi_1\chi_2 = \chi_3$, так что условие $\chi_3(A) = 1$ уже следует из условий $\chi_1(A) = \chi_2(A) = 1$. Чтобы установить количество независимых среди j условий (15), заметим, что совокупность характеров λ_k, однозначно определяющих характеры χ_k, как совокупность характеров группы $\mathfrak{G}/\mathfrak{U}$, образует изоморфную с ней группу и поэтому может быть представлена с помощью некоторого базиса, скажем, $\lambda_1, \ldots, \lambda_{r_0}$, где r_0 есть число элементов базиса группы $\mathfrak{G}/\mathfrak{U}$. Это значит, что каждый характер λ_k есть произведение степеней r_0 характеров базиса. Таким образом из r_0 условий

$$\chi_1(A) = \chi_2(A) = \ldots = \chi_{r_0}(A) = 1$$

уже следует, что для A выполняются все j условий (15), а значит, вытекает и принадлежность A к $\mathfrak{U}$. Если h_i есть порядок базисного характера λ_i и ζ_i $(i = 1, \ldots, r_0)$ — произвольно заданные корни h_i-й степени из единицы, то, как явствует из определения базисных характеров (см. стр. 40—41), всегда существует такой смежный класс $A\mathfrak{U}$, что $\lambda_i(A\mathfrak{U}) = \zeta_i$ при $i = 1, \ldots, r_0$. Этим доказана следующая теорема:

Теорема 33. *Пусть $\mathfrak{U}$ — подгруппа абелевой группы $\mathfrak{G}$ порядка h, и факторгруппа $\mathfrak{G}/\mathfrak{U}$ имеет r_0 базисных элементов. Тогда среди h характеров группы $\mathfrak{G}$ имеется r_0 характеров χ_i, порядки которых h_i $(i = 1, \ldots, r_0)$ суть степени простых чисел, причем эти характеры обладают тем свойством, что r_0 условий*

$$\chi_i(A) = 1 \quad (i = 1, \ldots, r_0)$$

выполняются для всех элементов A из $\mathfrak{U}$ и только для них, и, с другой стороны, в $\mathfrak{G}$ всегда существуют такие элементы B, для которых указанные r_0 характеров $\chi_i(B)$ суть какие-либо произвольно заданные корни h_i-й степени из единицы.

§ 11. Бесконечные абелевы группы

Теория бесконечных абелевых групп в настоящее время ни в каком направлении не достигла еще такой законченности, как только что развитая теория конечных абелевых групп. Немногие установленные здесь предложения относятся к группам еще более специального вида. В этом параграфе мы выясним те понятия и факты из теории абелевых групп бесконечного порядка, которые найдут применение в дальнейшем нашем изложении. Заметим, впрочем, что мы будем нуждаться в теории бесконечных абелевых групп лишь начиная с четвертой главы, в теории полей.

В бесконечной группе $\mathfrak{G}$ мы различаем элементы конечного порядка и элементы *бесконечного порядка*, в зависимости от того, равна ли E некоторая степень элемента или нет, — конечно, исключая нулевую степень. Как дальше будет показано на примерах, может случиться, что бесконечная абелева группа содержит только элементы бесконеч-

ного порядка (исключая E) или же только элементы конечного порядка. Систему конечного числа элементов из $\mathfrak{G}$

$$A_1, \ldots, A_r, \quad T_1, \ldots, T_q,$$

где каждое A_i имеет бесконечный порядок, а каждое T_k — конечный порядок h_k, мы называем *независимой*, если соотношение

$$A_1^{x_1} \ldots A_r^{x_r} T_1^{y_1} \ldots T_q^{y_q} = E$$

с целыми x, y имеет место только тогда, когда все $x_i = 0$ и каждое $y_k \equiv 0 \pmod{h_k}$. В этом случае выражение в левой части, очевидно, дает различные элементы, если каждое x_i пробегает все целые (положительные и отрицательные) числа, а каждое y_i — полную систему вычетов по модулю h_i.

Система из конечного или бесконечного количества элементов из $\mathfrak{G}$: A_i $(i = 1, 2, \ldots)$, T_k $(k = 1, 2, \ldots)$ (A_i — элементы бесконечного порядка, T_k — конечного) называется *базисом* группы $\mathfrak{G}$, если каждый элемент из $\mathfrak{G}$ можно представить в виде

$$C = A_1^{x_1} A_2^{x_2} \ldots T_1^{y_1} T_2^{y_2} \ldots,$$

причем: 1) показатели x_i и y_k суть целые числа, из которых только конечное число отлично от нуля, и 2) элементом C показатели x_i определяются однозначно, а показатели y_k — однозначно по модулю h_k.

Очевидно, что любая конечная подсистема элементов базиса должна быть независимой. Требование, чтобы порядки h_k были степенями простых чисел, мы здесь для простоты не будем ставить.

Базис называется *конечным*, если он состоит из конечного числа элементов.

Теорема 34. *Если бесконечная абелева группа $\mathfrak{G}$ имеет конечный базис, то каждая ее подгруппа тоже имеет конечный базис.*

Пусть $B_1, \ldots, B_m$ — базис группы $\mathfrak{G}$, причем $B_1, \ldots, B_r$ — элементы базиса, имеющие бесконечный порядок, и $B_{r+1}, \ldots, B_m$ — имеющие конечные порядки; мы обозначим эти порядки соответственно через $h_1, \ldots, h_{m-r}$. Рассмотрим системы показателей всех произведений степеней

$$U = B_1^{u_1} \ldots B_m^{u_m},$$

принадлежащих подгруппе $\mathfrak{U}$; пусть при этом последние $m - r$ показателей $u_{r+1}, \ldots, u_m$ также пробегают все целые числа, а не только лишь различные по модулям h_i, — лишь бы только соответственное произведение принадлежало подгруппе $\mathfrak{U}$. Так как $\mathfrak{U}$ есть группа, то очевидно, что вместе с системами показателей $(u_1, \ldots, u_m)$ и $(u'_1, \ldots, u'_m)$ всегда имеются также элементы U с системами показателей $(u_1 + u'_1, \ldots, u_m + u'_m)$ и $(u_1 - u'_1, \ldots, u_m - u'_m)$. Рассмотрим, в частности, для определенного k, $1 \leqslant k \leqslant m$, принадлежащие $\mathfrak{U}$ элементы вида

$$U = B_k^{z_k} B_{k+1}^{z_{k+1}} \ldots B_m^{z_m}, \tag{16}$$

у которых, следовательно, $u_1 = \ldots = u_{k-1} = 0$; такие элементы существуют, так как, когда все u_t равны нулю, мы получаем единичный элемент, который содержится в $\mathfrak{U}$. Совокупность возможных в (16) первых показателей z_k образует модуль в смысле § 1, если только z_k не всегда равно нулю. Но все числа модуля совпадают с кратными определенного целого числа; поэтому, если не всегда $z_k = 0$, то в $\mathfrak{U}$ существует элемент

$$U_k = B_k^{r_k} B_{k+1}^{r'_{k+1}} \ldots$$

с таким $r_k \neq 0$, что в (16) z_k есть кратное этого r_k. Среди элементов U_k с этим r_k — их, возможно, имеется бесконечное множество — мы выберем для каждого $k = 1, \ldots, m$ один определенный, причем, если в (16) для этого k z_k всегда равно нулю, то мы положим $U_k = E$, $r_k = 0$.

Покажем, что каждый элемент из $\mathfrak{U}$ может быть представлен в виде произведения степеней выбранных нами элементов $U_1, \ldots, U_m$. В самом деле, пусть

$$U = B_1^{u_1} \ldots B_m^{u_m}$$

— некоторый элемент из $\mathfrak{U}$. Согласно предыдущему, u_1 есть кратное r_1, $u_1 = v_1 r_1$, и поэтому

$$UU_1^{-v_1} = B_2^{u'_2} B_3^{u'_3} \ldots B_m^{u'_m} \tag{17}$$

есть произведение степеней уже только элементов $B_2, \ldots, B_m$, которое в силу свойства группы также принадлежит $\mathfrak{U}$. Если бы было $r_1 = 0$, $U_1 = E$, то мы положили бы $v_1 = 0$. Таким же образом, если $r_2 \neq 0$, то u'_2 в (17) должно быть кратным r_2, $u'_2 = v_2 r_2$. Если же $r_2 = 0$, то и $u'_2 = 0$, и мы тогда полагаем $v_2 = 0$. В обоих случаях $UU_1^{-v_1} U_2^{-v_2}$ есть элемент из $\mathfrak{U}$, представляющийся в виде произведения степеней одних только элементов $B_3, \ldots, B_m$. Продолжая этот процесс, мы придем в конце концов к единичному элементу и получим тогда представление

$$U = U_1^{v_1} U_2^{v_2} \ldots U_m^{v_m}.$$

Каждый из элементов $U_1, \ldots, U_r$, отличный от E, имеет бесконечный порядок, элементы же $U_{r+1}, \ldots, U_m$ имеют конечные порядки. Произведения степеней элементов $U_{r+1}, \ldots, U_m$ образуют конечную абелеву группу и могут поэтому быть представлены по теореме 26 с помощью некоторого базиса $C_1, \ldots, C_q$. Мы утверждаем теперь, что элементы $U_1, \ldots, U_r, C_1, \ldots, C_q$, после отбрасывания элементов U_i, равных E, образуют базис $\mathfrak{U}$. Прежде всего каждый элемент из $\mathfrak{U}$ можно представить с помощью $U_1, \ldots, U_m$, а потому и с помощью $U_1, \ldots, U_r, C_1, \ldots, C_q$. Если теперь

$$U_1^{v_1} \ldots U_r^{v_r} C_1^{c_1} \ldots C_q^{c_q} = E \tag{18}$$

есть представление единичного элемента, где $v_i = 0$, когда $U_i = E$ (т. е. $r_i = 0$), то, вставляя вместо U_i и C_k их выражения через B_i, мы получим прежде всего

$$v_1 r_1 = 0,$$

следовательно, либо $v_1 = 0$, либо $r_1 = 0$, но и в последнем случае, согласно условию, $v_1 = 0$. Таким же образом мы дальше получим $v_2 = 0, \ldots, v_r = 0$. Так как, далее, элементы C_k образуют базис конечной группы, то в (18) каждое c_k есть кратное порядка элемента C_k. Итак, единичный элемент группы $\mathfrak{U}$ единственным образом представляется в виде (18). Но каждый элемент группы $\mathfrak{U}$ может быть представлен с помощью U_i и C_k ровно столько раз, сколько единичный элемент. Поэтому элементы U_i и C_k действительно образуют базис группы $\mathfrak{U}$, что и требовалось доказать.

Главный интерес имеют для нас те бесконечные абелевы группы, которые не содержат никаких элементов конечного порядка, кроме единичного. Такие группы мы будем называть *группами без кручения*, остальные — *смешанными*. Одновременно с $\mathfrak{G}$ каждая ее подгруппа также есть группа без кручения. Пусть, в частности, $\mathfrak{U}$ будет подгруппа группы $\mathfrak{G}$ с конечным индексом (см. § 6). Тогда, каков бы ни был элемент из $\mathfrak{G}$, некоторая его степень с отличным от нуля показателем всегда принадлежит $\mathfrak{U}$. В самом деле, если A есть элемент из $\mathfrak{G}$, то смежные классы

$$A\mathfrak{U}, A^2\mathfrak{U}, \ldots, A^m\mathfrak{U}, .$$

не все различны между собой, так как, по предположению, индекс подгруппы $\mathfrak{U}$ конечен. Поэтому для какой-нибудь пары различных целых положительных чисел m, n должно иметь место равенство $A^m\mathfrak{U} = A^n\mathfrak{U}$, а тогда A^{m-n} будет принадлежать к $\mathfrak{U}$. Поэтому в вышеприведенном доказательстве теоремы 34, примененном к $\mathfrak{G}$ и $\mathfrak{U}$, не может случиться, чтобы $r_k = 0$, $U_k = E$, так как всегда существует система значений $z_k \neq 0$, $z_{k+1} = \ldots = z_m = 0$, при которой

$$U_k = B_k^{z_k}$$

принадлежит к $\mathfrak{U}$. Отсюда непосредственно получается следующая теорема:

Теорема 35. *Если $\mathfrak{G}$ есть абелева группа без кручения с конечным базисом $B_1, \ldots, B_n$, то каждая ее подгруппа $\mathfrak{U}$ с конечным индексом имеет базис $U_1, \ldots, U_n$ вида*

$$\begin{aligned}
U_1 &= B_1^{r_{11}} B_2^{r_{12}} \ldots B_n^{r_{1n}},\\
U_2 &= \quad B_2^{r_{22}} \ldots B_n^{r_{2n}},\\
&\ldots\ldots\ldots\ldots\\
&\ldots\ldots\ldots\ldots\\
U_n &= \qquad\qquad B_n^{r_{nn}},
\end{aligned}$$

где $r_{ii} \neq 0$ для $i = 1, \ldots, n$.

Теперь мы докажем следующую теорему:

Теорема 36. *Если подгруппа* $\mathfrak{U}$ *абелевой группы без кручения* $\mathfrak{G}$ *с конечным базисом имеет конечный индекс, то он равен* $|r_{11}r_{22}\dots r_{nn}|$, *где* $r_{11}, r_{22}, \dots, r_{nn}$ — *числа, определенные в теореме* 35.

Для доказательства мы должны установить, сколько существует в $\mathfrak{G}$ элементов, отличающихся не только множителем из $\mathfrak{U}$. Мы покажем прежде всего, что элемент

$$B_1^{x_1}\dots B_n^{x_n},$$

где все $|x_i| < r_{ii}$, принадлежит к $\mathfrak{U}$ только тогда, когда все $x_i = 0$. Действительно, согласно определению элементов U_i в доказательстве теоремы 34, x_1 должно делиться на r_{11}, и так как $|x_1| < r_{11}$, то $x_1 = 0$. Но тогда x_2 должно делиться на r_{22} и потому также $x_2 = 0$, и т. д.

Отсюда следует, далее, что среди $j = |r_{11}\dots r_{nn}|$ элементов

$$B_1^{z_1}\dots B_n^{z_n},\quad 0 \leqslant z_i < r_{ii}, \tag{19}$$

никакие два не отличаются только множителем из $\mathfrak{U}$; поэтому существует по крайней мере j различных смежных классов группы $\mathfrak{G}$ по подгруппе $\mathfrak{U}$, а именно, представленных каждым из этих элементов. Но, с другой стороны, из элементов (19) мы получим умножением на все элементы из $\mathfrak{U}$ каждый элемент из $\mathfrak{G}$. В самом деле, для любого произведения

$$P = B_k^{x_k}B_{k+1}^{x_{k+1}}\dots B_n^{x_n}$$

степеней базисных элементов $B_k, B_{k+1}, \dots, B_n$ можно всегда подобрать целое число b_k так, чтобы

$$PU_k^{-b_k} = B_k^{z_k}B_{k+1}^{z'_{k+1}}\dots,$$

причем первый показатель z_k уже удовлетворял условию $0 \leqslant z_k < r_{kk}$. Очевидно, что z_k есть наименьший положительный вычет числа x_k по модулю r_{kk}. Повторным применением этого рассуждения мы убедимся, что для каждого A из $\mathfrak{G}$ можно найти такую последовательность показателей $b_1, \dots, b_n$, что

$$AU_1^{-b_1}\dots U_n^{-b_n}$$

есть элемент из системы (19); таким образом A отличается от этого элемента только множителем из $\mathfrak{U}$. В совокупности с доказанным выше это показывает, что $j = |r_{11}\dots r_{nn}|$ есть точное значение индекса подгруппы $\mathfrak{U}$.

Мы займемся теперь исследованием связи между различными системами базисов группы $\mathfrak{G}$, чтобы найти те свойства базиса, которые определяются самой этой группой.

Теорема 37. *Если абелева группа без кручения* $\mathfrak{G}$ *имеет конечный базис из* n *элементов* $B_1, \ldots, B_n$, *то* n *есть не зависящее от выбора базиса максимальное число независимых элементов в* $\mathfrak{G}$.

Так как $B_1, \ldots, B_n$ во всяком случае независимы, то n независимых элементов в $\mathfrak{G}$ существуют, и мы должны, следовательно, только показать еще, что любые $n+1$ элементов в $\mathfrak{G}$ уже зависимы. В самом деле, между $n+1$ любыми элементами

$$A_i = B_n^{c_{i1}} \ldots B_n^{c_{in}} \quad (i = 1, \ldots, n+1)$$

имеет место соотношение

$$A_1^{x_1} \ldots A_{n+1}^{x_{n+1}} = E,$$

где $n+1$ целых чисел x_i выбраны так, чтобы они удовлетворяли n линейным однородным уравнениям

$$\sum_{i=1}^{n+1} x_i c_{ik} = 0 \quad (k = 1, \ldots, n).$$

Как известно, это всегда возможно, так как коэфициенты c_{ik} — целые числа.

Теорема 38. *Если* $\mathfrak{G}$ — *абелева группа без кручения с конечным базисом, то все ее базисы* $B_1', \ldots, B_n'$ *получаются из одного какого-нибудь базиса* $B_1, \ldots, B_n$ *в виде*

$$B_i' = B_1^{a_{i1}} \ldots B_n^{a_{in}} \quad (i = 1, \ldots, n),$$

где система показателей a_{ik} *состоит из любых целых чисел таких, что определитель*

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

равен ± 1.

Прежде всего построенные указанным способом элементы B_i' всегда образуют базис. Для этого нужно показать только, что элементы B_i можно выразить через B_i'. Но уравнение

$$B_m = B_1'^{x_1} \ldots B_n'^{x_n}$$

удовлетворяется, если мы выберем целые числа x так, чтобы они удовлетворяли n уравнениям

$$x_1 a_{1i} + \ldots + x_n a_{ni} = \begin{cases} 0, & \text{если } i \neq m, \\ 1, & \text{если } i = m. \end{cases}$$

Так как определитель, образованный из (целых) коэфициентов a_{ik}, равен ± 1, а в правых частях также стоят целые числа, то указанные n уравнений действительно разрешимы в целых числах, и притом однозначно.

Пусть теперь n элементов

$$B_i = B_1^{c_{i1}} \dots B_n^{c_{in}} \quad (i = 1, \dots, n)$$

образуют базис. Тогда элементы B должны выражаться через элементы B':

$$B_q = B_1'^{b_{q1}} \dots B_n'^{b_{qn}} \quad (q = 1, \dots, n),$$

и если мы здесь вставим вместо B' их выражения через B, то, в силу того, что элементы B образуют базис, мы получим n^2 равенств

$$\sum_{i=1}^{n} b_{qi} c_{ik} = \begin{cases} 0, & \text{если } q \neq k, \\ 1, & \text{если } q = k. \end{cases}$$

Определитель из этих n^2 чисел равен поэтому единице, но, с другой стороны, он по теореме об умножении определителей равен произведению определителей $|b_{ik}|$ и $|c_{ik}|$. Поэтому каждое из этих целых чисел должно быть делителем единицы, и, следовательно, определитель $|c_{ik}|$ равен ± 1.

Наконец, комбинированием последних трех теорем получается

Теорема 39. *Если* $\mathfrak{G}$ *есть абелева группа без кручения с конечным базисом* $B_1, \dots, B_n$, *а* $\mathfrak{U}$ — *ее подгруппа конечного индекса* j, *то* $\mathfrak{U}$ *также имеет конечный базис* $U_1, \dots, U_n$, *и определитель* $|a_{ik}|$ *n равенств*

$$U_i = B_1^{a_{i1}} \dots B_n^{a_{in}} \quad (i = 1, \dots, n)$$

всегда по абсолютной величине равен j.

Последнее утверждение справедливо для специального базиса, указанного в теореме 35 (см. теорему 36). Согласно теореме 38, переход от этого специального базиса U' к любому базису U осуществляется при помощи матрицы коэфициентов с определителем ± 1. Но при переходе от B к U мы, очевидно, получаем матрицу коэфициентов, определитель которой равен произведению определителей, фигурирующих при переходе от B к U' и от U' к U, а следовательно, равен $\pm j$.

В заключение приведем простой критерий конечности индекса подгруппы абелевой группы с конечным базисом.

Теорема 40. *Если* $\mathfrak{G}$ *есть абелева группа с конечным базисом* $B_1, \dots, B_n$, *то ее подгруппа* $\mathfrak{U}$ *имеет конечный индекс тогда и только тогда, когда некоторая степень каждого элемента из* $\mathfrak{G}$ *принадлежит* $\mathfrak{U}$.

Пусть N_h-я степень ($N_h > 0$) элемента B_h принадлежит $\mathfrak{U}$. Положим

$$N = N_1 \dots N_m,$$

тогда B_h^N также принадлежит $\mathfrak{U}$, а следовательно, N-я степень каждого элемента из $\mathfrak{G}$ также принадлежит $\mathfrak{U}$. Поэтому каждый элемент из $\mathfrak{G}$ отличается от некоторого

$$B_1^{x_1} \dots B_m^{x_m} \quad (0 \leqslant x_i < N)$$

множителем, принадлежащим $\mathfrak{U}$, и, значит, существует не больше чем N^m различных смежных классов группы $\mathfrak{G}$ по подгруппе $\mathfrak{U}$. Следовательно, индекс подгруппы $\mathfrak{U}$ конечен.

Обратно, если подгруппа $\mathfrak{U}$ имеет конечный индекс, то для всякого элемента A из $\mathfrak{G}$ в ряде смежных классов

$$A\mathfrak{U}, A^2\mathfrak{U}, \dots$$

есть только конечное число различных, а потому некоторая степень элемента A должна принадлежать $\mathfrak{U}$.

Нетрудно видеть также, что определение факторгруппы $\mathfrak{G}/\mathfrak{U}$ без изменений переносится с конечных абелевых групп на бесконечные, притом независимо от того, имеет ли группа $\mathfrak{G}$ базис.

ГЛАВА III

АБЕЛЕВЫ ГРУППЫ В ТЕОРИИ ЦЕЛЫХ РАЦИОНАЛЬНЫХ ЧИСЕЛ

§ 12. Группы целых чисел по сложению и по умножению

В элементах теории целых рациональных чисел мы постоянно имеем дело с абелевыми группами. Совокупность целых чисел обладает следующими свойствами:

I) Если a и b—целые числа, то и $a+b$ есть целое число; $a+b=b+a$.
II) $a+(b+c)=(a+b)+c$.
III) Из $a+b=a'+b$ следует $a=a'$.
IV) Для любых двух целых чисел a и b существует такое целое число x, что $a+x=b$.

Таким образом при композиции путем сложения совокупность всех целых (положительных и отрицательных) чисел образует бесконечную абелеву группу $\mathfrak{G}$. Единичным элементом ее служит число 0: $a+0=a$ для всех a. Вся группа получается путем композиции элемента 1 с самим собой. Мы имеем поэтому дело с *группой без кручения*, имеющей один базисный элемент, т. е. с бесконечной *циклической группой*. Целые числа какого-либо модуля, очевидно, также образуют абелеву группу и притом подгруппу группы $\mathfrak{G}$. То, что мы ранее доказали относительно модуля в теореме 2, выражается в терминах теории групп так: *Каждая подгруппа бесконечной циклической группы также является бесконечной циклической группой.*

Модуль целых чисел, делящихся на определенное число k, образует подгруппу $\mathfrak{U}_k$ группы $\mathfrak{G}$. Индекс подгруппы $\mathfrak{U}_k$ есть число различных целых чисел, которые аддитивно отличаются друг от друга на элемент не из $\mathfrak{U}_k$, т. е. не на кратное k; индекс подгруппы $\mathfrak{U}_k$ равен поэтому количеству чисел, несравнимых по модулю k, т. е. равен k (конечно, в предположении, что $k>0$). То, что мы в теории групп называли смежным классом $A\mathfrak{U}_k$, есть в этом случае система чисел, получающихся путем композиции определенного числа a со всеми элементами из $\mathfrak{U}_k$, т. е. прибавлением к a всех кратных k; следовательно, смежные классы в рассматриваемом случае — это просто различные классы по модулю k. Композиция смежных классов, приведшая нас к факторгруппе $\mathfrak{G}/\mathfrak{U}_k$, выступает здесь как композиция классов по модулю k, которую мы будем называть сложением классов.

Таким образом при композиции путем сложения k классов по модулю k образуют абелеву группу, изоморфную факторгруппе $\mathfrak{G}/\mathfrak{U}_k$, где $\mathfrak{G}$ — аддитивная группа всех целых чисел и $\mathfrak{U}_k$ — аддитивная группа всех кратных числа k.

Во всех этих случаях речь идет о циклических, т. е. очень простых группах. Важнее и труднее исследование другого рода композиции чисел — умножения.

Заметим прежде всего, что при композиции путем умножения целые положительные числа не образуют группы, так как хотя групповые аксиомы I—III выполняются, не выполняется аксиома IV: для целых чисел a, b не всегда существует такое целое x, что $ax = b$. Но если мы привлечем все положительные дроби, то увидим, что *при композиции путем умножения положительные рациональные числа образуют абелеву группу* $\mathfrak{M}$ *без кручения.*

Единичным элементом этой группы служит число 1. Теорема об однозначной разложимости целых чисел на простые множители, очевидно, означает, что *в группе* $\mathfrak{M}$ *положительные простые числа образуют бесконечный базис.*

Простейшими подгруппами группы $\mathfrak{M}$ являются, например, совокупности всех рациональных чисел, для представления которых используются только определенные простые числа (в конечном или бесконечном числе).

Присоединением отрицательных рациональных чисел мы получаем расширенную группу, в которой имеется элемент конечного порядка, а именно —1.

Мы будем теперь компонировать классы по модулю n при помощи известного рода умножения. Пусть A и B — два класса по модулю n и $a_1 \equiv a_2 \pmod{n}$, $b_1 \equiv b_2 \pmod{n}$ — соответственно по два представителя из A и B; тогда $a_1 b_1 \equiv a_2 b_2 \pmod{n}$, т. е. класс, которому принадлежит $a_1 b_1$, определяется только классами A и B и не зависит от выбора представителей этих классов. Класс, определенный таким образом классами A и B, мы будем обозначать через $A \cdot B$ или, короче, через AB. Очевидно, что $AB = BA$ и $A(BC) = (AB)C$. Однако классы по модулю n не образуют группы, так как для любых A, B имеем $R_0 A = R_0 B$, где R_0 означает класс нуля, и таким образом аксиома III не выполняется.

Но если A и B — классы, взаимно простые с n, то то же справедливо и относительно AB, причем если b и n взаимно простые, то из $ab \equiv a'b \pmod{n}$ следует $a \equiv a' \pmod{n}$. Этим доказана следующая теорема:

Теорема 41. *При композиции путем умножения система всех n классов по модулю n не образует группы, но при том же способе композиции $\varphi(n)$ классов, взаимно простых с n, образуют абелеву группу. Мы ее будем называть просто „группой классов по модулю n“ и будем обозначать через $\mathfrak{R}(n)$. Единичным элементом служит класс, содержащий число* 1.

Из этого факта мы получаем в качестве непосредственного следствия теоремы 21 (относящейся к группам) малую *теорему Ферма:*

$A^{\varphi(n)} = E$ или

$$a^{\varphi(n)} \equiv 1 \pmod{n}, \quad \text{если} \quad (a, n) = 1.$$

В следующем параграфе мы ставим себе задачей выяснение структуры введенной только что конечной абелевой группы.

§ 13. Структура группы $\mathfrak{R}(n)$ классов по модулю n, взаимно простых с n

Прежде всего мы сведем исследование группы $\mathfrak{R}(n)$ к тому случаю, когда n есть степень простого числа. Это сведение основывается на следующей теореме:

Теорема 42. *Пусть* $(n_1, n_2) = 1$, $n = n_1 n_2$. *Тогда*

$$\mathfrak{R}(n) = \mathfrak{R}(n_1)\,\mathfrak{R}(n_2).$$

В самом деле, отнесем каждому элементу A из $\mathfrak{R}(n)$ пару элементов C_1 из $\mathfrak{R}(n_1)$ и C_2 из $\mathfrak{R}(n_2)$ следующим образом. Если a есть число из класса A, то мы выберем каких-нибудь два числа c_1 и c_2, удовлетворяющих соответственно условиям

$$\left.\begin{aligned} c_1 &\equiv a \pmod{n_1}, \\ c_2 &\equiv a \pmod{n_2}. \end{aligned}\right\} \tag{20}$$

Очевидно, A однозначно определяет класс $C_1 \bmod n_1$, которому принадлежит c_1, и класс $C_2 \bmod n_2$, которому принадлежит c_2. Мы положим

$$A = (C_1, C_2);$$

здесь C_1 принадлежит к $\mathfrak{R}(n_1)$, а C_2 к $\mathfrak{R}(n_2)$.

Если, обратно, c_1 и c_2 — два числа, взаимно простых соответственно с n_1 и n_2, то по теореме 15, в силу условия $(n_1, n_2) = 1$, существует однозначно определенное по модулю $n_1 n_2$ число a, удовлетворяющее сравнениям (20). Далее, очевидно, что из

$$A = (C_1, C_2), \quad A' = (C_1', C_2')$$

следует

$$AA' = (C_1 C_1', C_2 C_2').$$

Таким образом группа $\mathfrak{R}(n)$, действительно, представлена как произведение групп $\mathfrak{R}(n_1)$ и $\mathfrak{R}(n_2)$.

Повторным применением этой теоремы для произведения степеней различных простых чисел $p_1, \ldots, p_k$ получим

$$\mathfrak{R}(p_k^{\alpha_1} \ldots p_k^{\alpha_k}) = \mathfrak{R}(p_1^{\alpha_1}) \ldots \mathfrak{R}(p_k^{\alpha_k}).$$

Исследование группы $\mathfrak{R}(n)$ сведено, таким образом, к случаю, когда n есть степень простого числа.

Теорема 43. *Если p есть простое число, то группа $\mathfrak{R}(p)$ классов по модулю p есть циклическая группа порядка $p-1$.*

Согласно теореме 28, мы должны лишь показать, что если q есть простой делитель $p-1$, то число классов A с $A^q = E$ равно q. (Но теоремам 22 и 27 это число по меньшей мере равно q). Но число классов A с $A^q = E$ совпадает с числом чисел a, несравнимых по модулю p и удовлетворяющих условию $a^q \equiv 1 \pmod p$, т. е. совпадает с числом различных по модулю p корней сравнения $x^q - 1 \equiv 0 \pmod p$. По теореме 12 это число не больше q, так как модуль есть простое число. Следовательно, будучи одновременно не меньше q, оно точно равно q.

Таким образом, если p — простое число, то существует образующий класс по модулю p. Каждое число g из этого класса называется *первообразным корнем числа* p. Согласно этому, g есть первообразный корень числа p, если $g, g^2, \ldots, g^{p-1}$ представляют собой числа, попарно несравнимые по модулю p. Нетрудно видеть, что первообразными корнями числа p служат все степени g^u, где $(u, p-1) = 1$, и только эти степени. Таким образом каждое простое число p имеет $\varphi(p-1)$ первообразных корней.

Теорема 44. *Если p есть нечетное простое число, то группа классов по модулю любой степени p^α циклична.*

Действительно, порядок этой группы есть $h = \varphi(p^\alpha) = p^{\alpha-1}(p-1)$. Мы можем здесь принять $\alpha \geqslant 2$. Простыми делителями числа h являются p и простые делители q числа $p-1$. По теореме 27, p^e, где e — базисное число, принадлежащее числу p в $\mathfrak{R}(p^\alpha)$, есть число несравнимых по модулю p^α решений сравнения

$$a^p \equiv 1 \pmod{p^\alpha}. \tag{21}$$

В силу теоремы Ферма, для каждого такого a имеем $a \equiv 1 \pmod p$. Мы примем, что $a \neq 1$, и положим $a = 1 + up^m$, где p^m есть наивысшая степень p, входящая в $a-1$, так что

$$m \geqslant 1, \quad (u, p) = 1. \tag{22}$$

Из (21) следует

$$a^p = (1 + up^m)^p \equiv 1 \pmod{p^\alpha}. \tag{23}$$

Развернем теперь p-ю степень в левой части этого сравнения по биномиальной теореме и заметим, что для простого числа p все биномиальные коэфициенты

$$\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{1.2\ldots k} \quad (k = 1, \ldots, p-1)$$

делятся на p, так как числитель делится на p, в то время как знаменатель на простое число p не делится. Покажем, что $m \geqslant \alpha - 1$. В самом деле, если бы было $m \leqslant \alpha - 2$, то из (23) следовало бы

$$(1 + up^m)^p \equiv 1 \pmod{p^{m-2}}; \tag{24}$$

но

$$(1 + up^m)^p = 1 + \binom{p}{1} up^m + \ldots + \binom{p}{p-1} u^{p-1} p^{m(p-1)} + u^p p^{mp},$$

и так как $p > 2$, $m \geqslant 1$, то все члены, начиная с третьего, делятся на p^{m+2}, т. е.

$$(1 + up^m)^p \equiv 1 + up^{m+1} \pmod{p^{m+2}}.$$

Из (24) следовало бы, таким образом,

$$up^{m+1} \equiv 0 \pmod{p^{m+2}} \quad \text{или} \quad u \equiv 0 \pmod{p},$$

что противоречит условию (22).

Значит, в (23) $a = 1 + up^m$ с $m \geqslant \alpha - 1$. Но среди таких чисел имеется не больше p несравнимых по модулю p^α.

Таким образом принадлежащее p базисное число e группы $\mathfrak{R}(p^\alpha)$ не превосходит единицы и, значит, равно единице. В том, что базисное число для каждого из простых делителей q числа $p-1$ также равно единице, проще всего убедиться следующим образом.

Согласно теоремам 23 и 24, элементы группы классов по модулю p^α можно однозначно представить в виде AB, где B пробегает те $p-1$ классов, для которых $B^{p-1} = 1$, а A — те $p^{\alpha-1}$ классов, для которых $A^{p^{\alpha-1}} = 1$. Таким образом должно быть еще только доказано, что подгруппа элементов B также циклична. Если, теперь, a — первообразный корень числа p, то, в силу соотношений $a \equiv a^p \equiv a^{p^2} \equiv \ldots \equiv a^{p^{\alpha-1}} = b$, b также есть первообразный корень числа p. Поэтому числа b, $b^2, \ldots, b^{p-1}$ различны по модулю p, а значит, a fortiori различны по модулю p^α. Однако их $(p-1)$-е степени сравнимы с единицей по модулю p^α. Таким образом группа классов B представлена степенями класса, содержащего b, и, значит, циклична. Тем самым доказательство теоремы 44 завершено.

Особое положение простого числа 2 выясняется следующей теоремой:

Теорема 45. *Группы* $\mathfrak{R}(2)$ *и* $\mathfrak{R}(4)$ *цикличны. Если* $\alpha \geqslant 3$, *то группа классов* $\mathfrak{R}(2^\alpha)$, *порядка* $h = \varphi(2^\alpha) = 2^{\alpha-1}$, *имеет точно два базисных класса, один — порядка* 2, *а другой — порядка* $\frac{h}{2} = 2^{\alpha-2}$.

Утверждения относительно модулей 2 и 4 тривиальны. Пусть теперь $\alpha \geqslant 3$. Группа классов по модулю 2^α имеет порядок $h = \varphi(2^\alpha) = 2^{\alpha-1}$. Покажем, что число несравнимых по модулю 2^α решений сравнения $x^2 \equiv 1 \pmod{2^\alpha}$ есть 2^2, т. е. $e = 2$. Действительно, x во всяком случае должно быть нечетным, $x = 1 + 2v$; тогда получаем

$$0 \equiv x^2 - 1 \equiv (1 + 2v)^2 - 1 \equiv 4v(v+1) \pmod{2^\alpha},$$

$$v(v+1) \equiv 0 \pmod{2^{\alpha-2}}.$$

Очевидно, что здесь только один из множителей может быть четным, и он должен делиться тогда на $2^{\alpha-2}$, т. е.

$$v = 2^{\alpha-2} w \quad \text{или} \quad v = -1 + 2^{\alpha-2} w,$$

так что

$$x = 1 + 2^{\alpha-1} w \quad \text{или} \quad x = -1 + 2^{\alpha-1} w$$

с целым w. Каждое такое x действительно есть решение сравнения $x^2 \equiv 1 \pmod{2^\alpha}$. Среди этих чисел имеется точно четыре несравнимых по модулю 2^α, а именно, для $w = 0$ и 1.

Так как теперь в рассматриваемой группе порядка $h = 2^{\alpha-1}$ имеется два базисных класса, то каждый из этих классов может иметь порядок, не больший чем $\frac{h}{2}$. Если существует класс порядка $\frac{h}{2}$, то он обязательно должен быть базисным классом, а другой базисный класс имеет тогда порядок 2 (ибо порядок группы равен произведению порядков базисных элементов). Мы покажем, что класс по модулю 2^α, представленный числом 5, имеет порядок $\frac{h}{2} = 2^{\alpha-2}$. Для этого нужно показать, что

$$5^{2^k} \not\equiv 1 \pmod{2^\alpha} \quad \text{при } \alpha \geqslant 3 \text{ и } k < \alpha - 2,$$

тогда как

$$5^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}.$$

Это, очевидно, равносильно равенству

$$5^{2^{\alpha-2}} = 1 + 2^\alpha u, \text{ где } u \text{ нечетное } (\alpha \geqslant 3).$$

Так как $25 = 1 + 8 \cdot 3$, то это равенство справедливо при $\alpha = 3$. Но если вообще оно справедливо для некоторого α, то возвышением в квадрат получаем

$$5^{2^{\alpha-1}} = (1 + 2^\alpha u)^2 = 1 + 2^{\alpha+1} u + 2^{2\alpha} u^2 = 1 + 2^{\alpha+1} u\,(1 + 2^{\alpha-1} u),$$

следовательно, утверждение справедливо тогда также для $\alpha + 1$. Тем самым теорема 45 полностью доказана.

Заметим еще, что для составных модулей n группа $\mathfrak{R}(n)$, вообще говоря, нециклична. В самом деле, если p есть делитель $\varphi(n)$, то вследствие теоремы 42 принадлежащее в $\mathfrak{R}(n)$ числу p базисное число $e(p)$ равно сумме базисных чисел $e_i(p)$, принадлежащих p в $\mathfrak{R}(p_i^{\alpha_i})$, где $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots$ есть разложение n на простые множители. Но для нечетных простых чисел p_i 2 есть делитель $\varphi(p_i^{\alpha_i})$, а потому, в силу теоремы 44, $e_i(2) = 1$. Поэтому, если в n входят два нечетных простых числа, то $e(2) \geqslant 2$ для $\mathfrak{R}(n)$, и, значит, согласно теореме 28, группа $\mathfrak{R}(n)$ нециклична.

§ 14. Степенные вычеты

С помощью предыдущих теорем нетрудно развить основы теории степенных вычетов, т. е. теории решения двучленных сравнений вида

$$x^q \equiv a \pmod{n}. \tag{25}$$

Если мы ограничимся случаем, когда выполняются следующие условия:

q — простое число,

n — степень нечетного простого числа, $n = p^\alpha$, $(a, n) = 1$,

то решения x, если таковые существуют, также будут взаимно просты с модулем p^α, и вопрос о разрешимости сравнения (25) в целых числах можно в терминах теории групп формулировать так:

Пусть дан класс A, принадлежащий группе классов по модулю p^α. Сколько существует в группе $\mathfrak{R}(p^\alpha)$ таких элементов X, что

$$X^q = A?$$

Мы будем различать два случая:

1. Простое число q *не* делит порядок $h = \varphi(p^\alpha)$ группы $\mathfrak{R}(p^\alpha)$. *Тогда существует точно один элемент требуемого рода.* В самом деле, определим целые числа m и n так, чтобы выполнялось равенство $qm + hn = 1$; это возможно в силу того, что по предположению $(q, h) = 1$. Так как $X^h = E$, то из равенства

$$X^q = A$$

следует, что

$$X = X^{qm+hn} = (X^q)^m = A^m,$$

а этот элемент действительно удовлетворяет уравнению $X^q = A$.

2. q делит $h = \varphi(p^\alpha)$. По теореме 44 существует такой элемент C (порядка h), степени которого дают все элементы группы $\mathfrak{R}(p^\alpha)$. Положим

$$A = C^{a'}, \quad X = C^x;$$

числа a', x вполне определенны по модулю h. Из

$$X^q = A \quad \text{или} \quad C^{xq} = C^{a'}$$

следует по теореме 20, что

$$xq \equiv a' \pmod{h},$$

и обратно. Но так как $q \mid h$, то это сравнение разрешимо в целых числах только тогда, когда $q \mid a'$, и тогда оно имеет точно q решений, различных по модулю h (см. стр. 20). Поэтому в рассматриваемом случае *уравнение* $X^q = A$ *либо не имеет ни одного решения, либо имеет точно* q *различных решений* X. Так как C есть первообразный класс, то условие $q \mid a'$ равнозначно с

$$A^{\frac{h}{q}} = C^{a'\frac{h}{q}} = (C^h)^{\frac{a'}{q}} = E.$$

Если мы теперь перейдем от классов к числам, то доказанные предложения дают следующую теорему:

Теорема 46. *Сравнение*

$$x^q \equiv a \pmod{p^\alpha},$$

где q и p — простые числа, $p \neq 2$, $(a, p) = 1$, имеет точно одно целое решение x, если q не есть делитель $\varphi(p^\alpha)$. Если же $q \mid \varphi(p^\alpha)$, то сравнение имеет решения — и притом точно q решений — только тогда, когда

$$a^{\frac{\varphi(p^\alpha)}{q}} \equiv 1 \pmod{p^\alpha}. \tag{26}$$

Если показатель взаимно прост с модулем, т. е. $q \neq p$, то условие (26) допускает еще более простую формулировку. Именно, из $q \mid \varphi(p^\alpha)$ и $q \neq p$ следует, — так как q — простое число, — что

$$q \mid (p-1) \quad \text{или} \quad q' = \frac{p-1}{q} \text{ — целое.}$$

Тогда условие (26) принимает вид

$$a^{p^{\alpha-1}q'} \equiv 1 \pmod{p^\alpha}, \tag{26a}$$

и, значит, a fortiori

$$a^{p^{\alpha-1}q'} \equiv 1 \pmod{p}.$$

Но, в силу теоремы Ферма (см. теорему 9),

$$a^{p^{\alpha-1}q'} \equiv a^{p^{\alpha-2}q'} \equiv \ldots \equiv a^{q'} \pmod{p}.$$

Следовательно, имеет место сравнение

$$a^{q'} \equiv 1 \pmod{p}. \tag{27}$$

Но из этого сравнения, которое, в силу теоремы 46, имеет своим следствием разрешимость сравнения $x^q \equiv a \pmod{p}$, вытекает также, обратно, (26). В самом деле, для каждого простого числа p из $m \equiv n \pmod{p^r}$ или $m = n + xp^r$ с целым x следует, что

$$m^p = (n + xp^r)^p = n^p + \binom{p}{1} xp^r + \ldots \equiv n^p \pmod{p^{r+1}},$$

$$m^p \equiv n^p \pmod{p^{r+1}},$$

так как, как мы уже выше (см. стр. 53) видели, биномиальные коэффициенты $\binom{p}{k}$ делятся на p при $k = 1, \ldots, p-1$. Поэтому, возводя последовательно $\alpha - 1$ раз обе части сравнения (27) в p-ю степень, мы и получим сравнение (26).

Таким образом, если $q \mid (p-1)$, то условием для разрешимости сравнения $x^q \equiv a \pmod{p^\alpha}$ является также выполнение сравнения (27), где показатель α уже не фигурирует. Тем самым мы доказали следующую теорему:

Теорема 46а. *Если p — нечетное простое число, $(a, p) = 1$ и q — простой множитель числа $p-1$, то сравнение $x^q \equiv a \pmod{p^\alpha}$ разрешимо тогда и только тогда, когда оно разрешимо по модулю p. Для этого необходимо и достаточно, чтобы выполнялось сравнение*

$$a^{\frac{p-1}{q}} \equiv 1 \pmod{p}.$$

Число решений, несравнимых по модулю p^α, равно тогда q.

Как показывает теорема 45, модули вида 2^α требуют отдельного рассмотрения.

Теорема 47. *Сравнение* $x^q \equiv a \pmod{2^\alpha}$ *имеет при нечетных* q *и* a *всегда точно одно решение. Если* $q = 2$ *и* a *нечетно, то сравнение* $x^q = x^2 \equiv a \pmod{2^\alpha}$ *при* $\alpha \geqslant 3$ *разрешимо тогда и только тогда, когда оно разрешимо по модулю* 8, *т. е. когда* $a \equiv 1 \pmod 8$, *причем в этом случае количество несравнимых решений равно* 4. $x^2 \equiv a \pmod 4$ *имеет при* $a \equiv 1 \pmod 4$ *два решения, а при других нечетных* a *— ни одного решения. Наконец,* $x^2 \equiv a \pmod 2$ *имеет всегда одно решение.*

Первая часть (q — нечетное) доказывается точно так же, как в случае сравнения $x^q \equiv a \pmod{p^\alpha}$ (p — нечетное простое число), когда q не делит $h = \varphi(p^\alpha)$ (см. стр. 56). Далее, так как по теореме 45 классы по модулю 2^α при $\alpha \geqslant 3$ могут быть представлены в виде $B_1^{a_1} B_2^{a_2}$, где $B_1^2 = B_2^{2^{\alpha-2}} = E$, то мы видим, что в форме X^2 могут быть представлены только такие классы $A = B_1^{a_1} B_2^{a_2}$, у которых $a_1 = 0$ и a_2 — четное, причем существует тогда столько классов X с $X^2 = B_2^{a_2}$, сколько существует классов с $X^2 = E$ (ибо из $X^2 = E$ имеем $(XB_2^{\frac{a_2}{2}})^2 = B_2^{a_2}$ и из $X^2 = B_2^{a_2}$ имеем $(XB_2^{-\frac{a_2}{2}})^2 = E$), т. е. в силу теоремы 45, $2^2 = 4$.

Простую форму для условия разрешимости сравнения $x^2 \equiv a \pmod{2^\alpha}$ при $\alpha \geqslant 3$ и нечетном a, в виде требования $a \equiv 1 \pmod 8$, мы получаем следующим образом. Прежде всего убеждаемся в том, что если сравнение $x^2 \equiv a \pmod{2^\alpha}$ ($\alpha \geqslant 3$) разрешимо, то разрешимо также сравнение $x^2 \equiv a \pmod{2^{\alpha+1}}$. Для этого достаточно показать, что если $x = x_0$ — какое-нибудь решение первого сравнения, то можно определить целое число z так, чтобы

$$(x_0 + 2^{\alpha-1} z)^2 - a = x_0^2 - a + 2^\alpha x_0 z + 2^{2\alpha-2} z^2 \equiv 0 \pmod{2^{\alpha+1}}.$$

Но так как

$$2\alpha - 2 = \alpha + (\alpha - 2) \geqslant \alpha + 1$$

и x_0 нечетно, то это приводит к действительно разрешимому сравнению

$$\frac{x_0^2 - a}{2^\alpha} + x_0 z \equiv 0 \pmod 2.$$

Из только что доказанного явствует, что если сравнение $x^2 \equiv a \pmod 8$ разрешимо, то разрешимо также сравнение $x^2 \equiv a \pmod{2^\alpha}$. Первое же сравнение, как показывает непосредственное испробование вычетов, разрешимо только при $a \equiv 1 \pmod 8$.

Последние два утверждения теоремы проверяются непосредственным подсчетом.

Теперь мы уже имеем возможность дать обзор решений сравнения

$$x^q \equiv a \pmod{n} \tag{28}$$

при составном n. Пусть $(a, n) = 1$. Для того чтобы сравнение (28) было разрешимо по модулю n, оно должно быть разрешимо по каждому модулю, являющемуся степенью простого числа, входящего в n. Если $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, где p_i — различные простые числа, и если N_i есть число различных по модулю $p_i^{\alpha_i}$ решений сравнения

$$x^q \equiv a \pmod{p_i^{\alpha_i}},$$

то число различных по модулю n решений сравнения (28) есть

$$N = N_1 \dots N_r.$$

В самом деле, если r чисел $z_1, \dots, z_r$ являются соответственно решениями сравнений $z_i^q \equiv a \pmod{p_i^{\alpha_i}}$, то мы определим x из сравнений

$$x \equiv z_i \pmod{p_i^{\alpha_i}} \qquad (i = 1, \dots, r).$$

Тогда

$$x^q \equiv z_i^q \equiv a \pmod{p_i^{\alpha_i}} \quad (i = 1, \dots, r)$$

и, следовательно,

$$x^q \equiv a \pmod{n},$$

и x определяется числами z_i однозначно по модулю n. Далее, две различные системы z_i и z_i' приводят к одному и тому же x по модулю n тогда и только тогда, когда $z_i \equiv z_i' \pmod{p_i^{\alpha_i}}$ для $i = 1, \dots, r$. С другой стороны, каждое решение x сравнения (28) есть система решений r сравнений $x \equiv z_i \pmod{p_i^{\alpha_i}}$ при $z_i = x$. Таким образом $N_1 \dots N_r$ есть точное число решений сравнения (28) по модулю n.

§ 15. Характеры вычетов по модулю n

В заключение остановимся на связи между рассмотрением чисел a по некоторому модулю n и понятием характеров абелевых групп, развитым в § 10.

Элементы группы $\mathfrak{R}(n)$ суть различные классы по модулю n, взаимно простые с n; им, как элементам конечной абелевой группы, соответствует система из $h = \varphi(n)$ характеров. Каждый такой характер χ порождает теоретико-числовую функцию, определенную для каждого целого числа a, взаимно простого с n, равенством

$$\chi(a) = \chi(A),$$

где A — тот класс вычетов по модулю n, к которому принадлежит a.

Эта функция $\chi(a)$ обладает следующими свойствами:

1. $\chi(a) = \chi(b)$, если $a \equiv b \pmod{n}$.
2. $\chi(a)\chi(b) = \chi(ab)$.
3. $\chi(a) \neq 0$ для всех a, взаимно простых с n.

Мы дополним это определение, положив

4. $\chi(a) = 0$, если $(a, n) > 1$.

Тем самым функция $\chi(a)$ определена для всех целых a, причем, очевидно, и для этой расширенной системы аргументов свойства 1—3 остаются в силе.

Каждая функция $\chi(a)$, обладающая свойствами 1—4, называется *характером a по модулю n*. Существует точно $h = \varphi(n)$ различных характеров по модулю n, и по теореме 31 для них имеют место соотношения

$$\sum_{k \bmod n} \chi(k) = \begin{cases} 0, & \text{если } \chi \text{ не есть главный характер,} \\ \varphi(n), & \text{если } \chi \text{ есть главный характер.} \end{cases} \tag{29}$$

При этом главным характером мы, в соответствии с терминологией, установленной в § 10, называем характер, равный единице для всех a, взаимно простых с n; запись „$k \bmod n$“ под знаком суммы означает, что число k, по которому производится суммирование, пробегает полную систему вычетов по модулю n. Аналогично имеют место также соотношения

$$\sum_{l} \chi(k) = \begin{cases} 0, & \text{если } k \not\equiv 1 \pmod{n}, \\ \varphi(n), & \text{если } k \equiv 1 \pmod{n}. \end{cases} \tag{30}$$

С помощью характеров по модулю n мы теперь иначе сформулируем приведенные в предыдущем параграфе условия разрешимости сравнения

$$x^q \equiv a \pmod{n}.$$

При этом мы будем предполагать, что

$$(q, n) = 1, \quad q \text{ — простое число и } \quad (a, n) = 1.$$

Рассматриваемое сравнение означает, что в группе $\mathfrak{R}(n)$ класс A, которому принадлежит a, должен быть q-й степенью. Но q-е степени всех классов образуют подгруппу $\mathfrak{A}_q$ в $\mathfrak{R}(n)$. По теореме 29 порядок факторгруппы $\mathfrak{R}/\mathfrak{A}_q$ есть q^e, где $e = e(q)$ — принадлежащее простому числу q базисное число в $\mathfrak{R}(n)$ и одновременно также число базисных элементов в $\mathfrak{R}/\mathfrak{A}_q$. Таким образом, согласно теореме 33, существуют точно e характеров группы $\mathfrak{R}(n)$, а значит, и характеров по модулю n

$$\chi_1(a), \ldots, \chi_e(a),$$

такого рода, что e равенств $\chi_i(a) = 1$ $(i = 1, \ldots, e)$ представляют собой необходимые и достаточные условия для того, чтобы класс A,

которому принадлежит a, был q-й степенью. Эти e характеров независимы между собой в том смысле, что всегда существуют такие целые числа a, для которых эти e характеров равны произвольно заданным корням q-й степени из единицы.

До сих пор мы использовали только то обстоятельство, что $\mathfrak{R}(n)$ есть конечная абелева группа; глубже структура этой группы выяснится тогда, когда мы захотим представить e как функцию от q и n. Если $n = p^\alpha$, где p — нечетное простое число, то группа $\mathfrak{R}(p^\alpha)$ является циклической (см. теорему 44), и поэтому $e(q) = 0$, если q не есть делитель числа $\varphi(p^\alpha)$, и $e(q) = 1$, если $q \mid \varphi(p^\alpha)$. Если же n составное, $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, и нечетное, то, вследствие теоремы 42, $e(q)$ равно для $\mathfrak{R}(n)$ числу тех p_i, для которых $q \mid \varphi(p_i^{\alpha_i})$.

Каждый характер $\chi(a)$, равный единице для всех a, для которых разрешимо сравнение $x^q \equiv a \pmod n$, называется *q-м степенным характером по модулю n*. По теореме 33 каждый q-й степенной характер может быть представлен в виде произведения степеней базисных характеров $\chi_1, \dots, \chi_e$.

В дальнейшем мы будем заниматься исключительно простейшим случаем $q = 2$, где речь идет о классах, которые могут быть представлены в виде квадратов; соответственные степенные характеры называются тогда *квадратичными характерами*.

§ 16. Квадратичные характеры по модулю n

Целое число a, взаимно простое с n, называется *квадратичным вычетом числа n* или, короче, вычетом числа n, если сравнение

$$x^2 \equiv a \pmod n$$

разрешимо в целых числах x. В противном случае a называется *невычетом числа n*. По сказанному в предыдущем параграфе, условия разрешимости указанного сравнения заключаются в том, чтобы некоторые $e(2)$ характеров по модулю n имели для a значение 1. Каждый из этих характеров $\chi(a)$ есть квадратный корень из 1 и может, следовательно, принимать только значения ± 1.

Если теперь $n = p$, где p — нечетное простое число, то $e(2) = 1$, так как 2 всегда есть делитель $p - 1$ и группа $\mathfrak{R}(p)$ циклична. Таким образом среди $p - 1$ характеров по модулю n имеется только один характер $\chi(a)$, являющийся квадратным корнем из единицы, но не тождественно равный $+1$, и $\chi(a) = 1$ есть условие для того, чтобы a было квадратичным вычетом числа p.

Мы будем пользоваться для этого характера $\chi(a)$ обозначением

$$\chi(a) = \left(\frac{a}{p}\right).$$

По определению, этот характер равен ± 1 для каждого a, не делящегося на p.

Таким образом для целых a, a', b, не делящихся на p, имеем

1. $\left(\frac{a}{p}\right)=\left(\frac{a'}{p}\right)$, если $a\equiv a' \pmod p$,
2. $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,
3. $\left(\frac{a^2}{p}\right)=1$,
4. $\left(\frac{a}{p}\right)$ не для каждого a равно 1.

Этими свойствами символ $\left(\frac{a}{p}\right)$ *вполне определен для каждого* a, *взаимно простого с* p. В самом деле, в силу свойств 1, 2, $\left(\frac{a}{p}\right)$ есть характер по модулю p; в силу свойства 3, этот характер принимает только значения ± 1, наконец, в силу свойства 4, он не всегда равен $+1$; таким образом классы вычетов A, для которых этот характер равен $+1$, образуют подгруппу группы $\mathfrak{R}(p)$, к которой принадлежат все квадраты; ее индекс $\leqslant 2$, но >1, и потому точно $=2$. Следовательно, $\left(\frac{a}{p}\right)$ равно $+1$ только для квадратичных вычетов числа a и равно -1 только для невычетов числа p.

Так как теперь

$$a^{p-1}-1\equiv 0 \pmod p$$

и, значит,

$$(a^{\frac{p-1}{2}}+1)(a^{\frac{p-1}{2}}-1)\equiv 0 \pmod p,$$

то, принимая во внимание теорему 46а, можно определить $\left(\frac{a}{p}\right)$ как то из двух чисел ± 1, для которого выполняется сравнение

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \pmod p. \tag{31}$$

Именно этим способом Лежандр и ввел в арифметику символ $\left(\frac{a}{p}\right)$.

В силу теоремы 29, число квадратичных вычетов числа p, несравнимых по модулю p, равно $\frac{p-1}{2}$. Следовательно, число невычетов числа p равно $p-1-\frac{p-1}{2}=\frac{p-1}{2}$. Таким образом существует столько же квадратичных вычетов числа p, сколько и невычетов.

Согласно теореме 46а, условие $\left(\frac{a}{p}\right)=+1$ одновременно является также и условием для того, чтобы a было квадратичным вычетом числа p^α. Количество вычетов числа p^α, несравнимых по модулю p^α, также равно количеству невычетов, т. е. равно $\frac{1}{2}\varphi(p^\alpha)=$ $=p^{\alpha-1}\frac{p-1}{2}$ $(\alpha>1)$.

Для составного нечетного n, $n=p_1^{\alpha_1}\dots p_r^{\alpha_r}$, условие того, чтобы a было вычетом числа n, дается $e(2)$ равенствами для некото-

рых $e(2)$ характеров по модулю n. При этом $e(2)=r$. В силу теоремы 29, число квадратичных вычетов числа n есть $\frac{\varphi(n)}{2^r}$, следовательно, при $r>1$ оно не равно числу невычетов. Как было показано в конце § 14, условия для того, чтобы a было вычетом числа n, заключаются в том, чтобы a было вычетом каждого простого числа p_i входящего в n, т. е. чтобы имело место r равенств

$$\left(\frac{a}{p_i}\right)=1 \quad (i=1, \ldots, r).$$

Для модуля 2^α, как мы знаем, группа $\mathfrak{R}(2^\alpha)$ при $\alpha\geqslant 3$ уже не циклична, а имеет два базисных класса. Поэтому вопрос о том, есть ли a квадратичный вычет числа 2^α или нет, нельзя теперь решить заданием одного характера по модулю 2^α; нужно задать два характера. Мы пока не будем вводить символа для вычета числа 2^α и вернемся к этому лишь впоследствии, в § 46.

Однако мы расширим определение символа $\left(\frac{a}{n}\right)$ на все составные нечетные n. Пусть

$$n=p_1^{\alpha_1}\ldots p_r^{\alpha_r}, \quad n \text{ нечетное}.$$

Положим

$$\left(\frac{a}{n}\right)=\left(\frac{a}{p_1}\right)^{\alpha_1}\ldots\left(\frac{a}{p_r}\right)^{\alpha_r},$$

если только все символы справа уже имеют смысл, т. е. если $(a, n)=1$. И наконец, пусть будет

$$\left(\frac{a}{n}\right)=0, \text{ если } (a, n)>1.$$

Из этого определения следует, что и для расширенного символа имеют место соотношения

$$\left(\frac{a}{n}\right)=\left(\frac{a'}{n}\right), \text{ если } a\equiv a' \pmod n,$$

$$\left(\frac{ab}{n}\right)=\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

при любых целых a, a', b, независимо от того, взаимно просты они с n или нет. Этот символ есть поэтому характер по модулю n. Напомним, однако, еще раз, что *при составном n из значения $\left(\frac{a}{n}\right)$ ничего нельзя заключить относительно того, есть ли a квадратичный вычет числа n или нет.* Если a есть вычет числа n, то $\left(\frac{a}{n}\right)=+1$, но обратное, вообще говоря, неверно.

Относительно этого символа Лежандр, а до него в применении к отдельным случаям еще Эйлер, сделал замечательное и чрезвычайно

плодотворное для всей арифметики открытие, которое называется теперь *квадратичным законом взаимности* и формулируется так:

Для положительных нечетных a, n

$$\left(\frac{a}{n}\right)=\left(\frac{n}{a}\right)(-1)^{\frac{a-1}{2}\frac{n-1}{2}}$$

Кроме того, имеют место так называемые дополнения к закону взаимности:

$$\left.\begin{aligned}\left(\frac{-1}{n}\right)&=(-1)^{\frac{n-1}{2}},\\ \left(\frac{2}{n}\right)&=(-1)^{\frac{n^2-1}{8}}\end{aligned}\right\}\quad n \text{ нечетное, } >0.$$

После того как Лежандр первый опубликовал попытку доказательства закона взаимности, недостаточную в одном существенном пункте, девятнадцатилетнему Гауссу удалось найти (1796) первое доказательство этого закона, которое он опубликовал в своем классическом труде „Disquisitiones arithmeticae". С того времени было дано очень много различных доказательств закона взаимности; Бахман перечисляет 45 доказательств, одному только Гауссу принадлежит 8.

Открытием закона взаимности можно датировать начало современной теории чисел. По форме этот закон принадлежит еще теории целых рациональных чисел, его можно выразить как простое соотношение исключительно между рациональными числами. Однако по своему содержанию он выходит за пределы области рациональных чисел. Уже Гаусс сознавал это. Он прежде всего пытался перенести арифметические понятия на целые комплексные числа $a+b\sqrt{-1}$, где a и b — целые рациональные числа, и тут ему удалось установить и доказать аналогичный закон для вычетов четвертой степени. (Весьма вероятно, что именно этот успех в комплексной теории чисел побудил его ввести комплексные числа, — которыми пользовались тогда с недоверием и лишь случайно, — и в другие части анализа как принципиально равноправные с вещественными числами.) Гаусс считал, что лежандров закон взаимности представляет собой частный случай более общего и более объемлющего закона. Поэтому как он, так и многие другие математики постоянно искали все новых доказательств, основные идеи которых можно было бы перенести и на другие числовые области, — в надежде таким образом ближе подойти к этому более общему закону. Последний решительный шаг сделал Куммер введением идеальных простых множителей. После этого Дедекинд обосновал общую теорию идеалов в алгебраических числовых полях и, наконец, в настоящее время Гильберт и его ученик Фуртвенглер установили и доказали наиболее общий закон взаимности для вычетов q-й степени, где q есть простое число.

Развитие алгебраической теории чисел действительно показало, что содержание квадратичного закона взаимности становится понятным

лишь тогда, когда переходят к общим алгебраическим числам, и что доказательство, отвечающее существу проблемы, лучше всего вести при помощи высших средств, в то время как относительно элементарных доказательств надо сказать, что они скорее носят характер последующей проверки каким-то образом добытого результата.

Поэтому мы здесь вовсе не будем давать элементарного доказательства. Мы ставим себе задачу перенесения понятий теории целых рациональных чисел, в частности понятия целого числа, на другие числовые области, причем мы одновременно получим новые соотношения между самими целыми рациональными числами, и, в частности, квадратичный закон взаимности получится как простой побочный результат.

ГЛАВА IV

АЛГЕБРА ЧИСЛОВЫХ ПОЛЕЙ

§ 17. Числовое поле. Полиномы в числовых полях. Неприводимость

Определение. Система вещественных или комплексных чисел называется *числовым полем* (короче, *полем*), если она содержит больше одного числа и вместе с числами α, β содержит $\alpha - \beta$ и, в случае $\beta \neq 0$, также $\frac{\alpha}{\beta}$.

Нетрудно видеть, что тогда в этой системе содержатся также числа $\alpha + \beta$ и $\alpha\beta$, т. е., что внутри нее все рациональные операции неограниченно выполнимы. Поэтому вместо названия „поле“ пользуются также, по Кронекеру, названием *„область рациональности“*. Дополнительное условие, чтобы система содержала больше одного числа, исключает систему, состоящую из одного только элемента 0, которая удовлетворяет всем остальным условиям определения.

Понятие поля родственно с понятием группы. Согласно определению, числа поля во всяком случае образуют бесконечную абелеву группу при композиции путем сложения. А числа поля, за исключением числа 0, образуют абелеву группу также и при композиции путем умножения.

Примерами числовых полей являются:

Система всех рациональных чисел.
Система всех вещественных чисел.
Система всех (вещественных и комплексных) чисел.

Система всех чисел вида $R(\omega)$, где $R(x)$ пробегает все рациональные функции от x с рациональными коэфициентами, а ω есть определенное число.

Так как $\frac{\alpha}{\alpha} = 1$, то каждое поле содержит число 1, а потому и $1 + 1 = 2$, $1 - 1 = 0$ и т. д., т. е. все целые числа, а значит, и их частные, т. е. все рациональные числа. Поле рациональных чисел, которое мы будем обозначать через $k(1)$, называют поэтому *абсолютной областью рациональности*. Оно содержится в каждом числовом поле.

В этой главе мы будем заниматься *алгеброй* числовых полей; в остальных главах, после введения понятия о „целых“ числах поля, мы займемся арифметикой числовых полей.

Пусть k — произвольное числовое поле. Под *полиномом* в k мы будем разуметь полином, все коэфициенты которого суть числа из k. Частное двух полиномов из k называется рациональной функцией в k. Если $f(x)$ и $g(x)$ — полиномы, из которых $g(x)$ — по крайней мере первой степени, то, как известно, можно однозначным образом определить два полинома $q(x)$ и $r(x)$ так, чтобы

$$f(x) = q(x)g(x) + r(x), \tag{32}$$

причем степень $r(x)$ меньше, чем степень $g(x)$. $r(x)$ называют *вычетом* $f(x) \bmod g(x)$. Коэфициенты полиномов $q(x)$, $r(x)$ вычисляются по коэфициентам полиномов $f(x)$ и $g(x)$ исключительно с помощью рациональных операций и поэтому также принадлежат k, если только $f(x)$ и $g(x)$ — полиномы в k. Если $r(x)$ равно нулю, то говорят, что $f(x)$ делится на $g(x)$, $g(x)$ входит в $f(x)$, и записывают это так:

$$g(x) \mid f(x).$$

Если в (32) степень m полинома $f(x)$ меньше, чем степень n полинома $g(x)$, то $q = 0$ и $r(x) = f(x)$. Если же $m \geqslant n$, то степень $q(x)$ равна $m - n$, $q(x)$ не есть нуль и степень $r(x)$ меньше n. Поэтому, если каждый из двух полиномов $f(x)$ и $g(x)$ делится на другой, то они отличаются только постоянным множителем. Тривиальными делителями каждого полинома $f(x)$ являются постоянные c, т. е. полиномы нулевой степени, и полиномы $cf(x)$. Полином первой степени $a(x - \alpha)$ не имеет никаких делителей, кроме этих тривиальных. По основной теореме алгебры, каждый полином $f(x)$ степени n можно одним и только одним способом разложить на множители первой степени $x - \alpha$ так, что

$$f(x) = c(x - \alpha_1) \ldots (x - \alpha_n),$$

где c есть отличная от нуля постоянная, а $\alpha_1, \ldots, \alpha_n$ суть n (одинаковых или различных) вещественных или комплексных чисел. Таким образом, если допустить для полиномов произвольные коэфициенты, то в вопросах делимости полиномы нулевой степени будут играть ту же роль, что в теории чисел единицы ± 1, а полиномы первой степени — роль простых чисел.

Существенно иначе обстоит дело, если мы ограничиваем себя рассмотрением полиномов в определенном поле k. Полином $f(x)$ в k мы называем *неприводимым в k* или *неразложимым в k*, если $f(x)$ нельзя представить в виде произведения двух полиномов в k, каждый из которых отличен от постоянной.

Согласно этому, например, каждый полином первой степени в k неприводим в k. Но так как основная теорема алгебры ничего не говорит о том, принадлежат ли корни α полинома $f(x)$ также к k, то и полиномы более высоких степеней могут быть неприводимы в k. Например полином $x^2 + 1$, очевидно, неприводим в поле вещественных чисел. Однако мы сейчас оставим в стороне вопрос о более точном исследовании свойств неприводимых в k полиномов и ограничимся только указанием на их существование.

Важнейший факт, относящийся к полиномам в k, выражается следующей теоремой:

Теорема 48. *Любые два отличных от нуля полинома $f_1(x)$ и $f_2(x)$ в k имеют однозначно определенный наибольший общий делитель $d(x)$, т. е. существует такой полином $d(x)$ со старшим коэфициентом 1, что*

$$d(x) \mid f_1(x), \quad d(x) \mid f_2(x)$$

и каждый полином, входящий как в $f_1(x)$, так и в $f_2(x)$, входит также в $d(x)$.

Кроме того, $d(x)$ можно представить в виде

$$d(x) = g_1(x) f_1(x) + g_2(x) f_2(x), \tag{33}$$

где $g_1(x)$ и $g_2(x)$ — полиномы в k, и поэтому $d(x)$ также есть полином в k.

Доказательство этой теоремы известно из элементов алгебры, однако там не придается значения природе фигурирующих коэфициентов. Поэтому мы здесь, опираясь на доказательство аналогичных предложений в теории целых рациональных чисел (теоремы 1 и 2), воспроизведем вкратце это доказательство. Среди полиномов

$$L(x) = u_1(x) f_1(x) + u_2(x) f_2(x),$$

где $u_1(x)$ и $u_2(x)$ пробегают все полиномы в k, рассмотрим полином (33) наименьшей степени, имеющий старшим коэфициентом единицу. Если $d(x)$ имеет степень 0, то он равен единице и входит поэтому в $f_1(x)$ и $f_2(x)$. Но и в том случае, когда он более высокой степени, он тоже должен входить в $f_1(x)$ и в $f_2(x)$. В самом деле, определим вычет $r(x)$ полинома $f_1(x)$ mod $d(x)$:

$$f_1(x) = q(x) d(x) + r(x),$$

$$r(x) = f_1(x) - q(x) d(x),$$

$$r = f_1 - qd = f_1 - q(g_1 f_1 + g_2 f_2) = (1 - qg_1) f_1 - qg_2 f_2.$$

Таким образом $r(x)$ также содержится среди полиномов $L(x)$, и в то же время его степень (как степень вычета полинома $d(x)$) меньше степени $d(x)$. Поэтому он не может содержать отличных от нуля коэфициентов и равен поэтому нулю, следовательно, $d(x) \mid f_1(x)$. Таким же образом мы покажем, что $d(x) \mid f_2(x)$. Но из (33) следует, что каждый общий делитель полиномов $f_1(x)$ и $f_2(x)$ входит также в $d(x)$. Если поэтому полином $d_0(x)$ обладает теми же свойствами, что и $d(x)$, то $d(x) \mid d_0(x)$ и $d_0(x) \mid d(x)$, а потому $d_0(x)$ и $d(x)$ отличаются только постоянным множителем, но так как их старшие коэфициенты равны единице, то $d_0(x) = d(x)$.

Мы пишем $d(x) = (f_1(x), f_2(x))$ и называем $f_1(x)$ и $f_2(x)$ *взаимно простыми*, если $d = 1$. Наибольший общий делитель двух полиномов определяется этими полиномами вполне, а не только по отношению

к определенному полю k, в то время как свойство неразложимости полинома принадлежит ему, вообще говоря, только относительно некоторого поля k.

Из теоремы 48 непосредственно вытекает

Теорема 49. *Если неприводимый в k полином $f(x)$ имеет с каким-либо полиномом $g(x)$ из k общий корень $x=\alpha$, то $f(x)$ есть делитель $g(x)$, и поэтому все корни $f(x)$ являются также корнями $g(x)$.*

В самом деле, $(f(x), g(x))$ делится по крайней мере на $x-\alpha$ и, значит, не равен единице. С другой стороны, $f(x)$ не имеет в k никаких других делителей, кроме констант c и полиномов $cf(x)$. Поэтому $(f(x), g(x)) = cf(x)$, $f(x) \mid g(x)$.

В частности, неприводимый в k полином $f(x)$ степени n имеет точно n различных корней, так как в противном случае он имел бы общий корень с производной $f'(x)$, которая также есть полином в k, но имеет степень $n-1$; поэтому $f(x)$ должен был бы входить в $f'(x)$, что невозможно.

§ 18. Алгебраические числа относительно поля k

Пусть число ϑ есть корень полинома $P(x)$ в k. Среди всех полиномов в k со старшим коэфициентом 1, имеющих ϑ своим корнем, существует полином, имеющий наименьшую степень. Этот полином непременно должен быть неприводим в k — иначе ϑ было бы корнем делителя этого полинома — и, значит, по теореме 49 вполне определяется корнем ϑ и полем k.

Степень n этого полинома называется *степенью числа ϑ относительно поля k* или *относительной степенью числа ϑ*. n, как мы видели, различных корней $\vartheta_1, \vartheta_2, \ldots, \vartheta_n$ этого полинома называются *сопряженными с ϑ* относительно k или *относительно сопряженными с ϑ*. Каждое из чисел ϑ называется *алгебраическим числом относительно поля k*. Если $k=k(1)$ есть абсолютная область рациональности, то указание на k вовсе опускается; в частности, число ϑ, являющееся корнем полинома с рациональными коэфициентами, называется просто *алгебраическим числом*. Очевидно, что сами числа из k имеют относительную степень 1.

Для дальнейших исследований нам нужна из алгебры *теорема о симметрических функциях*, которую мы формулируем следующим образом:

Пусть $\alpha_1, \ldots, \alpha_n$ будут n независимых переменных и $f_1, \ldots, f_n$ — их n элементарных симметрических функций, являющихся, как известно, коэфициентами полинома $(x-\alpha_1)\ldots(x-\alpha_n)$. Тогда каждая целая рациональная симметрическая функция $S(\alpha_1, \ldots, \alpha_n)$ может быть представлена как целая рациональная функция от $f_1, \ldots, f_n$:

$$S(\alpha_1, \ldots, \alpha_n) = G(f_1, \ldots, f_n).$$

Коэфициенты в G могут быть вычислены по коэфициентам функции S с помощью операций сложения, вычитания и умножения.

Применяя эту теорему повторно, получим следующий результат. Пусть $\beta_1, \ldots, \beta_m$ будут m других независимых переменных и $\varphi_1, \ldots, \varphi_m$ — их элементарные симметрические функции; если $S(\alpha_1, \ldots, \alpha_n; \beta_1, \ldots, \beta_m)$ есть целая рациональная функция этих $n+m$ аргументов, остающаяся неизменной при перестановке α между собой и β между собой, то S можно представить в виде целой рациональной функции от $f_1, \ldots, f_n$ и $\varphi_1, \ldots, \varphi_m$:

$$S(\alpha_1, \ldots, \alpha_n; \beta_1, \ldots, \beta_m) = G(f_1, \ldots, f_n; \varphi_1, \ldots, \varphi_m).$$

При этом коэфициенты в G могут быть вычислены по коэфициентам в S с помощью сложения, вычитания и умножения.

Отсюда мы прежде всего выводим следующую теорему:

Теорема 50. *Если α и β — алгебраические числа относительно k, то то же справедливо и для $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, а также, если $\beta \neq 0$, — и для $\frac{\alpha}{\beta}$.*

В самом деле, пусть $\alpha_1, \ldots, \alpha_n$ — числа, сопряженные с α, и $\beta_1, \ldots, \beta_m$ — сопряженные с β относительно k; тогда элементарные симметрические функции как чисел α, так и чисел β будут числами из k. По формулированной выше основной теореме, произведение

$$H(x) = \prod_{k=1}^{m} \prod_{i=1}^{n} (x - (\alpha_i + \beta_k)),$$

как симметрическая функция относительно α и β, есть тогда полином в k, и среди его корней находится также $\alpha+\beta$, которое, следовательно, есть алгебраическое число относительно k. Таким же образом проводится доказательство для $\alpha-\beta$ и $\alpha\beta$.

Для случая $\frac{\alpha}{\beta}$ такой способ рассуждения уже не годится, так как аналогичное произведение здесь не есть целая функция относительно β, а потому основная теорема неприменима. Но если $\beta \neq 0$, то мы положим в неприводимом уравнении

$$x^m + c_{m-1}x^{m-1} + \ldots + c_1 x + c_0 = 0,$$

которому β удовлетворяет в k, $x = \frac{1}{y}$, и умножим обе его части на y^n. Полученный таким образом полином относительно y имеет тогда корень $\frac{1}{\beta}$, а потому $\frac{1}{\beta}$ также есть алгебраическое число относительно k, следовательно, согласно предыдущему, алгебраическим числом является также и произведение $\alpha\frac{1}{\beta} = \frac{\alpha}{\beta}$.

Теорема 51. *Если ω есть корень полинома*

$$\varphi(x) = x^m + \alpha x^{m-1} + \beta x^{m-2} + \ldots + \varkappa x + \lambda,$$

коэфициенты которого суть алгебраические числа относительно k, то ω также есть алгебраическое число относительно k.

Пусть α_i пробегает числа, сопряженные с α, β_k — числа, сопряженные с β, и т. д.; тогда полином

$$F(x) = \prod_{i,\,k,\ldots,s} (x^m + \alpha_i x^{m-1} + \beta_k x^{m-2} + \ldots + \lambda_s),$$

как симметрическая функция относительно сопряженных элементов, имеет, по основной теореме о симметрических функциях, коэфициентами числа из k; так как $F(\omega) = 0$, то ω есть, следовательно, алгебраическое число относительно k.

§ 19. Алгебраические числовые поля над k

Каждое алгебраическое относительно k число ϑ порождает поле, а именно, поле всех рациональных функций от ϑ с коэфициентами из k. Это поле обозначается через $K(\vartheta; k)$ или, проще, через $K(\vartheta)$; говорят, что оно получается *присоединением* ϑ к k или что $k(\vartheta)$ является расширением k с помощью ϑ. Таким же образом присоединением к k нескольких чисел $\alpha, \beta, \ldots, \lambda$, алгебраических относительно k, получается поле $K(\alpha, \beta, \ldots, \lambda; k)$, элементы которого суть рациональные функции от $\alpha, \beta, \ldots, \lambda$ с коэфициентами из k.

Теорема 52. *Каждое поле, получаемое присоединением нескольких алгебраических относительно k чисел, может быть также получено присоединением одного алгебраического относительно k числа.*

Очевидно, достаточно эту теорему доказать для случая присоединения двух чисел. Пусть $\alpha_1, \ldots, \alpha_n$ будут n чисел, сопряженных с числом α_1 относительной степени n, и $\beta_1, \ldots, \beta_m$ будут m чисел, сопряженных с числом β_1 относительной степени m. Мы покажем, что при соответственном выборе чисел u и v из k число $u\alpha_1 + v\beta_1 = \omega_{11}$ порождает поле $K(\alpha_1, \beta_1; k)$. Для этого надо показать, что сами числа α_1 и β_1, — а потому и каждое число из $K(\alpha_1, \beta_1; k)$, — можно представить в виде рациональной функции от ω_{11} с коэфициентами из k.

С этой целью мы выберем в качестве u, v рациональные числа такого рода, чтобы nm чисел

$$\omega_{ik} = u\alpha_i + v\beta_k \quad (i = 1, \ldots, n;\ k = 1, \ldots, m)$$

были все между собой различны. Это возможно, так как требуется только, чтобы для всех пар индексов i, k и i', k' было

$$u(\alpha_i - \alpha_{i'}) + v(\beta_k - \beta_{k'}) \neq 0$$

за исключением того случая, когда одновременно $i = i'$ и $k = k'$. Но в этих линейных функциях от u, v оба коэфициента никогда не равны нулю одновременно, так как все α_i между собой и все β_k между собой различны. Надо поэтому выбрать $\frac{u}{v}$ отличным от конечного числа чисел

$$-\frac{\beta_k - \beta_{k'}}{\alpha_i - \alpha_{i'}}, \quad i \neq i', \quad k \neq k',$$

и $u \neq 0$, $v \neq 0$; тогда все ω_{ik} будут различны и будут корнями полинома в k

$$H(x) = \prod_{i,k} (x - (u\alpha_i + v\beta_k)) = \sum_{h=0}^{nm} c_h x^h.$$

Мы постараемся теперь составить такую рациональную функцию от x, которая при $x = \omega_{1k}$ $(k = 1, \ldots, m)$ принимала бы значения β_k. Рассмотрим для этого, по примеру интерполяционной формулы Лагранжа, выражение

$$\sum_{i=1}^{n} \sum_{k=1}^{m} \beta_k \frac{H(x)}{x - \omega_{ik}} = \Phi(x).$$

Это выражение есть полином в k. В самом деле, так как $H(\omega_{ik}) = 0$, то

$$\frac{H(x)}{x - \omega_{ik}} = \frac{H(x) - H(\omega_{ik})}{x - \omega_{ik}} = \sum_{h=0}^{nm} c_h \frac{x^h - \omega_{ik}^h}{x - \omega_{ik}} = G(x, \omega_{ik})$$

есть, очевидно, целое рациональное выражение относительно x и ω_{ik} с коэфициентами из k, а потому

$$\Phi(x) = \sum_{i=1}^{n} \sum_{k=1}^{m} \beta_k G(x, u\alpha_i + v\beta_k)$$

есть полином относительно x, коэфициенты которого суть целые рациональные выражения относительно α_i и β_k с коэфициентами из k, притом формально симметричные как относительно величин $\alpha_1, \ldots, \alpha_n$, так и относительно величин $\beta_1, \ldots, \beta_m$. Поэтому коэфициенты полинома $\Phi(x)$ суть числа из k и $\Phi(x)$ есть полином в k. Если мы положим теперь $x = \omega_{11}$, то все $G(\omega_{11}, \omega_{ik})$ обратятся в нуль, за исключением лишь $G(\omega_{11}, \omega_{11})$, и мы получим

$$\beta_1 = \frac{\Phi(\omega_{11})}{G(\omega_{11}, \omega_{11})}.$$

Аналогично доказывается, что и α_1 можно выразить в виде рационального выражения от ω_{11} с коэфициентами из k. А этим и доказано, что

$$K(\alpha_1, \beta_1; k) = K(\omega_{11}, k).$$

Таким образом достаточно ограничиться рассмотрением полей, получающихся присоединением к k одного только алгебраического числа.

Пусть теперь ϑ — алгебраическое число степени n относительно поля k. Для чисел из $K(\vartheta; k)$ имеет место следующая теорема:

Теорема 53. *Каждое число из* $K(\vartheta)$ *единственным образом представляется в форме*

$$\alpha = c_0 + c_1\vartheta + \ldots + c_{n-1}\vartheta^{n-1}, \tag{34}$$

когда $c_0, \ldots, c_{n-1}$ *пробегают все числа основного поля* k.

В самом деле, пусть $\alpha = \frac{P(\vartheta)}{Q(\vartheta)}$, где P и Q — полиномы в k и $Q(\vartheta) \neq 0$; $Q(x)$ и соответствующий ϑ в k неприводимый полином $f(x)$ не имеют ϑ общим корнем, а потому, в силу теоремы 49, $Q(x)$ и $f(x)$ взаимно просты; поэтому в k существуют два таких полинома $R(x)$ и $H(x)$, что

$$1 = Q(x)R(x) + f(x)H(x),$$

и при $x = \vartheta$, в силу $f(\vartheta) = 0$, получаем

$$1 = Q(\vartheta)R(\vartheta).$$

Таким образом

$$\alpha = \frac{P(\vartheta)}{Q(\vartheta)} = P(\vartheta)R(\vartheta) = F(\vartheta),$$

где $F(x) = P(x)R(x)$ — полином в k. Пусть теперь $g(x)$ — вычет $F(x) \bmod f(x)$, также являющийся полиномом в k, но уже степени $\leqslant n-1$. Имеем

$$F(x) = q(x)f(x) + g(x)$$

и

$$\alpha = F(\vartheta) = g(\vartheta).$$

Таким образом α действительно приведено к виду (34). Если бы теперь существовало два полинома $g(x)$ и $g_1(x)$ в k степени не выше $n-1$, таких, что $g(\vartheta) = g_1(\vartheta)$, то разность $g(x) - g_1(x)$ была бы полиномом в k степени, меньшей чем n, имеющим корень ϑ, и, следовательно, была бы тождественно равна нулю. Таким образом представление (34) каждого числа α из $K(\vartheta)$ единственно.

Теорема 54. *Каждое число $g(\vartheta)$ из поля $K(\vartheta)$, порождаемого алгебраическим относительно k числом ϑ степени n, есть алгебраическое относительно k число степени не выше n. Относительно сопряженными с числом $\alpha = g(\vartheta)$ являются различные среди чисел $g(\vartheta_i)$, $i = 1, \ldots, n$. При этом каждое из сопряженных с α встречается одинаково часто.*

В самом деле, пусть $\vartheta_1, \ldots, \vartheta_n$ — числа, сопряженные с ϑ относительно k. Образуем произведение

$$F(x) = \prod_{i=1}^{n} (x - g(\vartheta_i)).$$

Коэфициенты этого полинома представляют собой целые рациональные выражения относительно $\vartheta_1, \ldots, \vartheta_n$, причем они симметричны относительно $\vartheta_1, \ldots, \vartheta_n$ и коэфициенты их принадлежат k; поэтому $F(x)$ есть полином в k и, значит, каждое число $g(\vartheta_i)$ есть алгебраическое число относительно k. Если, далее, $\varphi(x)$ есть полином из k, среди корней которого имеется хотя бы одно из чисел $\alpha_i = g(\vartheta_i)$, то все α_i являются его корнями. В самом деле, пусть $f(y)$ — соответствующий ϑ неприводимый в k полином; полином в k $\varphi(g(y))$ имеет с $f(y)$ общий корень $y = \vartheta_i$ и должен, значит, по теореме 49, обращаться в нуль

для всех $\eta = \vartheta_1, \ldots, \vartheta_n$; следовательно, $\varphi(x)$ равно нулю при $x = \alpha_1, \ldots, \alpha_n$. Пусть теперь $\psi(x)$ — неприводимый в k полином со старшим коэфициентом 1, имеющий корнем α_1; $\psi(x)$ есть делитель $F(x)$; пусть $(\psi(x))^q$ — наивысшая степень полинома ψ, входящая в $F(x)$. Если бы полином $\frac{F(x)}{(\psi(x))^q}$ не был константой, то он имел бы своим корнем какой-либо из корней α_i полинома F и, значит, по доказанному выше, делился бы на $\psi(x)$, что противоречит предположению относительно q. Таким образом для некоторого целого q

$$F(x) = (\psi(x))^q.$$

Но это означает, что n чисел $\alpha_i = g(\vartheta_i)$ $(i = 1, \ldots, n)$ представляют все сопряженные с каждым α_i, и притом каждое q раз. Отсюда следует также, что n есть наивысшая относительная степень, какую может иметь относительно k какое бы то ни было число из $K(\vartheta)$, и, следовательно, n есть число, определяемое самим полем $K(\vartheta)$ и не зависящее от выбора производящего числа ϑ. n называется поэтому *относительной степенью поля* $K(\vartheta)$ (относительно k). Степень каждого числа из $K(\vartheta)$ есть, таким образом, делитель степени поля.

Принимая во внимание предыдущую теорему, мы модифицируем теперь понятие сопряженных чисел при помощи следующего определения:

Определение. Пусть n — степень поля $K(\vartheta)$ относительно поля k и $\alpha = g(\vartheta)$ — число из $K(\vartheta)$, степени $\frac{n}{q}$; n чисел $\alpha_i = g(\vartheta_i)$ $(i = 1, \ldots, n)$ (где ϑ_i — сопряженные с ϑ) мы будем называть *сопряженными с* α *в поле* $K(\vartheta)$ *относительно поля* k. Это суть числа, сопряженные с α относительно поля k, каждое повторенное q раз.

Система этих сопряженных, как целое, зависит поэтому только от α, основного поля k и поля K, но не зависит от выбора производящего числа ϑ. Так как в дальнейшем мы будем иметь дело почти исключительно с этим понятием сопряженных чисел, то для простоты мы добавочное указание „в поле $K(\vartheta)$ относительно поля k“ будем опускать.

Если мы сопряженные с производящим числом ϑ поля K перенумеруем в определенном порядке: $\vartheta_1, \ldots, \vartheta_n$, то этим самым будет определена также нумерация для n сопряженных с любым числом α из $K(\vartheta)$; именно, представляя α по теореме 53 в однозначно определенной форме $g(\vartheta)$, мы через α_i обозначим сопряженное с α число $g(\vartheta_i)$. Мы будем предполагать, что такая нумерация введена, и докажем следующую теорему:

Теорема 55. *Каждое рациональное соотношение* $R(\alpha, \beta, \gamma, \ldots) = 0$ *между числами* α, β, γ, ... *из* $K(\vartheta)$ *с коэфициентами из* k *остается справедливым, если числа* α, β, γ, ... *заменить сопряженными с одинаковым индексом.*

В самом деле, в качестве рациональной функции от $\alpha, \beta, \gamma, \ldots$ R тождественно относительно $\alpha, \beta, \gamma, \ldots$ равно частному двух целых рациональных выражений P и Q,

$$R(\alpha, \beta, \gamma, \ldots) = \frac{P(\alpha, \beta, \gamma, \ldots)}{Q(\alpha, \beta, \gamma, \ldots)}.$$

Если мы здесь вместо $\alpha, \beta, \gamma, \ldots$ подставим их представления через полиномы от ϑ,

$$\alpha = g(\vartheta), \quad \beta = h(\vartheta), \quad \gamma = r(\vartheta), \ldots,$$

то Q представится в виде полинома от ϑ, отличного от нуля для рассматриваемого значения ϑ, так как он равен для этого значения числу $Q(\alpha, \beta, \gamma, \ldots)$. Следовательно, этот полином будет отличен от нуля также для каждого из сопряженных с ϑ чисел $\vartheta_1, \ldots, \vartheta_n$. В силу условия $R = 0$, числитель

$$P(g(\vartheta), h(\vartheta), r(\vartheta), \ldots) = 0.$$

Следовательно, этот полином от ϑ должен обращаться в нуль для всех сопряженных с ϑ чисел ϑ_i. Таким образом

$$\left.\begin{aligned} P(\alpha_i, \beta_i, \gamma_i, \ldots) &= 0, \\ Q(\alpha_i, \beta_i, \gamma_i, \ldots) &\neq 0 \end{aligned}\right\} \quad (i = 1, \ldots, n),$$

и поэтому

$$R(\alpha_i, \beta_i, \gamma_i, \ldots) = 0 \qquad (i = 1, \ldots, n).$$

В частности, для любых двух чисел α, β из $K(\vartheta)$ имеем

$$\alpha_i \pm \beta_i = (\alpha \pm \beta)_i, \quad \alpha_i \beta_i = (\alpha\beta)_i, \quad \frac{\alpha_i}{\beta_i} = \left(\frac{\alpha}{\beta}\right)_i.$$

Например, для $\alpha = g(\vartheta)$; $\beta = h(\vartheta)$ имеем

$$g(\vartheta)\, h(\vartheta) = r(\vartheta),$$

где g, h, r — полиномы степени $\leqslant n-1$, и из этого одного равенства для значения ϑ по предыдущей теореме следует n равенств

$$g(\vartheta_i)\, h(\vartheta_i) = r(\vartheta_i),$$

т. е.

$$\alpha_i \beta_i = (\alpha\beta)_i \quad (i = 1, \ldots, n).$$

§ 20. Производящие числа поля. Фундаментальные системы. Под-поля поля $K(\vartheta)$

Теорема 56. *Число α из поля $K(\vartheta)$ тогда и только тогда принадлежит основному полю k, когда оно совпадает со своими n сопряженными. Число α из $K(\vartheta)$ тогда и только тогда имеет степень n относительно k, если оно отлично от всех своих сопряженных. Последнее одновременно есть условие, необходимое и достаточное для того, чтобы число α порождало поле $K(\vartheta)$.*

Оба первых утверждения вытекают из теоремы 54 и следующего за ней определения. Если теперь α из $K(\vartheta)$ порождает поле $K(\vartheta)$,

т. е. $K(\vartheta) = K(\alpha)$, то степень α должна быть равна степени поля $K(\vartheta)$, т. е. n; следовательно, все сопряженные с α должны быть различны. Покажем, что, обратно, если числа $\alpha_i = g(\vartheta_i)$ для $i = 1, \ldots, n$ все различны между собой, то ϑ можно рационально выразить через α, и потому все числа из $K(\vartheta)$ содержатся в $K(\alpha)$.

Чтобы выразить ϑ через α, мы прежде всего убеждаемся, как при доказательстве теоремы 52, в том, что

$$H(x) = \prod_{i=1}^{n} (x - \alpha_i) = \prod_{i=1}^{n} (x - g(\vartheta_i))$$

есть полином в k. Точно так же

$$\frac{H(x)}{x - \alpha_i} = G(x, \alpha_i)$$

есть полином от двух величин x и α_i с коэфициентами из k, а потому

$$\Phi(x) = \sum_{i=1}^{n} \vartheta_i \frac{H(x)}{x - \alpha_i} = \sum_{i=1}^{n} \vartheta_i G(x, g(\vartheta_i)),$$

как симметрическое относительно $\vartheta_1, \ldots, \vartheta_n$ выражение, также есть полином в k. Но отсюда при $x = \alpha_i$ следует

$$\vartheta_i = \frac{\Phi(\alpha_i)}{G(\alpha_i, \alpha_i)},$$

так как знаменатель, в силу предположения о различии всех чисел α_i, отличен от нуля.

Тем самым доказательство теоремы 56 завершено.

До сих пор мы каждое число из $K(\vartheta)$ представляли в виде линейной комбинации чисел $1, \vartheta, \vartheta^2, \ldots, \vartheta^{n-1}$ с коэфициентами из k. Однако для многих целей желательна бóльшая свобода в выборе этих основных элементов.

Мы называем n чисел $\omega^{(1)}, \ldots, \omega^{(n)}$ *фундаментальной системой* поля $K(\vartheta)$, если каждое число α из $K(\vartheta)$ можно представить в виде

$$\alpha = \sum_{i=1}^{n} x_i \omega^{(i)}$$

с коэфициентами x_i из k.

Теорема 57. *Для того чтобы n чисел*

$$\omega^{(i)} = \sum_{k=1}^{n} c_{ik} \vartheta^{k-1} \qquad (c_{ik} \text{ — числа из } k) \tag{35}$$

образовывали фундаментальную систему поля $K(\vartheta)$, необходимо и достаточно, чтобы определитель $|c_{ik}|$ был отличен от нуля.

Очевидно, надо только исследовать, при каких условиях числа $1, \vartheta, \vartheta^2, \ldots, \vartheta^{n-1}$ можно выразить через числа $\omega^{(1)}, \ldots, \omega^{(n)}$ в виде

$$\vartheta^{p-1} = \sum_{i=1}^{n} a_{pi}\omega^{(i)} \quad (p = 1, \ldots, n) \quad (a_{pi} \text{ — числа из } k). \tag{36}$$

Предположим, что в (35) определитель отличен от нуля. Тогда мы можем разрешить n уравнений (35) относительно неизвестных $1, \vartheta, \ldots, \vartheta^{n-1}$ и получим эти числа в виде линейных комбинаций чисел $\omega^{(i)}$ с коэфициентами, которые получаются из чисел c_{ik} путем рациональных операций и, следовательно, принадлежат к k.

С другой стороны, если возможно представление чисел ϑ^{k-1} через числа $\omega^{(i)}$ в виде (36), то, подставляя в (36) вместо $\omega^{(i)}$ их выражения (35), мы получим

$$\vartheta^{p-1} = \sum_{i,\,k=1}^{n} a_{pi}c_{ik}\vartheta^{k-1} \quad (p = 1, \ldots, n).$$

Но так как между числами $1, \vartheta, \ldots, \vartheta^{n-1}$ невозможно никакое линейное однородное соотношение с коэфициентами из k, за исключением случая, когда все коэфициенты равны нулю, то

$$\sum_{i=1}^{n} a_{ki}c_{ip} = \delta_{kp} = \begin{cases} 0, & \text{если } p \neq k, \\ 1, & \text{если } p = k. \end{cases}$$

Поэтому определитель $|\delta_{kp}|$, равный единице, с другой стороны равен произведению определителей $|a_{ki}|\,|c_{ip}|$; следовательно, определитель $|c_{ip}|$ отличен от нуля.

Теорема 58. *n чисел $\omega^{(1)}, \ldots, \omega^{(n)}$ из $K(\vartheta)$ образуют фундаментальную систему тогда и только тогда, когда линейное соотношение*

$$\sum_{i=1}^{n} u_i\omega^{(i)} = 0 \tag{37}$$

с коэфициентами u_i из k имеет место лишь в случае, если все u_i равны нулю.

n чисел $\omega^{(i)}$ такого рода называются линейно независимыми.

Действительно, пользуясь введенными при доказательстве теоремы 57 обозначениями, мы из (37) получили бы

$$0 = \sum_{i=1}^{n} u_i \sum_{k=1}^{n} c_{ik}\vartheta^{k-1},$$

следовательно, если u_i принадлежат к k и не все равны нулю, мы имели бы

$$\sum_{i=1}^{n} u_i c_{ik} = 0 \quad (k = 1, \ldots, n),$$

и, значит,

$$|c_{ik}| = 0,$$

в противоречие с теоремой 57.

Обратно, если система $\omega^{(1)}, \ldots, \omega^{(n)}$ не фундаментальная, то этот определитель равен нулю. Тогда, как известно, n однородных относительно u_i уравнений

$$\sum_{i=1}^{n} c_{ik} u_i = 0 \quad (k = 1, \ldots, n)$$

разрешимы, и притом среди ненулевых решений необходимо существуют такие, которые получаются из коэфициентов c_{ik} путем рациональных операций, следовательно, принадлежат к k. Но для таких решений мы имели бы

$$\sum_{i=1}^{n} u_i \omega^{(i)} = 0.$$

Тем самым доказательство теоремы 58 завершено.

Из теоремы 58 вытекает, что если $\omega^{(1)}, \ldots, \omega^{(n)}$ — фундаментальная система поля K, то числом α из этого поля однозначно определяются коэфициенты в его разложении

$$\alpha = \sum_{i=1}^{n} x_i \omega^{(i)},$$

если, конечно, потребовать, чтобы они принадлежали к k.

Определитель, составленный из n чисел $\omega^{(i)}$ и их сопряженных, мы будем обозначать через

$$|\omega_k^{(i)}| = \Delta(\omega^{(1)}, \ldots, \omega^{(n)}).$$

(Индекс k указывает здесь строку, а i — столбец определителя.) Из (35) следует, что

$$\Delta(\omega^{(1)}, \ldots, \omega^{(n)}) = |c_{ik}| \Delta(1, \vartheta, \ldots, \vartheta^{n-1}).$$

Поэтому, согласно теореме 57, этот определитель отличен от нуля для фундаментальных систем и только для них, ибо, как известно,

$$\Delta(1, \vartheta, \ldots, \vartheta^{n-1}) = \begin{vmatrix} 1 & \vartheta_1 & \vartheta_1^2 & \ldots & \vartheta_1^{n-1} \\ 1 & \vartheta_2 & \vartheta_2^2 & \ldots & \vartheta_2^{n-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \vartheta_n & \vartheta_n^2 & \ldots & \vartheta_n^{n-1} \end{vmatrix} = \prod_{1 \leqslant i < k \leqslant n} (\vartheta_i - \vartheta_k) \neq 0.$$

Последний определитель есть целая рациональная функция от $\vartheta_1, \ldots, \vartheta_n$ с коэфициентами из k (даже из $k(1)$). Если мы переставим какие-нибудь из ϑ_i, то определитель в крайнем случае изменит знак; следовательно, квадрат его симметричен относительно $\vartheta_1, \ldots, \vartheta_n$ и поэтому есть число основного поля k. То же самое имеет место, следовательно, и для $\Delta^2(\omega^{(1)}, \ldots, \omega^{(n)})$. Очевидно также, что это число не зависит от нумерации сопряженных чисел.

Легко установить, что между всякими $n+1$ величинами $\beta^{(1)}, \ldots, \beta^{(n+1)}$ поля K всегда имеет место линейное соотношение

$$\sum_{i=1}^{n+1} u_i \beta^{(i)} = 0,$$

где коэфициенты u_i — числа из основного поля k, не все равные нулю. *Степень поля K можно, следовательно, определить также как максимальное число линейно независимых элементов в K.*

Рассмотрим, наконец, поле $K(\vartheta)$ не относительно k, а относительно другого поля $K(\alpha)$, являющегося алгебраическим полем степени m относительно k, порожденным числом α, удовлетворяющим неприводимому уравнению m-й степени в k и содержащимся в $K(\vartheta)$. $K(\vartheta)$ есть поэтому алгебраическое поле над $K(\alpha)$, степени $q \leqslant n$, так как производящее число ϑ удовлетворяет уже уравнению n-й степени с коэфициентами из k, значит, a fortiori из $K(\alpha)$. $K(\alpha)$ называется *под-полем поля* $K(\vartheta)$. Если рассматривать $K(\alpha)$ как основное поле, то каждая величина из $K(\vartheta)$ может быть однозначно приведена к виду

$$\omega = \gamma_0 + \gamma_1 \vartheta + \ldots + \gamma_{q-1} \vartheta^{q-1},$$

где величины γ суть числа из $K(\alpha)$; точно так же каждое число из $K(\alpha)$ допускает однозначное представление

$$c_0 + c_1 \alpha + \ldots + c_{m-1} \alpha^{m-1},$$

где коэфициенты c принадлежат k. Таким образом каждое ω допускает однозначное представление в виде линейной комбинации mq величин $\alpha^i \vartheta^k$ ($i = 0, 1, \ldots, m-1$; $k = 0, 1, \ldots, q-1$) с коэфициентами из k. Эти mq чисел также образуют поэтому фундаментальную систему в $K(\vartheta)$ (относительно основного поля k), следовательно, $mq = n$, $q = \frac{n}{m}$. Этим доказана следующая теорема:

Теорема 59. *Если α есть число m-й степени относительно k и β есть число q-й степени относительно $K(\alpha; k)$, то поле $K(\alpha, \beta; k)$ имеет степень mq относительно k. Кроме того, числа $\vartheta_1, \ldots, \vartheta_n$ ($n = mq$), сопряженные с производящим числом поля $K(\alpha, \beta; k)$ относительно k, распадаются на m рядов по q в каждом, причем q чисел одного ряда образуют систему чисел, сопряженных относительно $K(\alpha_i)$, где $\alpha_1, \ldots, \alpha_m$ суть m чисел, сопряженных с α относительно k.*

Поле $K(\beta; k)$, которое совпадает со всеми своими сопряженными полями $K(\beta_i; k)$, $i = 1, \ldots, n$, называется *полем Галуа* или *нормальным полем* относительно k. Всякое числовое поле $K(\alpha; k)$ всегда содержится как под-поле в некотором поле Галуа. Именно, нетрудно убедиться с помощью метода, примененного в доказательстве теоремы 52, что поле, получающееся присоединением всех относительно сопряженных чисел $\alpha_1, \ldots, \alpha_m$, есть поле Галуа относительно k.

В последующем мы будем заниматься исключительно числами, алгебраическими относительно $k(1)$, т. е. просто алгебраическими. О числах другого рода мы только упомянем следующее:

Числа, не являющиеся алгебраическими, называются *трансцендентными*. Существование трансцендентных чисел впервые доказал Лиувилль (1851)[1]), одновременно указавший метод построения произвольного количества таких чисел. Позднее (1874) совершенно другое доказательство существования трансцендентных чисел дал Георг Кантор[2]), показав, что множество трансцендентных чисел имеет даже высшую „мощность", чем множество алгебраических чисел. Однако установление трансцендентности или нетрансцендентности чисел в конкретных случаях до сих пор удавалось весьма редко[3]). Общие методы для этого не известны. Трансцендентность числа e доказал Эрмит (1873)[4]), трансцендентность числа π — Линдеманн (1882)[5]); их доказательства были впоследствии значительно упрощены Гильбертом, Гурвицем и Горданом[6]).

---

[1]) Liouville, Sur des classes très étendus de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques, Journal de Mathématiques pures et appliquées, sér. I, t. 16, 1851.

[2]) Cantor, Über eine Eigenschaft der Inbegriffes aller reellen algebraischen Zahlen, Crelles Journal f. d. reine u. angew. Mathematik, Bd. 77, 1874.

[3]) В 1934 г. советским математиком А. О. Гельфондом была решена известная седьмая проблема Гильберта (из числа двадцати трех, указанных Гильбертом) о трансцендентности числа η^x, где η — отличное от единицы алгебраическое, а x — любое иррациональное, но алгебраическое число. См. Gelfond, C. R. Paris, 1929, 1, 2, и Доклады Академии наук СССР, 1934, т. II, № 1; см. также Труды Второго Всесоюзного съезда математиков, т. I, изд. Ак. наук СССР, 1935, стр. 141—164. *Ред.*

[4]) Hermite, Sur la fonction exponentielle, Comptes rendus, t. 77, 1873.

[5]) Lindemann, Über die Zahl π, Mathem. Annalen, Bd. 20, 1882.

[6]) Эти три работы находятся в Mathem. Annalen, Bd. 43, 1892.

ГЛАВА V

ОБЩАЯ АРИФМЕТИКА АЛГЕБРАИЧЕСКИХ ЧИСЛОВЫХ ПОЛЕЙ

§ 21. Определение целых алгебраических чисел. Делимость. Единицы

Понятия, развитые в предыдущей главе в отношении к некоторому основному полю k, мы будем теперь относить к абсолютной области рациональности $k = k(1)$. В основе арифметики алгебраических чисел лежит понятие целого алгебраического числа. К понятию целочисленности представляется естественным предъявить следующие требования:

1. Если α, β — целые алгебраические числа, то такими же должны быть также $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$.

2. Если целое алгебраическое число рационально, то оно должно быть обыкновенным целым числом.

3. Если число α есть целое алгебраическое, то такими же должны быть и его сопряженные (относительно $k(1)$).

Согласно условию 1, каждое целое рациональное относительно целых алгебраических чисел выражение с целыми рациональными коэфициентами должно быть целым алгебраическим числом. В частности, согласно условию 3, все элементарные симметрические функции целого алгебраического числа и его сопряженных должны быть целыми алгебраическими числами; но, с другой стороны, они рациональны, следовательно, согласно условию 2, они должны быть целыми рациональными числами. Поэтому, если α есть целое алгебраическое число, то в неприводимом в $k(1)$ уравнении со старшим коэфициентом 1, которому удовлетворяет α, коэфициенты должны быть целыми рациональными числами. В соответствии с этим целые алгебраические числа определяют следующим образом:

Определение. Алгебраическое число α степени n называется *целым алгебраическим числом*, если в неприводимом в $k(1)$ уравнении со старшим коэфициентом 1, которому удовлетворяет α, коэфициенты суть целые рациональные числа.

В дальнейшем мы под „целым числом будем всегда понимать „целое алгебраическое число".

Для определенных таким образом целых чисел требования 2 и 3, очевидно, выполняются.

ТЕОРЕМА 60. *Если α вообще удовлетворяет уравнению с целыми рациональными коэфициентами и со старшим коэфициентом* 1, *то α — целое.*

Действительно, пусть

$$\varphi(x) = x^N + a_1 x^{N-1} + \ldots + a_N$$

имеет целые рациональные коэфициенты и $\varphi(\alpha) = 0$. Пусть, далее,

$$f(x) = c_0 x^n + c_1 x^{n-1} + \ldots + c_n$$

— неприводимый в $k(1)$ полином, имеющий α корнем; мы можем, очевидно, предполагать, что коэфициенты c_i этого полинома — целые рациональные с наибольшим общим делителем 1 и $c_0 > 0$. По теореме 49, $f(x) \mid \varphi(x)$. Следовательно,

$$\frac{\varphi(x)}{f(x)} = \frac{b' g(x)}{b}$$

есть полином с рациональными коэфициентами, в котором при соответствующем выборе целых рациональных и положительных чисел b и b' можно $g(x)$ считать целочисленным полиномом, наибольший общий делитель коэфициентов которого равен единице. Но из

$$b\varphi(x) = b' f(x) g(x)$$

следует, что $b = b'$, так как по теореме 13а, $f(x)g(x)$, как произведение двух примитивных полиномов, примитивно, и $\varphi(x)$ также примитивно. Но из $\varphi(x) = f(x)g(x)$ путем сравнения старших коэфициентов получается, что c_0 должно делить старший коэфициент полинома φ, т. е. единицу, следовательно, $c_0 = 1$, что и требовалось доказать.

Доказанная теорема более пригодна для проверки целости алгебраического числа, чем приведенное выше определение, ибо в ней не требуется установления неприводимости полинома, корнем которого данное число является.

ТЕОРЕМА 61. *Сумма, разность и произведение двух целых чисел также есть целое число; поэтому каждая целая рациональная функция от целых чисел с целочисленными коэфициентами является также целым числом.*

В самом деле, пусть $\alpha_1, \ldots, \alpha_n$ — числа, сопряженные с целым числом α, и точно так же $\beta_1, \ldots, \beta_m$ — числа, сопряженные с целым числом β. Тогда

$$F(x) = \prod_{i=1}^{n} \prod_{k=1}^{m} (x - (\alpha_i + \beta_k))$$

есть полином относительно x, коэфициенты которого симметричны как относительно $\alpha_1, \ldots, \alpha_n$, так и относительно $\beta_1, \ldots, \beta_m$. Но так как, по предположению, элементарные симметрические функции как чисел α, так и чисел β суть целые рациональные числа, то по основной тео-

реме о симметрических функциях $F(x)$ есть целочисленный полином в $k(1)$; при этом старший коэфициент его равен единице и, значит, его корни $\alpha+\beta$ суть целые числа. Точно так же доказывается утверждение относительно $\alpha-\beta$ и $\alpha\beta$. Таким образом целые алгебраические числа действительно удовлетворяют всем поставленным выше (см. стр. 81) условиям.

Комбинируя соображения, использованные при доказательстве теорем 61 и 51, легко получаем следующий результат:

Теорема 62. *Если ω есть корень уравнения*

$$x^m+\alpha x^{m-1}+\beta x^{m-2}+\ldots+\lambda=0,$$

где α, β, ..., λ — целые числа, то ω также есть целое число.

Таким образом, например, корень m-й степени из целого числа также есть целое число.

Теорема 63. *Каждое алгебраическое число α можно умножением на соответственным образом выбранное целое рациональное число (отличное от нуля) превратить в целое число.*

В самом деле, пусть

$$c_0x^n+c_1x^{n-1}+\ldots+c_{n-1}x+c_n=0$$

— уравнение с целыми рациональными коэфициентами, которому удовлетворяет α, и $c_0\neq 0$. Умножением на c_0^{n-1} мы получим целочисленное уравнение относительно $y=c_0x$ со старшим коэфициентом 1, которое имеет корень $c_0\alpha$.

Понятие целого алгебраического числа влечет за собой и определение делимости:

Целое число α называется *делящимся* на целое число $\beta(\neq 0)$, если $\frac{\alpha}{\beta}$ есть целое число; как и для обыкновенных целых чисел, делимость α на β записывается так: $\beta\,|\,\alpha$.

Если $\beta\,|\,\alpha$ и $\beta\,|\,\gamma$, то $\beta\,|\,\lambda\alpha+\mu\gamma$ при любых целых λ, μ, так как по теореме 61

$$\frac{\lambda\alpha+\mu\gamma}{\beta}=\lambda\frac{\alpha}{\beta}+\mu\frac{\gamma}{\beta}$$

есть целое число.

Целое число ε называется единицей, если $\frac{1}{\varepsilon}$ также есть целое число.

Если ε входит в 1, то ε входит также в $1\cdot\alpha=\alpha$, т. е. в каждое целое число; числа, сопряженные с единицей (относительно $k(1)$), также суть единицы; каждый делитель единицы и каждое произведение единиц также есть единица.

Два целых числа α и β, отличающихся только множителем, являющимся единицей, называются *ассоциированными*.

Для того чтобы целое число ε было единицей, необходимо и достаточно, чтобы произведение всех его сопряженных было равно ± 1.

Действительно, это произведение $\varepsilon_1 \dots \varepsilon_n$ как элементарная симметрическая функция есть целое рациональное число a и как произведение единиц есть также единица, т. е. $a \mid 1$ и, значит, $a = \pm 1$. Обратно, если $\varepsilon_1 \dots \varepsilon_n = \pm 1$, то $\frac{1}{\varepsilon_1} = \pm \varepsilon_2 \dots \varepsilon_n$ также есть целое число, следовательно, ε_1 есть единица.

Все корни из числа 1, очевидно, суть единицы; кроме того, они все имеют абсолютную величину 1. Но существует бесчисленное множество других единиц. Так, например, единицами являются числа $2 \pm \sqrt{3}$, ибо оба они — целые числа, как корни уравнения $x^2 - 4x + 1 = 0$ и

$$\frac{1}{2+\sqrt{3}} = 2 - \sqrt{3}, \quad \frac{1}{2-\sqrt{3}} = 2 + \sqrt{3}.$$

Заметим теперь, что $\varepsilon = 2 - \sqrt{3} < 1$ и > 0, поэтому среди степеней ε, ε^2, ε^3, ... существуют произвольно малые числа. Кратные этих чисел $N\varepsilon^k$ ($N = \pm 1, \pm 2, \dots, k = 1, 2, \dots$), очевидно, лежат поэтому всюду плотно в совокупности вещественных чисел; но, с другой стороны, все они — целые числа, принадлежащие полю $K(\sqrt{3})$. Таким образом, если вещественные целые алгебраические числа расположить по величине, то *не существует целого числа, ближайшего к данному*. Это обстоятельство имеет своим следствием то, что многие методы доказательств, которыми мы пользовались в теории целых рациональных чисел, нельзя перенести на общие целые алгебраические числа.

Каждое целое число α имеет бесчисленное множество „тривиальных" делителей, именно, ε и $\varepsilon\alpha$, где ε пробегает все единицы. Но если даже отвлечься от этих тривиальных разложений, то все же α может быть разложено на целые множители, например,

$$\alpha = \sqrt{\alpha}\,\sqrt{\alpha},$$

каждый из которых — не единица (если, конечно, α — не единица). Поэтому в области всех целых алгебраических чисел не существует неразложимых чисел и, значит, наверное не существует также аналога с рациональными простыми числами.

Чтобы получить неразложимые числа, необходимо область рассматриваемых чисел ограничить рамками определенного числового поля n-й степени.

§ 22. Целые числа поля как абелева группа. Базис и дискриминант поля

Мы кладем в основу дальнейших исследований определенное алгебраическое числовое поле $K(\vartheta)$, порожденное алгебраическим числом ϑ степени n. Без всякого ограничения общности можно предполагать, что ϑ — число целое, так как ϑ всегда можно превратить в целое умножением на некоторое целое рациональное число, а поле $K(\vartheta)$

от этого не изменится. Для чисел, сопряженных с ϑ, мы предполагаем установленной определенную нумерацию; этим, как показано в § 19, установлена также определенная нумерация для сопряженных каждого числа из K. С настоящего момента мы будем пользоваться для нумерации сопряженных верхними индексами.

Мы определяем теперь для каждого числа α из поля K

$$\textit{норму}\ \alpha = N(\alpha) = \alpha^{(1)} \dots \alpha^{(n)}$$

и

$$\textit{след}\ \alpha = S(\alpha) = \alpha^{(1)} + \dots + \alpha^{(n)}.$$

Очевидно

$$N(\alpha\beta) = N(\alpha)\,N(\beta) \text{ и } S(\alpha+\beta) = S(\alpha) + S(\beta).$$

$N(\alpha)$ и $S(\alpha)$ суть рациональные числа и притом целые рациональные, если α есть число целое. $N(\alpha) = 0$ только для $\alpha = 0$. Если α — целое число, отличное от нуля, то $\alpha \mid N(\alpha)$ и частное $\frac{N(\alpha)}{\alpha}$ принадлежит полю K.

Теорема 64. *Целые числа поля K образуют по сложению абелеву группу без кручения. Эта группа имеет n базисных элементов. Таким образом в K существует n таких целых чисел $\omega_1, \dots, \omega_n$, что мы получим все целые числа из K, и притом каждое точно один раз, если в выражении*

$$\alpha = x_1\omega_1 + \dots + x_n\omega_n$$

мы заставим числа x_i независимо друг от друга пробежать все целые рациональные значения. Мы будем говорить, что числа ω образуют базис поля.

Первая часть теоремы следует непосредственно из теоремы 61. Чтобы доказать вторую часть, мы сначала исследуем представление целых чисел ρ поля в виде

$$\rho = c_0 + c_1\vartheta + \dots + c_{n-1}\vartheta^{n-1}$$

с рациональными c. Эти коэфициенты c можно однозначно определить из n сопряженных уравнений

$$\rho^{(i)} = c_0 + c_1\vartheta^{(i)} + \dots + c_{n-1}\vartheta^{(i)n-1} \qquad (i = 1, \dots, n),$$

так как определитель $\Delta = \Delta(1, \vartheta, \dots, \vartheta^{n-1})$ отличен от нуля (см. § 20). В результате решения мы получаем, что $\Delta \cdot c_k$ равно определителю, среди элементов которого фигурируют только числа $\rho^{(i)}$ и степени чисел $\vartheta^{(i)}$. Так как ρ и ϑ — целые, то этот определитель во всяком случае есть целое алгебраическое число A_k. Но из

$$c_k = \frac{A_k}{\Delta} = \frac{A_k\Delta}{\Delta^2}$$

вытекает, что $A_k\Delta = \Delta^2 c_k$ есть целое рациональное число; в самом деле, оно целое в силу того, что A_k и Δ — целые, и оно рационально, так как Δ^2 и c_k рациональны. Следовательно,

$$c_k = \frac{x_k}{D},$$

где x_k — целое рациональное число и знаменатель $D = |\Delta^2|$ не зависит от ρ. Таким образом система чисел

$$\alpha = x_0\frac{1}{D} + x_1\frac{\vartheta}{D} + \ldots + x_{n-1}\frac{\vartheta^{n-1}}{D},$$

получающихся, когда x_i независимо друг от друга пробегают все целые рациональные значения, содержит все целые числа поля (и сверх того может быть еще и нецелые числа) и сама во всяком случае есть абелева группа без кручения (по сложению) с базисом из n элементов, а именно, $\frac{1}{D}, \frac{\vartheta}{D}, \ldots, \frac{\vartheta^{n-1}}{D}$. Но тогда по теореме 34 содержащаяся в этой группе подгруппа всех целых чисел поля также имеет базис. Эта подгруппа имеет по теореме 40 конечный индекс, так как для каждого α из рассматриваемой группы $D\alpha$ (т. е. в смысле теории групп D-я степень элемента α), очевидно, есть целое число и принадлежит поэтому подгруппе. Следовательно, по теореме 35 базис группы целых чисел поля также состоит из n элементов. Тем самым теорема полностью доказана.

Две различные системы базисных элементов связаны, согласно теореме 38, зависимостью

$$\alpha_i = \sum_{k=1}^{n} c_{ik}\omega_k \qquad (i = 1, \ldots, n)$$

с целыми рациональными c_{ik}, определитель которых равен ± 1. Таким образом $\Delta^2(\omega_1, \ldots, \omega_n)$ не зависит от выбора базиса и вполне определяется самим полем. Так как $1, \vartheta, \ldots, \vartheta^{n-1}$ во всяком случае представляются линейными комбинациями чисел ω_i, то эти последние образуют фундаментальную систему, и потому (см. § 20) $\Delta^2 \neq 0$.

Определение. Не зависящее, по доказанному, от выбора базиса число $\Delta^2(\omega_1, \ldots, \omega_n)$ называется *дискриминантом поля* и будет обозначаться через d. d есть отличное от нуля целое рациональное число.

Нетрудно также убедиться в том, что для фундаментальной системы из целых α_i всегда $|\Delta^2(\alpha_1, \ldots, \alpha_n)| \geqslant |d|$ и равенство достигается тогда и только тогда, когда фундаментальная система образует базис поля (см. теорему 64), вследствие чего базис поля называется также *минимальным базисом*.

Естественно в связи со всем сказанным ввести понятие модуля. Под *модулем* (из целых чисел) в поле K мы будем понимать такую систему целых чисел из K, которая вместе с α и β всегда содержит также $\alpha - \beta$ (а значит, и $\alpha + \beta$) и которая содержит число, отличное от нуля.

Таким образом числа модуля образуют при композиции путем сложения абелеву группу без кручения, являющуюся подгруппой группы всех целых чисел поля и имеющую поэтому, в силу теоремы 34, базис из k элементов, где $0 < k \leqslant n$. Такие модули мы называем

k-членными. В дальнейшем мы будем иметь дело только с n-членными модулями. Они, очевидно, характеризуются тем, что содержат n линейно независимых чисел.

§ 23. Разложение целых чисел поля $K(\sqrt{-5})$ на множители. Наибольшие общие делители, не принадлежащие полю

Мы сосредоточим теперь наше внимание на изучении мультипликативного строения целых чисел поля. Целое число α называется *неразложимым в K*, если α не может быть представлено в виде произведения двух целых чисел из K, каждое из которых не есть единица. Таким образом свойство быть неразложимым присуще числу не самому по себе, но лишь по отношению к определенному полю. Каждое рациональное простое число неразложимо в $k(1)$, но, например, 3 разлагается на $\sqrt{3}\cdot\sqrt{3}$ в поле $K(\sqrt{3})$.

Возникает вопрос: существуют ли неразложимые числа также в алгебраических полях степени выше первой и можно ли каждое целое число поля представить в виде произведения таких неразложимых чисел одним (в существенных чертах) и только одним способом?

Мы на некоторых числовых примерах покажем, что однозначность разложения *не* всегда имеет место, и постараемся вскрыть причины этого явления.

Для этого мы рассмотрим поле $K(\sqrt{-5})$. Производящее его число $\vartheta=\sqrt{-5}$ есть корень уравнения $x^2+5=0$ и, как число невещественное, наверное не удовлетворяет никакому уравнению низшей степени в $k(1)$, следовательно, имеет степень 2. Все числа из $K(\sqrt{-5})$ имеют поэтому вид

$$\alpha=r_1+r_2\sqrt{-5},$$

где r_1 и r_2 рациональны. Число, сопряженное с α, мы будем обозначать через α'. Имеем

$$\alpha'=r_1-r_2\sqrt{-5}, \quad \text{следовательно,} \quad (\alpha')'=\alpha.$$

Целые числа в $K(\sqrt{-5})$ суть числа $m+n\sqrt{-5}$ с целыми рациональными m, n. Действительно, для того чтобы α из $K(\sqrt{-5})$ было целым, необходимо и достаточно, чтобы $\alpha+\alpha'$ и $\alpha\alpha'$ были целыми (рациональными) числами, т. е. чтобы целыми были

$$2r_1 \quad \text{и} \quad r_1^2+5r_2^2.$$

Это показывает прежде всего, что знаменатели чисел r_1 и r_2 не могут превышать числа 2. Положим $r_1=\frac{g_1}{2}$, $r_2=\frac{g_2}{2}$. Тогда $\frac{g_1^2+5g_2^2}{4}$ должно быть целым, т. е. должно удовлетворяться сравнение

$$g_1^2+5g_2^2\equiv 0 \pmod 4.$$

Но все квадраты $\equiv 0$ или $1 \pmod 4$, поэтому g_1 и g_2 должны быть четными, а следовательно, r_1 и r_2 должны быть целыми.

В поле $K(\sqrt{-5})$ не существует других единиц, кроме ± 1. В самом деле, для единицы $\varepsilon = m + n\sqrt{-5}$ должно иметь место равенство

$$\pm 1 = N(\varepsilon) = \varepsilon\varepsilon' = m^2 + 5n^2.$$

Но при $n \neq 0$ имеем $m^2 + 5n^2 \geqslant 5$, следовательно, $n = 0$ и $m = \pm 1$, т. е. $\varepsilon = \pm 1$.

Теперь, целые числа

$$\alpha = 1 + 2\sqrt{-5},$$
$$\alpha' = 1 - 2\sqrt{-5},$$
$$\beta = 3,$$
$$\rho = 7$$

неразложимы в $K(\sqrt{-5})$. В самом деле, если бы $\beta = 3$ разлагалось в произведение $\gamma\delta$, в котором оба множителя отличны от единицы, то мы имели бы

$$9 = N(3) = N(\gamma)\,N(\delta).$$

Но разложение числа 9 на целые рациональные положительные множители, из которых ни один не равен единице, возможно только в виде $9 = 3 \cdot 3$, так что должно было бы быть

$$N(\gamma) = N(\delta) = 3,$$

и для $\gamma = x + y\sqrt{-5}$ с целыми рациональными x, y мы имели бы

$$x^2 + 5y^2 = 3, \quad x^2 \leqslant 3, \quad 5y^2 \leqslant 3,$$

что, очевидно, невозможно. Следовательно, $\beta = 3$ неразложимо в $K(\sqrt{-5})$. Таким же образом убеждаемся в том, что $\rho = 7$ неразложимо. Если бы, наконец, α разлагалось в произведение $\gamma\delta$ с $N(\gamma) \neq 1$ и $N(\delta) \neq 1$, то мы имели бы

$$N(\gamma)\,N(\delta) = N(\alpha) = 21,$$

следовательно, либо $N(\gamma) = 3$, $N(\delta) = 7$, либо наоборот. Но мы только что видели, что не может быть никакого целого γ с $N(\gamma) = 3$. Следовательно, α, а потому и его сопряженное α', неразложимо.

Таким образом *число* 21 *двумя существенно различными способами представлено в виде произведения неразложимых в* $K(\sqrt{-5})$ *целых чисел*:

$$21 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = 3 \cdot 7.$$

Чтобы уяснить себе это обстоятельство, — когда неразложимое число 3, являясь делителем произведения $\alpha\alpha'$, в то же время не входит ни в один из множителей α и α', — заметим, что оба неразложимых в $K(\sqrt{-5})$ числа α и 3, хотя и не имеют общего множителя, принадлежащего $K(\sqrt{-5})$ (за исключением ± 1), тем не менее

имеют общий множитель (не являющийся единицей) в другом поле. В самом деле, квадраты

$$\alpha^2 = -19 + 4\sqrt{-5}$$

и

$$\beta^2 = 9$$

делятся на целое число

$$\lambda = 2 + \sqrt{-5},$$

не являющееся единицей:

$$\alpha^2 = (2+\sqrt{-5})(-2+3\sqrt{-5}),$$

$$\beta^2 = (2+\sqrt{-5})(2-\sqrt{-5}).$$

Следовательно, $\frac{\alpha^2}{\lambda}$ и $\frac{\beta^2}{\lambda}$ — целые, а потому, в силу теоремы 62, являются целыми и их квадратные корни

$$\frac{\alpha}{\sqrt{\lambda}} \quad \text{и} \quad \frac{\beta}{\sqrt{\lambda}}.$$

Точно так же квадраты α'^2 и ρ^2 делятся на $\varkappa = 2+3\sqrt{-5}$:

$$\alpha'^2 = (-2+\sqrt{-5})(2+3\sqrt{-5}),$$

$$\rho^2 = 7^2 = (2+3\sqrt{-5})(2-3\sqrt{-5}),$$

т. е.

$$\frac{\alpha'}{\sqrt{\varkappa}} \quad \text{и} \quad \frac{\rho}{\sqrt{\varkappa}}$$

— целые. Теперь число $\sqrt{\lambda}$ (не принадлежащее полю $K(\sqrt{-5})$) имеет в точности свойства наибольшего общего делителя чисел α и β: каждое целое число ω — из $K(\sqrt{-5})$ или не из него, — входящее в α и в β, входит также и в $\sqrt{\lambda}$, и каждое целое число, входящее в $\sqrt{\lambda}$, есть также делитель чисел α и β. Последняя часть утверждения непосредственно вытекает из определения делимости. Первая же часть утверждения вытекает из того обстоятельства, что число $\sqrt{\lambda}$ может быть представлено в виде

$$A\alpha + B\beta = \sqrt{\lambda} \tag{38}$$

с целыми (конечно, не принадлежащими полю $K(\sqrt{-5})$) A и B, например,

$$A = -\frac{2\alpha}{\sqrt{\lambda}}, \quad B = -\frac{(4-\sqrt{-5})\beta}{\sqrt{\lambda}},$$

и таким образом, если $\omega \mid \alpha$ и $\omega \mid \beta$, то из равенства (38) действительно следует $\omega \mid \sqrt{\lambda}$.

Двойное разложение

$$\alpha\alpha' = \beta\rho$$

на неразложимые в $K(\sqrt{-5})$ множители оказывается возможным потому, что

$$\alpha = \sqrt{\lambda}\,\sqrt{-\varkappa'}, \quad \beta = \sqrt{\lambda}\,\sqrt{\lambda'},$$

$$\alpha' = \sqrt{\lambda'}\,\sqrt{-\varkappa}, \quad \rho = \sqrt{\varkappa}\,\sqrt{\varkappa'},$$

и в произведении

$$21 = \sqrt{\lambda}\,\sqrt{\lambda'}\,\sqrt{-\varkappa}\,\sqrt{-\varkappa'}$$

четыре не принадлежащих полю множителя несколькими способами могут быть соединены в пары, дающие при перемножении числа из K, причем все они попарно взаимно просты.

Мы можем теперь сформулировать два важнейших из полученных нами результатов следующим образом.

I. Может случиться, что два неразложимых в $K(\sqrt{-5})$ числа, отличающихся не только единичным множителем, имеют общий делитель, который тогда не принадлежит полю $K(\sqrt{-5})$.

II. Совокупность целых чисел из $K(\sqrt{-5})$, делящихся на неразложимое число α из K, не обязательно должна совпадать с совокупностью целых чисел из $K(\sqrt{-5})$, делящихся на (не принадлежащий K и не являющийся единицей) делитель числа α.

Так, в разобранном выше случае α неразложимо, $\sqrt{\lambda}$ есть делитель α и число $\beta = 3$ делится на $\sqrt{\lambda}$, но не делится на α, хотя и принадлежит полю $K(\sqrt{-5})$.

В поле $k(1)$ ни то, ни другое не может случиться. В самом деле, два неразложимых числа, отличающихся не только единичным множителем, представляют здесь всегда два существенно различных, т. е. взаимно простых, числа, скажем, p, q, из которых всегда можно составить 1:

$$1 = px + qy,$$

с помощью целых рациональных x, y. Отсюда следует, что общие делители чисел p и q должны входить в 1, т. е. должны быть единицами. Далее, если p — простое число и φ — произвольное входящее в p целое (вообще говоря, не рациональное) число, не являющееся единицей, то совокупность всех целых рациональных чисел, делящихся на φ, образует модуль и поэтому, согласно теореме 2, совпадает с совокупностью всех кратных некоторого целого рационального числа n. Кроме того, p должно входить в n, так как в противном случае из n и p можно было бы скомбинировать 1, и φ входило бы тогда в 1. Следовательно, $n = \pm p$, т. е. *каждое рациональное число, делящееся на φ, делится также и на p, если только φ не есть единица и является делителем p, где p — простое число.*

Мы видим, таким образом, что в высших алгебраических полях неразложимые числа не являются последними строительными камнями, из которых можно составить каждое число поля, поскольку они, вообще говоря, не обладают указанным только что свойством простых чисел.

Речь идет теперь о расширении области чисел таким образом, чтобы ввести в рассмотрение также и те числа, которые, как указанные выше $\sqrt{\lambda}$, $\sqrt{\varkappa}$, являются наибольшими общими делителями чисел поля, не принадлежа в то же время сами полю. При этом нам нет необходимости рассматривать именно самые индивидуумы $\sqrt{\lambda}$, $\sqrt{\varkappa}$, так как при исследованиях внутри K нам нет нужды считать различными два алгебраических числа, обладающих тем свойством, что каждое число из K, делящееся на одно из них, делится и на другое. Поэтому мы будем характеризовать не принадлежащее полю K число A просто заданием совокупности чисел поля, делящихся на A.

Подобная совокупность целых чисел обладает следующим свойством: если ей принадлежат α и β, то ей принадлежат также $\lambda\alpha + \mu\beta$, где λ и μ — произвольные целые числа поля. Но теперь, оказывается (правда, в нашем изложении этот результат будет получен значительно позже), что справедливо и обратное предложение: Если множество целых чисел из K обладает указанным свойством, то существует некоторое — возможно не принадлежащее полю K — целое алгебраическое число A такое, что рассматриваемое множество состоит из всех чисел поля, делящихся на A. Такое множество можно, следовательно, рассматривать как образ целого числа; оно называется, по Дедекинду, *идеалом*. Куммер, который еще прежде исследовал эти соотношения для случая поля деления круга и которого следует считать творцом теории идеалов, назвал числа A, которые являются наибольшими общими делителями чисел поля, не принадлежа в то же время полю, *идеальными числами поля*.

Как явствует из этих предварительных замечаний, мы при дальнейшем развитии теории идеалов постоянно должны иметь в виду, что идеалы служат только для того, чтобы известное, не принадлежащее полю число характеризовать при помощи операций внутри поля. В области, расширенной с помощью идеалов, вновь найдут себе место, точно так же как в теории целых рациональных чисел, понятие простого числа и факт однозначного разложения на простые элементы.

§ 24. Определение и основные свойства идеалов

Определение. Система S из целых чисел поля K называется *идеалом в* K (короче, *идеалом*), если вместе с α и β к S принадлежит также каждая комбинация $\lambda\alpha + \mu\beta$ при произвольных целых коэфициентах λ, μ из K[1]).

Таким образом свойство быть идеалом принадлежит системе S не абсолютно, а лишь по отношению к определенному полю K. Идеалы мы в дальнейшем будем обозначать готическими буквами $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$,... Идеал, состоящий из одного только числа 0, мы будем обозначать через (0); этот идеал во многих отношениях занимает исключительное

[1]) Начиная с § 31, мы будем пользоваться несколько более общим определением идеала, при котором принимаются во внимание также и нецелые числа.

положение. Два идеала $\mathfrak{a}$, $\mathfrak{b}$ называются равными ($\mathfrak{a} = \mathfrak{b}$), если они состоят из одних и тех же чисел. Примерами идеалов служат:

I. Множество S чисел, представляемых некоторой определенной линейной формой $\xi_1\alpha_1 + \ldots + \xi_r\alpha_r$ с целыми $\alpha_1, \ldots, \alpha_r$ из K, когда $\xi_1, \ldots, \xi_r$ пробегают все целые числа из K. Это числовое множество называется *областью значений* формы. Этот идеал мы будем обозначать через $(\alpha_1, \ldots, \alpha_r)$.

II. Множество всех целых чисел из K, делящихся на определенное целое число A, независимо от того, принадлежит ли A к полю или нет.

Как уже упомянуто, мы в качестве окончательного результата нашей теории получим, что каждый идеал может быть охарактеризован как множество вида II (см. § 33). Но уже теперь мы можем доказать следующую теорему:

Теорема 65. *Каждый идеал $\mathfrak{a}$ может быть представлен в форме $(\alpha_1, \ldots, \alpha_r)$ при надлежащем выборе целых α из K. При этом можно даже принять $r \leqslant n$.*

Действительно, числа идеала $\mathfrak{a}$, отличного от (0) (случай $\mathfrak{a} = (0)$ тривиален), очевидно, образуют бесконечную абелеву группу по сложению, составляющую подгруппу группы всех целых чисел из K. Поэтому идеал $\mathfrak{a}$, согласно теореме 34, имеет базис, число элементов которого $\leqslant n$. С другой стороны, число элементов базиса по теореме 37 равно числу независимых элементов в $\mathfrak{a}$, следовательно, равно n, так как, если $\alpha \neq 0$ принадлежит к $\mathfrak{a}$, то n независимых чисел α, $\vartheta\alpha$, $\vartheta^2\alpha, \ldots, \vartheta^{n-1}\alpha$ также принадлежат к $\mathfrak{a}$. Таким образом каждый идеал $\mathfrak{a} \neq (0)$ содержит точно n таких чисел $\alpha_1, \ldots, \alpha_n$, что когда в

$$\alpha = x_1\alpha_1 + \ldots + x_n\alpha_n$$

числа $x_1, \ldots, x_n$ пробегают все целые рациональные значения, то α пробегает все числа идеала и притом каждое точно один раз. Такая система $\alpha_1, \ldots, \alpha_n$ называется *базисом идеала*. В силу определения идеала, числа из $\mathfrak{a}$ образуют тогда одновременно также область значений формы $\xi_1\alpha_1 + \ldots + \xi_n\alpha_n$, следовательно, $\mathfrak{a} = (\alpha_1, \ldots, \alpha_n)$; но часть чисел α может линейно выражаться, с целыми коэфициентами из K, через другие, так что имеем (меняя в случае нужды нумерацию) $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$, $r \leqslant n$.

Заметим, что $(\alpha_1, \ldots, \alpha_r) = (\beta_1, \ldots, \beta_s)$ тогда и только тогда, когда каждое α линейно выражается через числа β и каждое β линейно выражается через числа α, с целыми коэфициентами из K. В частности, следовательно,

$$\mathfrak{a} = (\alpha_1, \ldots, \alpha_r) = (\alpha_1, \ldots, \alpha_r, \omega) = \\ = (\alpha_1 - \lambda\omega, \alpha_2, \ldots, \alpha_r, \omega), \tag{39}$$

каковы бы ни были число ω из $\mathfrak{a}$ и целое число λ из K.

Идеал $\mathfrak{a}$ называется *главным идеалом*, если существует такое целое число α из K, что $\mathfrak{a} = (\alpha)$. $(\alpha) = (\beta)$ тогда и только тогда, когда α и β ассоциированы, т. е. отличаются только единичным множителем.

В поле $k(1)$, каждый идеал, будучи модулем, если он отличен от (0), есть по теореме 2 главный идеал. Напротив, в поле $K(\sqrt{-5})$, как показывают рассмотрения предыдущего параграфа, идеал $(1+2\sqrt{-5}, 3)$ не есть главный идеал. Он состоит из всех чисел поля K, делящихся на $\sqrt{\lambda}$.

Если

$$(\alpha_1, \ldots, \alpha_r) = (A_1, \ldots, A_s) \quad \text{и} \quad (\beta_1, \ldots, \beta_p) = (B_1, \ldots, B_q),$$

то

$$(\alpha_1\beta_1, \ldots, \alpha_i\beta_k, \ldots, \alpha_r\beta_p) = (A_1B_1, \ldots, A_lB_m, \ldots, A_sB_q).$$

Действительно,

$$\alpha_i = \sum_l \lambda_{il}A_l, \quad \beta_k = \sum_m \mu_{km}B_m,$$

так что

$$\alpha_i\beta_k = \sum_{l,m} \lambda_{il}\mu_{km}A_lB_m$$

с целыми λ, μ; но точно так же и, обратно, каждое A_lB_m есть линейная комбинация чисел $\alpha_i\beta_k$ с целыми коэфициентами.

Под *произведением* $\mathfrak{ab}$ двух идеалов $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ и $\mathfrak{b} = (\beta_1, \ldots \beta_p)$ мы будем понимать однозначно определенный, согласно сделанному только что замечанию, идеалами $\mathfrak{a}$ и $\mathfrak{b}$ идеал

$$\mathfrak{ab} = (\alpha_1\beta_1, \ldots, \alpha_i\beta_k, \ldots, \alpha_r\beta_p).$$

Из этого определения непосредственно следует, что умножение идеалов коммутативно и ассоциативно:

$$\mathfrak{ab} = \mathfrak{ba}, \quad \mathfrak{a}(\mathfrak{bc}) = (\mathfrak{ab})\mathfrak{c}.$$

Мы полагаем $\mathfrak{a} = \mathfrak{a}^1$, и для каждого целого рационального положительного m, $\mathfrak{a}^{m+1} = \mathfrak{a}^m\mathfrak{a}$, так что, как и для обычных степеней, $\mathfrak{a}^p\mathfrak{a}^q = \mathfrak{a}^{p+q}$.

Мы будем называть идеал $\mathfrak{a}$ *делящимся* на идеал $\mathfrak{c}$, или идеал $\mathfrak{c}$ *делителем* идеала $\mathfrak{a}$, если $\mathfrak{c} \neq (0)$ и существует такой идеал $\mathfrak{b}$, что $\mathfrak{a} = \mathfrak{bc}$. Делимость идеала $\mathfrak{a}$ на идеал $\mathfrak{c}$ записываем обычным способом: $\mathfrak{c} \mid \mathfrak{a}$.

Связь между делимостью чисел и идеалов устанавливается следующим предложением: *Главный идеал* (α) *делится на главный идеал* $(\gamma) \neq (0)$ *тогда и только тогда, когда число* α *делится на число* γ.

Действительно, из $(\alpha) = (\gamma)(\beta_1, \ldots, \beta_r) = (\gamma\beta_1, \ldots, \gamma\beta_r)$ следует $\alpha = \sum_i \lambda_i\gamma\beta_i = \gamma\sum_i \lambda_i\beta_i$ с целыми λ_i, следовательно, $\gamma \mid \alpha$. Обратно, если $\gamma \mid \alpha$, так что при некотором целом β имеем $\alpha = \gamma\beta$, то $(\alpha) = (\gamma)(\beta)$ и $(\gamma) \mid (\alpha)$.

Единичный идеал (1) состоит из всех целых чисел поля; если в каком-либо идеале имеется число 1, то он содержит все целые

числа поля и потому равен (1). Для каждого идеала $\mathfrak{a} \neq (0)$ имеют место соотношения

$$\mathfrak{a} = \mathfrak{a} \cdot (1), \quad \mathfrak{a} \mid \mathfrak{a}, \quad (1) \mid \mathfrak{a}, \quad \mathfrak{a} \mid (0).$$

Каждый идеал $\mathfrak{a}$ имеет „тривиальные" делители $\mathfrak{a}$ и (1).

Определение. Идеал $\mathfrak{p}$ называется *простым идеалом*, если он отличен от (1), и, кроме $\mathfrak{p}$ и (1), не имеет никаких других делителей.

Вопрос о существовании простых идеалов мы пока оставляем открытым.

Для обоснования теории идеалов и для действий над ними решающее значение имеет то обстоятельство, что делимость идеалов может быть сведена к делимости чисел, а не только наоборот. Основой для этого служит следующая теорема:

Теорема 66. *Для каждого идеала* $\mathfrak{a}$ *существует такой отличный от* (0) *идеал* $\mathfrak{b}$, *что* $\mathfrak{ab}$ *есть главный идеал.*

В способе доказательства этой теоремы различаются между собой разные методы обоснования теории идеалов. Мы здесь применим метод Гурвица, значительно упрощенный Штейницем. Он основывается на обобщении теоремы Гаусса на полиномы с целыми алгебраическими коэфициентами.

Теорема 67. *Пусть*

$$A(x) = \alpha_p x^p + \alpha_{p-1} x^{p-1} + \ldots + \alpha_0, \quad B(x) = \beta_r x^r + \beta_{r-1} x^{r-1} + \ldots + \beta_0$$

— полиномы с целыми коэфициентами, $\alpha_p \neq 0$, $\beta_r \neq 0$. *Если при этом целое число* δ *входит множителем во все коэфициенты* γ *произведения*

$$C(x) = A(x) B(x) = \gamma_s x^s + \gamma_{s-1} x^{s-1} + \ldots + \gamma_0,$$

то оно входит также во все произведения $\alpha_i \beta_k$.

Для доказательства этого утверждения докажем предварительно две леммы.

Лемма а). *Если*

$$f(x) = \delta_m x^m + \delta_{m-1} x^{m-1} + \ldots + \delta_1 x + \delta_0 \quad (\delta_m \neq 0)$$

— полином с целыми коэфициентами и ρ *— его корень, то* $\dfrac{f(x)}{x-\rho}$ *также имеет целые коэфициенты.*

Прежде всего $\delta_m \rho$ во всяком случае есть целое число, ибо это следует из теоремы 62 точно таким же способом, как и при доказательстве теоремы 63.

Далее, лемма справедлива при $m = 1$, когда $\rho = -\dfrac{\delta_0}{\delta_1}$, $\dfrac{f(x)}{x-\rho} = \delta_1$.

Допустим, что она уже доказана для всех полиномов степени $\leqslant m-1$; так как

$$\varphi(x) = f(x) - \delta_m x^{m-1}(x-\rho),$$

очевидно, есть целочисленный (в силу нашего первого замечания) полином степени $m-1$ с корнем ρ, то

$$\frac{\varphi(x)}{x-\rho} = \frac{f(x)}{x-\rho} - \delta_m x^{m-1},$$

а следовательно, и $\frac{f(x)}{x-\rho}$ есть целочисленный полином. Тем самым путем полной индукции лемма a) доказана.

Лемма b). *Если, при прежних обозначениях,*

$$f(x) = \delta_m (x-\rho_1)\ldots(x-\rho_m),$$

то также $\delta_m \rho_1 \ldots \rho_k$ *для каждого* k, $1 \leqslant k \leqslant m$, *есть целое число.*

Действительно, повторным применением леммы a) мы получаем, что

$$\frac{f(x)}{(x-\rho_{k+1})(x-\rho_{k+2})\ldots(x-\rho_m)} = \delta_m (x-\rho_1)\ldots(x-\rho_k)$$

есть целочисленный полином; но свободный член его равен $\pm \delta_m \rho_1 \ldots \rho_k$.

Перейдем теперь к доказательству теоремы 67. Пусть

$$A(x) = \alpha_p (x-\rho_1)\ldots(x-\rho_p),$$
$$B(x) = \beta_r (x-\sigma_1)\ldots(x-\sigma_r)$$

— разложения полиномов $A(x)$ и $B(x)$ на линейные множители. По предположению, полином

$$\frac{C(x)}{\delta} = \frac{\alpha_p \beta_r}{\delta}(x-\rho_1)\ldots(x-\sigma_r)$$

имеет целые коэфициенты, и, следовательно, по лемме b), каждое произведение

$$\frac{\alpha_p \beta_r}{\delta} \rho_{n_1} \ldots \rho_{n_i} \sigma_{m_1} \ldots \sigma_{m_k}, \tag{40}$$

где $n_1, \ldots, n_i$ и $m_1, \ldots, m_k$ — любые системы различных индексов ($i \leqslant p$, $k \leqslant r$), есть целое число. Но так как $\frac{\alpha_i}{\alpha_p}$ и $\frac{\beta_k}{\beta_r}$ суть элементарные симметрические функции соответственно чисел ρ и σ, то $\frac{\alpha_i \beta_k}{\delta}$ есть сумма членов вида (40) и, значит, — целое число, что и требовалось доказать.

Теперь мы в состоянии доказать теорему 66. Пусть $\alpha = (\alpha_1, \ldots, \alpha_r)$. Образуем целочисленный полином

$$g(x) = \alpha_1 x + \ldots + \alpha_r x^r$$

и сопряженные с ним полиномы

$$g^{(i)}(x) = \alpha_1^{(i)} x + \ldots + \alpha_r^{(i)} x^r \quad (i = 1, \ldots, n),$$

среди которых, скажем, при $i=1$, фигурирует и наш первоначальный полином $g(x)$. Произведение

$$F(x)=\prod_{i=1}^{n} g^{(i)}(x)=\sum_{p} c_p x^p,$$

как выражение, симметрическое относительно сопряженных величин, есть полином с целыми рациональными коэфициентами c_p. $F(x)$ делится на $g(x)$, и частное

$$h(x)=\frac{F(x)}{g(x)}=\prod_{i=2}^{n} g^{(i)}(x)$$

есть, следовательно, полином с коэфициентами из K, являющимися, сверх того, целыми числами, так что

$$h(x)=\beta_1 x+\ldots+\beta_m x^m$$

с целыми β из K. Обозначим через N наибольший общий делитель целых рациональных чисел c_p, так что $\frac{F(x)}{N}$ — примитивный полином, и положим

$$\mathfrak{b}=(\beta_1, \ldots, \beta_m).$$

Мы утверждаем, что имеет место равенство

$$\mathfrak{a}\mathfrak{b}=(N).$$

Действительно, $\mathfrak{a}\mathfrak{b}=(\ldots, \alpha_i\beta_k, \ldots)$. По теореме 67 N входит во все $\alpha_i\beta_k$, так как оно входит в каждый коэфициент произведения $g(x)\,h(x)$. Поэтому в

$$\alpha_i\beta_k=\lambda_{ik}N$$

λ_{ik} есть целое число и, значит, все $\alpha_i\beta_k$, а следовательно, и все числа из $\mathfrak{a}\mathfrak{b}$ принадлежат (N). С другой стороны, так как N есть наибольший общий делитель всех коэфициентов c_p полинома $h(x)\,g(x)$, то существуют такие целые рациональные числа x_p, что

$$N=c_1x_1+c_2x_2+\ldots$$

Каждое c есть сумма произведений $\alpha_i\beta_k$, так что N может быть представлено в виде

$$N=\sum_{i,k}\mu_{ik}\alpha_i\beta_k$$

с целыми (и даже рациональными) μ_{ik}; поэтому N и все числа из (N) принадлежат к $\mathfrak{a}\mathfrak{b}$, что в соединении с доказанными выше и дает $(N)=(\mathfrak{a}\mathfrak{b})$.

Основываясь на последней теореме, мы можем теперь доказать однозначность деления идеалов.

Теорема 68. *Если* $\mathfrak{a}\mathfrak{b}=\mathfrak{a}\mathfrak{c}$ *и* $\mathfrak{a}\neq(0)$, *то* $\mathfrak{b}=\mathfrak{c}$.

В самом деле, определим идеал $\mathfrak{m}$ так, чтобы $\mathfrak{am}$ было главным идеалом, $\mathfrak{am} = (\alpha)$. Тогда

$$\mathfrak{amb} = \mathfrak{amc}, \quad (\alpha)\mathfrak{b} = (\alpha)\mathfrak{c}.$$

Последнее равенство означает, что произведение α на каждое число из $\mathfrak{b}$ равно произведению α на некоторое число из $\mathfrak{c}$, и обратно, т. е каждое число из $\mathfrak{b}$ принадлежит $\mathfrak{c}$ и каждое число из $\mathfrak{c}$ принадлежит $\mathfrak{b}$. Следовательно, $\mathfrak{b} = \mathfrak{c}$.

Отсюда мы получаем теперь новое определение делимости:

Теорема 69. *Идеал* $\mathfrak{c} = (\gamma_1, \ldots, \gamma_r)$ *тогда и только тогда есть делитель идеала* $\mathfrak{a} = (\alpha_1, \ldots, \alpha_m)$, *если каждое число из* $\mathfrak{a}$ *содержится в* $\mathfrak{c}$.

В самом деле, если $\mathfrak{c} \mid \mathfrak{a}$, то существует такое $\mathfrak{b} = (\beta_1, \ldots, \beta_p) \neq (0)$, что

$$(\alpha_1, \ldots, \alpha_m) = (\beta_1, \ldots, \beta_p)(\gamma_1, \ldots, \gamma_r) = (\ldots, \beta_i\gamma_k, \ldots),$$

так что каждое число α из $\mathfrak{a}$ может быть представлено в виде

$$\alpha = \sum_{i,k} \lambda_{ik}\beta_i\gamma_k = \sum_{k=1}^{r} \gamma_k \left(\sum_{i=1}^{p} \lambda_{ik}\beta_i \right)$$

с целыми λ_{ik}, т. е. принадлежит $\mathfrak{c}$.

Если, обратно, известно, что каждое число из $\mathfrak{a}$ есть также число из $\mathfrak{c}$, т. е. для любых целых λ_{ik} существуют такие целые μ_{pk}, что

$$\sum_i \lambda_{ik}\alpha_i = \sum_p \mu_{pk}\gamma_p,$$

то тогда и для каждого идеала $\mathfrak{d} = (\delta_1, \ldots, \delta_s)$

$$\sum_k \sum_i \lambda_{ik}\alpha_i\delta_k = \sum_k \sum_p \mu_{pk}\gamma_p\delta_k,$$

т. е. каждое число из $\mathfrak{ad}$ принадлежит также $\mathfrak{cd}$. Выберем теперь $\mathfrak{d}$ так чтобы $\mathfrak{cd} = (\delta)$ было главным идеалом ($\delta \neq 0$). Если $\mathfrak{ad} = (\rho_1, \rho_2, \ldots)$, то каждое ρ_i есть число из (δ), т. е. имеет вид $\lambda_i\delta$ с целым λ_i, и потому

$$(\rho_1, \rho_2, \ldots) = (\delta)(\lambda_1, \lambda_2, \ldots)$$

или

$$\mathfrak{ad} = \mathfrak{cd} \quad (\lambda_1, \lambda_2, \ldots),$$

значит, на основании теоремы 68

$$\mathfrak{a} = \mathfrak{c} \cdot (\lambda_1, \lambda_2, \ldots),$$

т. е. $\mathfrak{c} \mid \mathfrak{a}$.

Отметим следующие непосредственные следствия этой теоремы (предполагается, что $\mathfrak{a} \neq (0)$):

Целое число α входит в $\mathfrak{a}$ тогда и только тогда, когда $\mathfrak{a} \mid (\alpha)$. Если $\mathfrak{a} \mid (\alpha)$ и $\mathfrak{a} \mid (\beta)$, то $\mathfrak{a} \mid (\lambda\alpha + \mu\beta)$ при любых целых λ, μ.

Из $\mathfrak{ab} = (1)$ следует $\mathfrak{a} = (1)$ и $\mathfrak{b} = (1)$.

Если из двух идеалов каждый есть делитель другого, то эти идеалы равны.

§ 25. Основная теорема теории идеалов

Теорема 70. *Для каждых двух идеалов* $\mathfrak{a}=(\alpha_1, \ldots, \alpha_r)$ *и* $\mathfrak{b}=(\beta_1, \ldots, \beta_s)$ *существует однозначно определенный наибольший общий делитель* $\mathfrak{d}=(\mathfrak{a}, \mathfrak{b})$, *т. е. идеал, обладающий следующими свойствами:* $\mathfrak{d}$ *есть делитель идеалов* $\mathfrak{a}$ *и* $\mathfrak{b}$ *и если* $\mathfrak{d}_1 \mid \mathfrak{a}$, *и* $\mathfrak{d}_1 \mid \mathfrak{b}$, *то* $\mathfrak{d}_1 \mid \mathfrak{d}$. *При этом* $\mathfrak{d}=(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s)$.

Мы покажем, что $\mathfrak{d}=(\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s)$ обладает указанными свойствами. Прежде всего, очевидно, все числа из $\mathfrak{a}$ и из $\mathfrak{b}$ принадлежат к $\mathfrak{d}$ и, значит, по теореме 69 $\mathfrak{d} \mid \mathfrak{a}$ и $\mathfrak{d} \mid \mathfrak{b}$.

Если, далее, $\mathfrak{d}_1 \mid \mathfrak{a}$ и $\mathfrak{d}_1 \mid \mathfrak{b}$, то все числа из $\mathfrak{a}$ и из $\mathfrak{b}$, а следовательно, и все суммы каждого числа из $\mathfrak{a}$ с каждым числом из $\mathfrak{b}$ принадлежат к $\mathfrak{d}_1$, т. е. каждое число из $\mathfrak{d}$ принадлежит к $\mathfrak{d}_1$, и, следовательно, $\mathfrak{d}_1 \mid \mathfrak{d}$.

Наконец, если идеал $\mathfrak{d}_2$ также обладает теми же свойствами, то $\mathfrak{d}_2 \mid \mathfrak{d}$ и $\mathfrak{d} \mid \mathfrak{d}_2$, значит, $\mathfrak{d}=\mathfrak{d}_2$. Таким образом указанными свойствами идеал $\mathfrak{d}$ вполне определяется.

Мы видим, что согласно этому *идеал* $\mathfrak{a}=(\alpha_1, \ldots, \alpha_r)$ *можно рассматривать как наибольший общий делитель главных идеалов* $(\alpha_1), \ldots, (\alpha_r)$.

Из выражения для $\mathfrak{d}$ непосредственно следует, что

$$\mathfrak{c} \cdot (\mathfrak{a}, \mathfrak{b}) = (\mathfrak{ca}, \mathfrak{cb}). \tag{41}$$

А отсюда уже вытекает часть основной теоремы:

Теорема 71. *Если для простого идеала* $\mathfrak{p}$ *имеет место* $\mathfrak{p} \mid \mathfrak{ab}$, *то* $\mathfrak{p}$ *есть делитель по крайней мере одного из идеалов* $\mathfrak{a}$, $\mathfrak{b}$.

Действительно, если $\mathfrak{p}$ не входит в множитель $\mathfrak{b}$, то необходимо

$$(\mathfrak{p}, \mathfrak{b}) = (1),$$

так как $\mathfrak{p}$, как простой идеал, не имеет никаких делителей, кроме (1) и $\mathfrak{p}$. Из (41) следует тогда

$$\mathfrak{a} = \mathfrak{a} \cdot (1) = \mathfrak{a} \cdot (\mathfrak{p}, \mathfrak{b}) = (\mathfrak{ap}, \mathfrak{ab}),$$

и так как $\mathfrak{p} \mid \mathfrak{ab}$, то $\mathfrak{p}$ должно делить $\mathfrak{a}$.

Отсюда получается, так же как в теории целых рациональных чисел (теорема 5), что если представление идеала в качестве произведения простых идеалов вообще возможно, то только одним способом, конечно, если отвлечься от порядка множителей.

Чтобы завершить доказательство основной теоремы теории идеалов, нам остается еще, следовательно, доказать, что разложение идеала на простые идеалы всегда возможно. Для этого мы должны доказать два предложения:

a) Каждый идеал $\mathfrak{a}$, отличный от (0), имеет только конечное число делителей.

b) Каждый делитель идеала $\mathfrak{a}$ ($\mathfrak{a} \neq (0)$), отличный от самого $\mathfrak{a}$, имеет меньше делителей, чем $\mathfrak{a}$.

Для доказательства предложения a) заметим прежде всего, что так как каждый идеал $\mathfrak{a}$, отличный от (0), есть делитель нескольких главных идеалов (α) и так как при этом каждый делитель идеала $\mathfrak{a}$ есть также делитель идеала (α), то достаточно доказать конечность числа делителей для каждого главного идеала (α). При этом α можно считать целым рациональным числом, так как $\alpha \mid N(\alpha)$, следовательно, $(\alpha) \mid (N(\alpha))$, а $N(\alpha) = N$ есть целое рациональное число.

По теореме 69 идеал (N) делится только на такие идеалы $\mathfrak{a}$, в которых содержится число N. Пусть теперь $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ есть делитель идеала (N), так что $\mathfrak{a}$ содержит N. В силу теоремы 65, можно принять $r \leqslant n$. Но в силу равенства (39), для любых целых λ_i из K

$$(\alpha_1, \ldots, \alpha_r) = (\alpha_1, \ldots, \alpha_r, N) = (\alpha_1 - N\lambda_1, \alpha_2 - N\lambda_2, \ldots, \alpha_r - N\lambda_r, N).$$

Покажем, что λ_i можно выбрать так, чтобы числа $\alpha_i - N\lambda_i$ принадлежали определенной конечной области значений. Пусть $\omega_1, \ldots, \omega_n$ — базис поля. Для каждого целого числа $\alpha = x_1\omega_1 + \ldots + x_n\omega_n$, очевидно, можно подобрать такое целое $\lambda = u_1\omega_1 + \ldots + u_n\omega_n$ (x_i и u_i — целые рациональные числа), чтобы в

$$\alpha - N\lambda = (x_1 - Nu_1)\,\omega_1 + \ldots + (x_n - Nu_n)\,\omega_n$$

n целых рациональных чисел $x_i - Nu_i$ принадлежали интервалу $(0, N-1)$. Среди этих чисел, которые мы будем называть здесь „приведенными mod N“, существует только $|N|^n$ различных. Выберем теперь λ_i так, чтобы все числа $\alpha_i - \lambda_i N$ были приведенными mod N. Тогда числа $\alpha_i - \lambda_i N$, которых не более n, принадлежат некоторому определенному конечному множеству чисел, определяемому исключительно числом N. Из них можно поэтому образовать только конечное число различных идеалов $\mathfrak{a}$, т. е. (N) имеет только конечное число делителей, чем предложение a) и доказано. Чтобы доказать b), допустим, что $\mathfrak{c}$ есть делитель идеала $\mathfrak{a}$, отличный от самого $\mathfrak{a}$, так что $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, где $\mathfrak{b} \neq (1)$, $\mathfrak{c} \neq \mathfrak{a}$. Тогда $\mathfrak{c}$ наверное не имеет $\mathfrak{a}$ в качестве делителя, а следовательно, имеет по крайней мере одним делителем меньше, чем $\mathfrak{a}$. Тем самым также предложение b) доказано.

Мы можем теперь утверждать, что среди конечного числа, скажем, m, делителей идеала $\mathfrak{a} \neq (1)$, отличных от (1), должен быть по крайней мере один простой идеал, а именно, в силу предложения b), простыми идеалами будут из указанных делителей те, которые сами имеют наименьшее число делителей. Таким образом от $\mathfrak{a}$ можно отделить простой идеал $\mathfrak{p}_1$, $\mathfrak{a} = \mathfrak{p}_1\mathfrak{a}_1$, где $\mathfrak{a}_1$ имеет уже не больше $m-1$ множителей $\neq (1)$; если $\mathfrak{a}_1 \neq (1)$, то от $\mathfrak{a}_1$ можно, далее, отделить простой идеал $\mathfrak{p}_2$, так что получим $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{a}_2$, где $\mathfrak{a}_2$ имеет уже не больше $m-2$ делителей $\neq (1)$, и т. д. Так как числа делителей идеалов $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$ убывают, то этот процесс должен после конечного числа k шагов закончиться, что может наступить только тогда, когда $\mathfrak{a}_k = (1)$. Тогда $\mathfrak{a}$ будет представлено как произведение простых идеалов, $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_k$. В соединении с теоремой 71 это дает *основную теорему теории идеалов*:

Теорема 72. *Каждый идеал в K, отличный от* (0) *и* (1), *можно одним и только одним способом (если отвлечься от порядка множителей) представить в виде произведения конечного числа простых идеалов.*

§ 26. Первые применения основной теоремы

В том, что доказанная нами основная теорема теории идеалов может служить для исследования свойств делимости чисел поля, можно убедиться, например, из того, что она дает совершенно новый метод для решения вопроса о том, делится ли целое число α на целое число β или нет. Согласно § 24, надо исследовать, делится ли (α) на (β). Для этого мы разлагаем оба последних идеала на их различные простые множители:

$$\left.\begin{aligned}(\alpha) &= \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\ldots\mathfrak{p}_k^{a_k},\\ (\beta) &= \mathfrak{p}_1^{b_1}\mathfrak{p}_2^{b_2}\ldots\mathfrak{p}_k^{b_k}\end{aligned}\right\}\quad (a_i,\ b_i \geqslant 0),$$

и на основании теоремы 72 β входит в α тогда и только тогда, когда $a_i - b_i \geqslant 0$ для $i = 1, \ldots, k$.

Теорема 73. *В каждом поле существует бесчисленное множество простых идеалов.*

Действительно, каждое рациональное простое число p определяет идеал (p), и если p, q — различные положительные простые числа, то $((p), (q)) = (1)$; так как для некоторых целых рациональных x, y имеем $px + qy = 1$), и, значит, в $((p), (q))$ входит число 1. Поэтому в (p) и (q) никогда не входят одни и те же простые идеалы, следовательно, существует по крайней мере столько простых идеалов, сколько положительных простых чисел p.

Мы упростим теперь наш способ выражения, *опуская при обозначении главных идеалов скобки* там, где это не повлечет опасности недоразумений. При этом мы должны, однако, иметь всегда в виду, что из равенства идеалов α и β следует только, что $\alpha = \beta \times$ единица. Точно так же мы в формулировке всех предложений, относящихся к делимости какого-либо главного идеала (α), будем заменять идеал числом α. Так, утверждение: α делится на $\mathfrak{a}$ будет означать: (α) делится на $\mathfrak{a}$. Утверждение $\beta \mid \alpha$ уже имеет смысл, определенный ранее, но, согласно § 24, оно действительно равнозначно с утверждением $(\beta) \mid (\alpha)$. Наибольший общий делитель $\alpha_1, \ldots, \alpha_r$ есть теперь идеал $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$. Если он равен (1), то мы называем числа $\alpha_1, \ldots, \alpha_r$ *взаимно простыми*. Для того чтобы числа $\alpha_1, \ldots, \alpha_r$ были взаимно простыми, необходимо и достаточно, чтобы $\mathfrak{a}$ содержал число 1, т. е. чтобы существовали такие целые числа λ_i из K, для которых

$$\lambda_1\alpha_1 + \ldots + \lambda_r\alpha_r = 1.$$

Из $\mathfrak{a} \mid \alpha$ и $\mathfrak{a} \mid \beta$ следует $\mathfrak{a} \mid \lambda\alpha + \mu\beta$ при любых целых λ, μ из K.

Теорема 74. Если $\mathfrak{a}$, $\mathfrak{b}$ — *отличные от* (0) *и друг от друга идеалы, то всегда существует такое число* ω, *что*

$$(\omega, \mathfrak{ab}) = \mathfrak{a}.$$

Такое ω, очевидно, должно иметь разложение $\omega = \mathfrak{ac}$, где $(\mathfrak{c}, \mathfrak{b}) = (1)$. Следовательно, теорема утверждает, что каждый идеал $\mathfrak{a}$ можно превратить в главный идеал умножением на некоторый идеал $\mathfrak{c}$, взаимно простой с данным идеалом $\mathfrak{b}$.

Для доказательства обозначим через $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ все различные входящие в $\mathfrak{ab}$ простые идеалы, и пусть будет $\mathfrak{a} = \mathfrak{p}_1^{a_1} \ldots \mathfrak{p}_r^{a_r}$ $(a_i \geqslant 0)$. Определим r идеалов $\mathfrak{b}_1, \ldots, \mathfrak{b}_r$ равенствами

$$\mathfrak{p}_i^{a_i+1}\mathfrak{b}_i = \mathfrak{a}\mathfrak{p}_1 \ldots \mathfrak{p}_r \quad (i = 1, \ldots, r),$$

так что $\mathfrak{b}_i$ взаимно просто с $\mathfrak{p}_i$, но все остальные простые идеалы $\mathfrak{p}$ содержит в более высоких степенях, чем $\mathfrak{a}$. Так как эти идеалы $\mathfrak{b}$ в совокупности взаимно просты, то существуют такие числа δ_i из $\mathfrak{b}_i$, что

$$\delta_1 + \ldots + \delta_r = 1.$$

При этом δ_i делится на $\mathfrak{b}_i$, следовательно, на все $\mathfrak{p}_k$ при $k \neq i$, а потому наверное не делится на $\mathfrak{p}_i$, так как 1 на $\mathfrak{p}_i$ не делится.

Определим теперь r чисел α_i так, чтобы $\mathfrak{p}_i^{a_i} \mid \alpha_i$, но $\mathfrak{p}_i^{a_i+1}$ уже не входило бы в α_i. Это, очевидно, всегда возможно; достаточно, чтобы α_i было числом из $\mathfrak{p}_i^{a_i}$, не входящим в $\mathfrak{p}_i^{a_i+1}$. Мы утверждаем, что число

$$\omega = \alpha_1\delta_1 + \ldots + \alpha_r\delta_r$$

обладает свойством, указанным в теореме 74. Действительно, каждый из простых идеалов $\mathfrak{p}_i$ входит в $r-1$ слагаемых $\alpha_k\delta_k$ $(k \neq i)$ по меньшей мере в степени $\mathfrak{p}_i^{a_i+1}$, в то время как в i-е слагаемое он входит точно в степени $\mathfrak{p}_i^{a_i}$. Поэтому ω делится точно на a_i-ю степень каждого простого идеала $\mathfrak{p}_i$ и, значит, $(\omega, \mathfrak{ab}) = \mathfrak{a}$.

Беря теперь в качестве $\mathfrak{ab}$ главный идеал β, делящийся на $\mathfrak{a}$ (см. теорему 66), мы получаем следующий результат:

Теорема 75. *Каждый идеал* $\mathfrak{a}$ *можно представить как наибольший общий делитель двух чисел поля*: $\mathfrak{a} = (\omega, \beta)$.

§ 27. Сравнения и классы вычетов по идеалам. Группа классов вычетов по сложению и по умножению

Мы перенесем теперь в теорию идеалов понятие сравнения, использованное ранее в теории целых рациональных чисел. При этом понадобится ввести лишь незначительные изменения в употреблявшиеся прежде методы доказательств, вследствие чего мы сможем быть при доказательствах очень кратки.

Пусть α и β — два целых числа и $\mathfrak{a}$ — идеал, который мы в этом параграфе будем постоянно предполагать отличным от 0.

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

(читается: α сравнимо с β по модулю $\mathfrak{a}$) есть лишь другая запись соотношения

$$\mathfrak{a} \mid \alpha - \beta.$$

Если $\mathfrak{a}$ не есть делитель $\alpha - \beta$, то мы пишем

$$\alpha \not\equiv \beta \pmod{\mathfrak{a}}.$$

Введенные так сравнения подчиняются тем же вычислительным законам, что и сравнения в поле рациональных чисел, и для рациональных α, β, $\mathfrak{a}$ полностью совпадают с ними.

Все числа, сравнимые между собой по модулю $\mathfrak{a}$, образуют класс вычетов $\bmod \mathfrak{a}$.

Теорема 76. *Число классов вычетов* $\bmod \mathfrak{a}$ *конечно. Обозначим его через* $N(\mathfrak{a})$, *и пусть* $\alpha_1, \ldots, \alpha_n$ *есть базис идеала* $\mathfrak{a}$ *и* d *— дискриминант поля; тогда* $N(\mathfrak{a}) = \left| \frac{\Delta(\alpha_1, \ldots, \alpha_n)}{\sqrt{d}} \right|$. *Если же* $\mathfrak{a}$ *есть главный идеал* α, *то* $N(\mathfrak{a}) = |N(\alpha)|$.

Действительно, числа идеала $\mathfrak{a}$ образуют подгруппу группы $\mathfrak{G}$ всех целых чисел поля. Различные классы вычетов $\bmod \mathfrak{a}$ образуют, очевидно, различные смежные классы, определяемые идеалом $\mathfrak{a}$ внутри $\mathfrak{G}$. Число различных классов вычетов $\bmod \mathfrak{a}$ есть, следовательно, индекс $\mathfrak{a}$ относительно $\mathfrak{G}$. *Этот индекс конечен.* В самом деле, если α есть какое-нибудь отличное от нуля число из $\mathfrak{a}$, то положительное целое рациональное число $a = |N(\alpha)|$ также принадлежит $\mathfrak{a}$, так как $\alpha \mid N(\alpha)$. Следовательно, произведение a на произвольное целое число поля принадлежит $\mathfrak{a}$. Таким образом в терминах теории групп a-я степень каждого элемента из $\mathfrak{G}$ принадлежит $\mathfrak{a}$ и, следовательно, по теореме 40 индекс подгруппы $\mathfrak{a}$ конечен; он обозначается через $N(\mathfrak{a})$ и называется *нормой идеала* $\mathfrak{a}$.

Если теперь $\alpha_1, \ldots, \alpha_n$ — базис $\mathfrak{a}$ и $\omega_1, \ldots, \omega_n$ — базис $\mathfrak{G}$, то имеет место система равенств

$$\alpha_i = \sum_{k=1}^{n} c_{ik}\omega_k \quad (i = 1, \ldots, n)$$

с целыми рациональными c_{ik}, и по теореме 39 абсолютная величина определителя $|c_{ik}|$ равна индексу $N(\mathfrak{a})$. С другой стороны, переходя к сопряженным равенствам, мы получаем

$$\Delta(\alpha_1, \ldots, \alpha_n) = |c_{ik}|\,\Delta(\omega_1, \ldots, \omega_n)$$

и потому, в силу

$$\Delta^2(\omega_1, \ldots, \omega_n) = d \neq 0,$$

имеем

$$N(\mathfrak{a}) = \left| \frac{\Delta(\alpha_1, \ldots, \alpha_n)}{\sqrt{d}} \right|.$$

Наконец, если мы имеем дело с главным идеалом (α), то очевидно, что в качестве базиса можно взять $\alpha\omega_1, \ldots, \alpha\omega_n$, а потому $\Delta(\alpha\omega_1, \ldots, \alpha\omega_n) = N(\alpha)\Delta(\omega_1, \ldots, \omega_n)$ и $N(\mathfrak{a}) = |N(\alpha)|$.

Теорема 78. *Сравнение*

$$\alpha\xi \equiv \beta \pmod{\mathfrak{a}}$$

удовлетворяется при данных целых α, β *некоторым целым числом* ξ *тогда и только тогда, когда* $(\alpha, \mathfrak{a}) \mid \beta$. *Если* $(\alpha, \mathfrak{a}) = 1$, *то решение вполне определено по модулю* $\mathfrak{a}$.

Пусть сначала $(\alpha, \mathfrak{a}) = 1$ и ξ пробегает систему $N(\mathfrak{a})$ чисел, несравнимых по модулю $\mathfrak{a}$. Тогда также $\alpha\xi$ будет пробегать все классы вычетов по модулю $\mathfrak{a}$; действительно, из $\alpha\xi_1 \equiv \alpha\xi_2 \pmod{\mathfrak{a}}$ вытекает $\mathfrak{a} \mid \alpha(\xi_1 - \xi_2)$ и так как, по предположению, $(\alpha, \mathfrak{a}) = 1$, то, вследствие теоремы 72, $\mathfrak{a} \mid (\xi_1 - \xi_2)$, т. е. $\xi_1 \equiv \xi_2 \pmod{\mathfrak{a}}$. Таким образом среди чисел $\alpha\xi$ встретится число, принадлежащее тому же классу вычетов, что и β; соответствующее ξ будет, в силу сказанного, единственным mod $\mathfrak{a}$ решением рассматриваемого сравнения.

Если теперь $(\alpha, \mathfrak{a}) = \mathfrak{d}$ и существует целое число ξ_0 такое, что $\alpha\xi_0 \equiv \beta \pmod{\mathfrak{a}}$, то $\alpha\xi_0 = \beta + \rho$, где $\mathfrak{a} \mid \rho$, и мы имеем поэтому $\mathfrak{d} \mid \rho$, $\mathfrak{d} \mid (\alpha\xi_0 - \rho)$, т. е. $\mathfrak{d} \mid \beta$. Пусть, обратно,

$$\mathfrak{d} = (\alpha, \mathfrak{a}) \mid \beta, \quad \beta = \mathfrak{d}\mathfrak{b}.$$

Положим $\alpha = \mathfrak{d}\mathfrak{a}_1$, $\mathfrak{a} = \mathfrak{d}\mathfrak{a}_2$, так что $(\mathfrak{a}_1, \mathfrak{a}_2) = 1$, и выберем число $\mu = \mathfrak{m}\mathfrak{a}_1$ так, чтобы $(\mu, \mathfrak{a}_1\mathfrak{d}\mathfrak{a}_2) = \mathfrak{a}_1$, т. е. $(\mathfrak{m}, \mathfrak{d}\mathfrak{a}_2) = 1$; в силу теоремы 74, это возможно. Тогда $\mathfrak{d}\mathfrak{a}_1 \mid \mathfrak{m}\mathfrak{a}_1\mathfrak{d}\mathfrak{b}$ или, иначе, $\alpha \mid \mu\beta$. В силу доказанного, сравнение

$$\mu\xi \equiv \frac{\mu\beta}{\alpha} \pmod{\mathfrak{a}_2}$$

разрешимо, ибо $(\mathfrak{m}, \mathfrak{a}_2) = (\mathfrak{a}_1, \mathfrak{a}_2) = 1$ и поэтому $(\mu, \mathfrak{a}_2) = (\mathfrak{m}\mathfrak{a}_1, \mathfrak{a}_2) = 1$. Но из

$$\mathfrak{a}_2 \left| \left(\mu\xi - \frac{\mu\beta}{\alpha}\right)\right.$$

вытекает

$$\alpha\mathfrak{a}_2 \mid (\alpha\mu\xi - \mu\beta),$$

т. е.

$$\mathfrak{d}\mathfrak{a}_1\mathfrak{a}_2 \mid (\mu)(\alpha\xi - \beta), \quad \mathfrak{d}\mathfrak{a}_1\mathfrak{a}_2 \mid \mathfrak{m}\mathfrak{a}_1(\alpha\xi - \beta),$$

$$\mathfrak{d}\mathfrak{a}_2 \mid \mathfrak{m}(\alpha\xi - \beta),$$

и так как $(\mathfrak{m}, \mathfrak{d}\mathfrak{a}_2) = 1$, то получаем $\mathfrak{d}\mathfrak{a}_2 \mid (\alpha\xi - \beta)$ или

$$\alpha\xi \equiv \beta \pmod{\mathfrak{a}}.$$

Два числа, сравнимых по модулю $\mathfrak{a}$, имеют с $\mathfrak{a}$ один и тот же наибольший общий делитель, который определяется, таким образом, классом вычетов, к которому эти числа принадлежат. Число классов вычетов, взаимно простых с $\mathfrak{a}$, мы будем обозначать через $\varphi(\mathfrak{a})$.

Теорема 79. *Для любых двух идеалов* $\mathfrak{a}, \mathfrak{b}$ *всегда* $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.

В самом деле, пусть α — такое делящееся на $\mathfrak{a}$ число, что $(\alpha, \mathfrak{ab}) = \mathfrak{a}$ (см. теорему 74). Пусть, далее, ξ_i $(i = 1, 2, \ldots, N(\mathfrak{b}))$ пробегает полную систему вычетов по модулю $\mathfrak{b}$ и η_k $(k = 1, 2, \ldots, N(\mathfrak{a}))$ — полную систему вычетов по модулю $\mathfrak{a}$. Тогда, в силу теоремы 78, числа $\alpha\xi_i + \eta_k$ попарно несравнимы по модулю $\mathfrak{ab}$. С другой стороны, каждое целое число ρ сравнимо с одним из этих чисел $\alpha\xi_i + \eta_k$ по модулю $\mathfrak{ab}$. Чтобы убедиться в этом, определяем η_k из сравнения

$$\eta_k \equiv \rho \pmod{\mathfrak{a}}$$

и рассматриваем сравнение

$$\alpha\xi \equiv \rho - \eta_k \pmod{\mathfrak{ab}}.$$

Так как $(\alpha, \mathfrak{ab}) = \mathfrak{a}$ и $\mathfrak{a} \mid (\rho - \eta_k)$, то, в силу теоремы 78, это сравнение разрешимо, и вместе с ξ имеет, очевидно, своим решением также все числа, сравнимые с ξ по модулю $\mathfrak{b}$, так что ξ может быть принято равным одному из ξ_i; но тогда $\rho \equiv \alpha\xi_i + \eta_k \pmod{\mathfrak{ab}}$.

Тем самым мы доказали, что $N(\mathfrak{a})N(\mathfrak{b})$ чисел $\alpha\xi_i + \eta_k$ образуют полную систему вычетов по модулю $\mathfrak{ab}$, и их число должно поэтому совпадать с $N(\mathfrak{ab})$.

Теорема 80. *Если* $(\mathfrak{a}, \mathfrak{b}) = 1$, *то* $\varphi(\mathfrak{ab}) = \varphi(\mathfrak{a})\varphi(\mathfrak{b})$. *Имеет место общая формула*

$$\varphi(n) = N(\mathfrak{a}) \prod_{\mathfrak{p} \mid \mathfrak{a}} \left(1 - \frac{1}{N(\mathfrak{p})}\right)$$

где $\mathfrak{p}$ *в произведении пробегает все простые делители идеала* $\mathfrak{a}$.

Для доказательства первой части теоремы выберем α и β так, чтобы $(\alpha, \mathfrak{ab}) = \mathfrak{a}$ и $(\beta, \mathfrak{ab}) = \mathfrak{b}$. Так как $\mathfrak{a}$ и $\mathfrak{b}$ взаимно просты, то, заставляя ξ в форме $\alpha\xi + \beta\eta$ пробегать полную систему вычетов по модулю $\mathfrak{b}$ и η — полную систему вычетов по модулю $\mathfrak{a}$, мы получим полную систему вычетов по модулю $\mathfrak{ab}$, причем $\alpha\xi + \beta\eta$ будет тогда и только тогда взаимно просто с $\mathfrak{ab}$, когда $(\xi, \mathfrak{b}) = 1$ и $(\eta, \mathfrak{a}) = 1$. Тем самым первая часть теоремы доказана.

Рассмотрим теперь степень $\mathfrak{p}^a$ простого идеала $\mathfrak{p}$. Не взаимно простыми с ней являются числа, делящиеся на $\mathfrak{p}$. Среди них имеется $N(\mathfrak{p}^{a-1})$ несравнимых по модулю $\mathfrak{p}^a$. Но $N(\mathfrak{p}^{a-1}) = N(\mathfrak{p})^{a-1}$ (см. теорему 79). Поэтому

$$\varphi(\mathfrak{p}^a) = N(\mathfrak{p})^a - N(\mathfrak{p})^{a-1} = N(\mathfrak{p}^a)\left(1 - \frac{1}{N(\mathfrak{p})}\right).$$

Отсюда, в силу первой части теоремы и теоремы 72, вытекает общая формула для $\varphi(\mathfrak{a})$.

Теорема 81. *Норма простого идеала* $\mathfrak{p}$ *является степенью некоторого рационального простого числа,* $N(\mathfrak{p}) = p^f$. f *называется степенью* $\mathfrak{p}$. *Каждый идеал* (p), *порождаемый рациональным простым числом* p, *распадается самое большее на* n *множителей, где* n — *степень поля.*

В самом деле, по теореме 66 идеал $\mathfrak{p}$ входит в некоторый главный идеал (α) и, значит, в целое рациональное число $N(\alpha)$. Но так как $\mathfrak{p}$ — простой идеал, то по теореме 71 он входит тогда также в некоторое рациональное простое число p. Пусть $p = \mathfrak{p}\mathfrak{a}$, тогда $N(p) = N(\mathfrak{p})N(\mathfrak{a})$ и, следовательно, целое рациональное число $N(\mathfrak{p})$ входит в $N(p) = p^n$, т. е. $N(\mathfrak{p}) = p^f$, $f \leqslant n$. Пусть теперь $p = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r$ — разложение идеала (p) на простые идеальные множители; тогда произведение целых положительных рациональных чисел $N(\mathfrak{p}_i)$ равно $N(p) = p^n$, и так как ни одно из $N(\mathfrak{p}_i)$, очевидно, не равно единице, то их число r не может превосходить n.

Мы получаем, таким образом, одно из немногих предложений, связывающих степень поля с другими свойствами чисел этого поля: если известно, что рациональное простое число p разложимо в некотором числовом поле на k идеальных множителей, то степень поля по меньшей мере равна k.

Так же как теорема 12 для рациональных простых чисел, доказывается

Теорема 82. *Сравнение по простому идеалу* $\mathfrak{p}$

$$x^m + \alpha_1 x^{m-1} + \ldots + \alpha_{m-1}x + \alpha_m \equiv 0 \pmod{\mathfrak{p}}$$

с целыми коэфициентами α *имеет самое большее* m *несравнимых по модулю* $\mathfrak{p}$ *решений* x.

Система $N(\mathfrak{a})$ классов вычетов по модулю $\mathfrak{a}$ образует по сложению абелеву группу, так как класс вычетов, к которому принадлежит сумма $\alpha + \beta$ двух целых чисел α, β, зависит только от классов вычетов, к которым принадлежат слагаемые. Определенную таким образом абелеву группу порядка $N(\mathfrak{a})$ мы будем обозначать через $\mathfrak{G}(\mathfrak{a})$. Теорема 19 в применении к этой группе утверждает, что для всех α

$$\alpha^{N(\mathfrak{a})} \equiv 0 \pmod{\mathfrak{a}}.$$

Для $\alpha = 1$ получаем, в частности,

$$N(\mathfrak{a}) \equiv 0 \pmod{\mathfrak{a}}. \tag{42}$$

Группа $\mathfrak{G}(\mathfrak{a})$, вообще говоря, не циклична, в отличие от случая поля $k(1)$. Пусть, например, $\mathfrak{a} = (a)$, где a — целое положительное рациональное число. Так как число $x_1\omega_1 + \ldots + x_n\omega_n$ (x_i — целые рациональные, $\omega_1, \ldots, \omega_n$ — базис поля) тогда и только тогда делится на a, когда все x_i делятся на a, то форма $x_1\omega_1 + \ldots + x_n\omega_n$ проходит через все классы вычетов по модулю a точно по одному разу, когда x_i независимо друг от друга пробегают значения $0, 1, \ldots, a-1$. Тем самым для каждого входящего в a простого числа p существует, вследствие теоремы 27, точно n базисных классов, порядки которых суть степени p, тогда как по теореме 28 для циклических групп для каждого p должен существовать только один такой базисный класс.

Далее, для простого идеала $\mathfrak{p}$ имеет место следующая теорема:

Теорема 83. *Группа классов вычетов* $\bmod \mathfrak{p}$ *по сложению есть абелева группа* $\mathfrak{G}(\mathfrak{p})$ *порядка* $N(\mathfrak{p}) = p^f$; *число ее базисных элементов равно степени* f *простого идеала* $\mathfrak{p}$.

Действительно, так как $\mathfrak{p} \mid p$, то число классов вычетов, элементы α которых удовлетворяют условию

$$p\alpha \equiv 0 \pmod{\mathfrak{p}},$$

равно числу всех вообще классов вычетов, т. е. p^f, и значит, в силу теоремы 27, f есть число базисных элементов. Иными словами, существует точно f целых чисел $\omega_1, \ldots, \omega_f$, обладающих тем свойством, что $x_1\omega_1 + \ldots + x_f\omega_f$ проходит через все классы вычетов $\bmod \mathfrak{p}$ по одному разу, когда x_i независимо друг от друга пробегают значения $0, 1, \ldots, p-1$.

Таким образом группа $\mathfrak{G}(\mathfrak{p})$ является циклической для простых идеалов первой степени, и только для них. Простые идеалы первой степени, которые, как будет показано в § 43, всегда существуют в бесконечном числе, играют при исследовании числового поля решающую роль.

Система классов вычетов $\bmod \mathfrak{a}$, взаимно простых с $\mathfrak{a}$, образует конечную абелеву группу и по умножению, поскольку класс вычетов, содержащий произведение $\alpha\beta$, определяется классами вычетов, содержащими сомножители α, β, независимо от выбора этих сомножителей в их классах, и при этом, очевидно, он также взаимно прост с $\mathfrak{a}$. Точно таким же образом, как и раньше, мы получаем поэтому следующую теорему:

Теорема 84. *Классы вычетов* $\bmod \mathfrak{a}$, *взаимно простые с* $\mathfrak{a}$, *образуют по умножению абелеву группу порядка* $\varphi(\mathfrak{a})$. *Мы будем обозначать ее через* $\mathfrak{R}(\mathfrak{a})$. *Если* $\mathfrak{p}$ — *простой идеал, то* $\mathfrak{R}(\mathfrak{p})$ — *циклическая группа.*

Число ρ, степени которого дают все классы группы $\mathfrak{R}(\mathfrak{p})$, называется *первообразным корнем* $\bmod \mathfrak{p}$.

Для каждого простого идеала $\mathfrak{p}$ и каждого целого числа α из рассматриваемого поля имеет место обобщение теоремы Ферма:

$$\alpha^{N(\mathfrak{p})} \equiv \alpha \pmod{\mathfrak{p}}. \tag{43}$$

В отличие от случая поля $k(1)$ мы не можем утверждать, что также все группы $\mathfrak{R}(\mathfrak{p}^\alpha)$ цикличны.

Те классы вычетов из $\mathfrak{R}(\mathfrak{p})$, которые могут быть представлены рациональным числом, образуют, очевидно, подгруппу группы $\mathfrak{R}(\mathfrak{p})$. Если $N(\mathfrak{p}) = p^f$, то это суть классы, представимые числами $1, 2, \ldots, p-1$. Указанные числа различны по модулю $\mathfrak{p}$, так как если a и p взаимно просты в $k(1)$, то при подходящем выборе целых рациональных x, y форма $ax + py$ принимает значение 1 и потому (a) и (p) взаимно просты в K, откуда, наконец, вытекает, что также $(a, \mathfrak{p}) = 1$, т. е. a не делится на $\mathfrak{p}$. Для каждого класса A этой подгруппы, состоящей, таким образом, из $p-1$ элементов, A^{p-1} является единичным классом. Но так как вся группа $\mathfrak{R}(\mathfrak{p})$ циклична, то суще-

ствует не больше $p-1$ классов C, для которых $C^{p-1}=1$. Следовательно, подгруппа рациональных классов вычетов из $\mathfrak{R}(\mathfrak{p})$ совпадает с группой классов, дающих при возвышении в $(p-1)$-ю степень единичный класс. Это дает следующую теорему:

Теорема 85. *Для того чтобы число α было сравнимо с рациональным числом по модулю $\mathfrak{p}$, необходимо и достаточно, чтобы* $\alpha^p \equiv \alpha \pmod{\mathfrak{p}}$.

§ 28. Полиномы с целыми алгебраическими коэфициентами

В заключение этих элементарных замечаний о сравнениях мы коснемся еще вкратце функциональных сравнений. Они играют решающую роль в кронекеровском обосновании теории идеалов, некоторые факты которой и поныне проще всего доказываются с их помощью.

В этом параграфе под полиномом будет пониматься целая рациональная функция произвольного числа переменных $x_1, \ldots, x_m$, у которой все коэфициенты при произведениях степеней переменных суть целые числа из K.

Полином $P(x_1, \ldots, x_m)$ называется сравнимым с нулем по модулю $\mathfrak{a}$

$$P(x_1, \ldots, x_m) \equiv 0 \pmod{\mathfrak{a}},$$

если все его коэфициенты делятся на $\mathfrak{a}$. Далее, два полинома P и Q называются сравнимыми между собой по модулю $\mathfrak{a}$, если $P-Q \equiv 0 \pmod{\mathfrak{a}}$. Для полиномов, приводящихся к константам, это определение совпадает с определением сравнимости чисел.

Теорема 86. *Если $\mathfrak{p}$ — простой идеал и*

$$P(x_1, \ldots, x_m)\, Q(x_1, \ldots, x_m) \equiv 0 \pmod{\mathfrak{p}},$$

то по крайней мере один из полиномов P, Q сравним с нулем по модулю $\mathfrak{p}$.

Эта теорема верна для полиномов от 0 переменных, т. е. для констант. Мы докажем ее справедливость в общем случае с помощью индукции. Пусть теорема уже доказана для всех полиномов, число переменных в которых не превосходит m. Каждый полином от $m+1$ переменных может быть представлен в форме

$$P(x_0, x_1, \ldots, x_m) = \sum_k x_0^k P_k(x_1, \ldots, x_m),$$

где P_k — полиномы от m переменных $x_1, \ldots, x_m$. $P \equiv 0 \pmod{\mathfrak{p}}$ означает, очевидно, что $P_k \equiv 0 \pmod{\mathfrak{p}}$ для всех k. Если не все члены полиномов P и Q сравнимы с нулем, — в каковом случае вообще нечего доказывать, — то эти полиномы можно без ограничения общности заменить такими сравнимыми с ними по модулю $\mathfrak{p}$ полиномами, у которых члены с высшими степенями переменного x_0 не сравнимы с нулем. Если эти старшие члены суть соответственно $x_0^p P_p(x_1, \ldots, x_m)$

и $x_0^q Q_q(x_1, \ldots, x_m)$, то старшим членом полинома PQ служит произведение $x_0^{p+q} P_p Q_q$ и из

$$P(x_0, x_1, \ldots, x_m)\, Q(x_0, x_1, \ldots, x_m) \equiv 0 \pmod{\mathfrak{p}}$$

вытекает поэтому

$$P_p(x_1, \ldots, x_m)\, Q_q(x_1, \ldots, x_m) \equiv 0 \pmod{\mathfrak{p}}.$$

Но так как здесь в левой части стоят полиномы от m переменных, то по крайней мере один из них должен быть сравним с нулем по модулю $\mathfrak{p}$, иными словами, по крайней мере в одном из полиномов $P(x_0, \ldots, x_m)$ или $Q(x_0, \ldots, x_m)$ не существует членов, не сравнимых с нулем по модулю $\mathfrak{p}$. Таким образом один из полиномов P или Q должен быть сравним с нулем по модулю $\mathfrak{p}$.

Из этой теоремы вытекает, что если $\mathfrak{p}^a$ и $\mathfrak{p}^b$ — высшие степени простого идеала $\mathfrak{p}$, входящие во все коэфициенты, соответственно, полиномов $A(x_1, \ldots, x_m)$ и $B(x_1, \ldots, x_m)$, то $\mathfrak{p}^{a+b}$ будет высшей степенью $\mathfrak{p}$, входящей во все коэфициенты произведения $A(x_1, \ldots, x_m)\, B(x_1, \ldots, x_m)$.

Доказательство этого утверждения мы проведем следующим образом. Пусть α_1 — какое-нибудь число, содержащее $\mathfrak{p}^a$, так что $\alpha_1 = \mathfrak{a}\mathfrak{p}^a$. Тогда существует такое число $\alpha_2 = \mathfrak{a}\mathfrak{m}$, что $(\mathfrak{m}, \mathfrak{p}) = 1$. В самом деле, если $\mathfrak{p}^m$ — наивысшая степень $\mathfrak{p}$, входящая в $\mathfrak{a}$, то в $\mathfrak{a}$ существуют числа, не входящие в $\mathfrak{p}^{m+1}$, и каждое такое число, очевидно, разлагается требуемым образом. Покажем, что $\frac{\alpha_2}{\alpha_1} A(x_1, \ldots, x_m)$ будет полиномом с целыми коэфициентами, не сравнимым с нулем по модулю $\mathfrak{p}$. Пусть γ — какой-нибудь коэфициент полинома $A(x_1, \ldots, x_m)$, так что $\gamma = c\mathfrak{p}^{a+c}$, где $(\mathfrak{c}, \mathfrak{p}) = 1$ и c — целое рациональное неотрицательное число. Тогда $\frac{\alpha_2\gamma}{\alpha_1} = \frac{\mathfrak{a}\mathfrak{m}c\mathfrak{p}^{a+c}}{\mathfrak{a}\mathfrak{p}^a} = \mathfrak{m}c\mathfrak{p}^c$, т. е. $(\alpha_1) \mid (\alpha_2\gamma)$, а тогда и $\alpha_1 \mid \alpha_2\gamma$, т. е. $\frac{\alpha_2\gamma}{\alpha_1}$ — целое алгебраическое число. Далее, так как полином A имеет коэфициент γ, у которого $c = 0$, то полином $\frac{\alpha_2}{\alpha_1} A$ имеет коэфициент $\frac{\alpha_2\gamma}{\alpha_1} = \mathfrak{m}c$, не делящийся на $\mathfrak{p}$. Определяя аналогичным образом числа $\beta_1 = \mathfrak{b}\mathfrak{p}^b$ и $\beta_2 = \mathfrak{b}\mathfrak{n}$ для полинома $B(x_1, \ldots, x_m)$, мы видим, что, в силу теоремы 86, произведение

$$\frac{\alpha_2}{\alpha_1} A(x_1, \ldots, x_m) \frac{\beta_2}{\beta_1} B(x_1, \ldots, x_m) = C(x_1, \ldots, x_m)$$

есть полином, не сравнимый с нулем по модулю $\mathfrak{p}$. Но $AB = \frac{\alpha_1\beta_1}{\alpha_2\beta_2} C$ есть полином с целыми коэфициентами, и теперь уже нетрудно видеть, что $\mathfrak{p}^{a+b}$ есть высшая степень $\mathfrak{p}$, входящая во все эти коэфициенты. Действительно, пусть γ — какой-нибудь коэфициент полинома C; соответствующим коэфициентом полинома AB будет

$$\gamma' = \frac{\alpha_1\beta_1}{\alpha_2\beta_2}\gamma = \frac{\mathfrak{a}\mathfrak{p}^a\mathfrak{b}\mathfrak{p}^b}{\mathfrak{a}\mathfrak{m}\mathfrak{b}\mathfrak{n}}\gamma = \mathfrak{p}^{a+b}\frac{\gamma}{\mathfrak{m}\mathfrak{n}};$$

так как γ' есть целое число, а m и n взаимно просты с $\mathfrak{p}$, то γ делится на mn и, следовательно, $\mathfrak{p}^{a+b} | \gamma'$. С другой стороны, как мы видели, в C имеется коэфициент γ, не делящийся на $\mathfrak{p}$; соответствующий коэфициент γ' полинома AB не будет делиться поэтому ни на какую степень $\mathfrak{p}$, высшую чем $\mathfrak{p}^{a+b}$.

Назовем *содержанием* полинома P, $J(P)$, идеал, равный наибольшему общему делителю коэфициентов этого полинома. Тогда из доказанного вытекает следующий результат:

Теорема 87. *Содержание произведения двух полиномов равно произведению содержаний множителей.*

Тем самым мы получили существенное усиление кронекеровской теоремы 67, а также обобщение гауссовской теоремы 13а на полиномы нескольких переменных в произвольных алгебраических числовых полях.

Если данный полином удовлетворяет некоторому полиномиальному сравнению по модулю $\mathfrak{a}$, то, заменяя в нем переменные произвольными целыми числами из поля K, которому принадлежит идеал $\mathfrak{a}$, мы получим, очевидно, правильное числовое сравнение по тому же модулю.

Покажем, наконец, что из сравнения

$$\alpha^{N(\mathfrak{p})} \equiv \alpha \pmod{\mathfrak{p}}, \tag{43}$$

которое, как мы видели, справедливо для всех целых α, вытекает, что для всякого полинома $P(x_1, \ldots, x_m)$ имеет место сравнение

$$P(x_1, \ldots, x_m)^{N(\mathfrak{p})} \equiv P(x_1^{N(\mathfrak{p})}, \ldots, x_m^{N(\mathfrak{p})}) \pmod{\mathfrak{p}}. \tag{44}$$

Это утверждение, в силу (43), справедливо для полиномов, состоящих из одного единственного члена. Пусть оно уже доказано для полиномов, содержащих не более k членов. Если G — такой полином и α — произвольное целое число из K, то для каждого положительного рационального простого числа p имеет место сравнение

$$(G(x_1, \ldots, x_m) + \alpha x_1^{a_1} \ldots x_m^{a_m})^p \equiv G^p + \alpha^p x_1^{pa_1} \ldots x_m^{pa_m} \pmod{p},$$

ибо разность между обеими частями этого сравнения, в силу делимости на p биномиальных коэфициентов $\binom{p}{i}$, $i = 1, \ldots, p-1$, есть полином, все коэфициенты которого делятся на p. Повторным возвышением в степень получаем, что для каждого положительного рационального f имеет место сравнение

$$(G + \alpha x_1^{a_1} \ldots x_m^{a_m})^{p^f} \equiv G^{p^f} + \alpha^{p^f} x_1^{p^f a_1} \ldots x_m^{p^f a_m} \pmod{p}.$$

Пусть теперь $\mathfrak{p}$ входит в p и $N(\mathfrak{p}) = p^f$ (см. теорему 81). Тогда написанное только что сравнение справедливо также по модулю $\mathfrak{p}$ и представляет собой сравнение (44) для $(k+1)$-членного полинома, стоящего в левой части в скобках. Тем самым сравнение (44) имеет место для всех полиномов без исключения.

§ 29. Первый тип законов разложения для рациональных простых чисел: разложение в квадратичных числовых полях

После того как в § 27 была установлена связь между рациональными простыми числами и простыми идеалами алгебраического числового поля, естественно возникает задача более точного изучения этой связи. Речь идет о следующих трех вопросах:

1. Сколько различных простых идеалов рассматриваемого числового поля входит в заданное рациональное простое число p?

2. Какую степень имеют эти идеалы?

3. В какой степени входят они в p?

Прежде всего укажем принадлежащий Дедекинду весьма общий результат, относящийся к третьему вопросу:

Простые числа, входящие в дискриминант поля, выделяются среди всех простых чисел тем характеристическим свойством, что они и только они делятся на степень простого идеала высшую, чем первая (см. §§ 36; 38).

В противоположность этому наши познания, относящиеся к первым двум вопросам, чрезвычайно бедны. Общий и исчерпывающий ответ на вопрос о числе и степени простых идеалов, входящих в данное простое рациональное число p, мы можем до сих пор дать лишь для одного очень специального типа алгебраических числовых полей; эти поля вполне характеризуются некоторым свойством их „группы Галуа“ [1]). При этом встречаются два формально совершенно различных типа законов разложения, к ознакомлению с которыми мы сейчас и перейдем.

Что же касается всех других полей, то мы до сих пор не имеем даже и приблизительного представления о природе господствующих в них законов разложения.

Предпошлем исследованию обоих известных типов законов разложения одно общее замечание о полях Галуа.

Каждый идеал $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ поля определяет n идеалов $\mathfrak{a}^{(i)}$ $(i = 1, \ldots, n)$, получающихся из $\mathfrak{a}$ путем замены каждого из входящих в него чисел сопряженным, с одним и тем же индексом i; очевидно, $\mathfrak{a}^{(i)} = (\alpha_1^{(i)}, \ldots, \alpha_r^{(i)})$. Это суть сопряженные с $\mathfrak{a}$ идеалы. В силу теоремы 55, каждое сравнение остается справедливым при замене всех входящих в него чисел и идеалов сопряженными. Но в поле Галуа (см. конец § 20) сопряженные идеалы можно перемножать, так как все они принадлежат этому же полю. При этом имеет место следующая теорема:

Теорема 88. *Для каждого идеала $\mathfrak{a}$ поля Галуа главный идеал $(N(\mathfrak{a}))$ равен $\mathfrak{a}^{(1)}\mathfrak{a}^{(2)}\ldots\mathfrak{a}^{(n)}$.* (См. теорему 107.)

---

[1]) Это — те поля, производящие числа которых могут быть получены с помощью последовательных извлечений корня. Соответствующие уравнения суть так называемые алгебраически разрешимые уравнения с рациональными коэфициентами.

Пусть $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$. Образуем полином $P(x) = \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_r x^r$; наибольший общий делитель его коэфициентов есть $\mathfrak{a}$. Произведение всех сопряженных полиномов

$$f(x) = \prod_{i=1}^{n} (\alpha_1^{(i)} x + \ldots + \alpha_r^{(i)} x^r)$$

будет тогда полиномом с целыми рациональными коэфициентами; пусть (целое рациональное) a — их наибольший общий делитель. Так как число 1 представимо в виде линейной комбинации коэфициентов полинома $\frac{1}{a} f(x)$, то также идеал (a) является наибольшим общим делителем коэфициентов $f(x)$ в рассматриваемом числовом поле В силу теоремы 87 мы имеем тогда

$$\mathfrak{a}^{(1)}\mathfrak{a}^{(2)} \ldots \mathfrak{a}^{(n)} = (a).$$

Но, очевидно, сопряженные идеалы имеют одинаковые нормы. Поэтому, для каждого i,

$$N(\mathfrak{a}^{(1)}) \ldots N(\mathfrak{a}^{(n)}) = N(\mathfrak{a}^{(i)})^n = N((a)) = |a|^n,$$

следовательно,

$$N(\mathfrak{a}^{(i)}) = \pm a, \quad (N(\mathfrak{a}^{(i)})) = (a) = \mathfrak{a}^{(1)} \ldots \mathfrak{a}^{(n)},$$

чем утверждение теоремы и доказано. Это соотношение оправдывает название „норма“ для количества чисел, несравнимых mod $\mathfrak{a}$.

В частности, для простого идеала степени f имеем

$$p^f = N(\mathfrak{p}) = \mathfrak{p}^{(1)} \ldots \mathfrak{p}^{(n)}.$$

Это показывает, что в p входят лишь сопряженные простые идеалы, и если p не делится на квадрат простого идеала, то среди $\mathfrak{p}^{(1)}, \ldots, \mathfrak{p}^{(n)}$ должно быть точно по f совпадающих, так что p будет произведением $k = \frac{n}{f}$ различных среди n сопряженных простых идеалов $\mathfrak{p}^{(i)}$.

Таким образом, *если рациональное простое число p представимо в некотором поле Галуа степени n в виде произведения k различных простых идеалов, то эти последние являются сопряженными и имеют одну и ту же степень $f = \frac{n}{k}$, являющуюся, следовательно, делителем n.*

Мы обратимся теперь к *квадратичным числовым полям*; каждое такое поле можно, без ограничения общности, считать произведенным с помощью корня уравнения $x^2 - D = 0$, где D — положительное или отрицательное целое рациональное число, не делящееся ни на какой рациональный квадрат, кроме 1. Это поле $K(\sqrt{D})$ есть поле Галуа его числа могут быть однозначно представлены в форме

$$\alpha = x + y\sqrt{D},$$

где x и y рациональны, а $\sqrt{D}$ — какое-нибудь произвольно выбранное фиксированное значение корня. Обозначая число, сопряженное с α, через α', имеем

$$\alpha' = x - y\sqrt{D}, \quad (\alpha')' = \alpha.$$

Для того чтобы α было целым, необходимо и достаточно, чтобы целыми были $\alpha + \alpha'$ и $\alpha\alpha'$, т. е. $2x$ и $x^2 - Dy^2$. Так как, по предположению, D не делится ни на какой квадрат, то последнее может иметь место лишь, если у y, как и у x, знаменатель не превосходит 2. Положим $x = \frac{u}{2}$, $y = \frac{v}{2}$, где u и v — целые рациональные числа. Тогда должно удовлетворяться сравнение

$$u^2 - Dv^2 \equiv 0 \pmod 4.$$

Если $D \equiv 2$ или $3 \pmod 4$, то отсюда вытекает, так как квадрат может быть сравнимым лишь с 0 или 1 mod 4, что u и v оба четны и, значит, x и y — целые. Если же $D \equiv 1 \pmod 4$, то получаем $u \equiv v \pmod 2$. Таким образом α будет целым числом, если

а) при $D \equiv 2, 3 \pmod 4$: $\alpha = x + y\sqrt{D}$, x и y — целые;

базисом $K(\sqrt{D})$ служит 1, $\sqrt{D}$; дискриминант $d = 4D$;

б) при $D \equiv 1 \pmod 4$: $\alpha = g + v\frac{1+\sqrt{D}}{2}$, $g = \frac{u-v}{2}$ и v — целые;

базисом $K(\sqrt{D})$ служит 1, $\frac{1+\sqrt{D}}{2}$; дискриминант $d = D$. Очевидно, в обоих случаях в качестве базиса можно взять

$$1, \frac{d+\sqrt{d}}{2},$$

где d — дискриминант поля. Действительно, оба эти числа целые и их дискриминант равен d.

Докажем теперь следующую теорему разложения:

Теорема 89. *Пусть p — рациональное простое число, не входящее в d. Если сравнение*

$$x^2 \equiv d \pmod{4p} \tag{45}$$

имеет целое рациональное решение x, то p разлагается в поле $k(\sqrt{d})$ в произведение двух различных простых идеалов $\mathfrak{p}$, $\mathfrak{p}'$. Если же это сравнение неразрешимо, то p есть простой идеал в $k(\sqrt{d})$.

В самом деле, если простое число p разложимо в поле $k(\sqrt{d})$, то, в силу теоремы 81, оно разлагается в произведение лишь двух простых идеалов $\mathfrak{p}$ и $\mathfrak{p}'$, каждый из которых имеет степень 1. Вследствие теоремы 85 и обобщения теоремы Ферма (43) каждое целое число из $k(\sqrt{d})$ сравнимо тогда с некоторым рациональным числом по модулю $\mathfrak{p}$, поэтому существует целое рациональное r, удовлетворяющее сравнению

$$r \equiv \frac{d+\sqrt{d}}{2} \pmod{\mathfrak{p}}.$$

Отсюда получаем

$$2r - d \equiv \sqrt{d} \pmod{2\mathfrak{p}},$$
$$(2r-d)^2 \equiv d \pmod{4\mathfrak{p}}.$$

Но это сравнение между рациональными числами справедливо тогда и по модулю $4p$. Следовательно, $x = 2r - d$ есть решение сравнения (45). Идеал

$$\mathfrak{a} = \left(p,\ r - \frac{d+\sqrt{d}}{2}\right),$$

очевидно, делится на $\mathfrak{p}$ и

$$\mathfrak{a}\mathfrak{a}' = \left(p^2,\ p\left(r - \frac{d+\sqrt{d}}{2}\right),\ p\left(r - \frac{d-\sqrt{d}}{2}\right),\ \frac{(2r-d)^2 - d}{4}\right) =$$
$$= (p)\left(p,\ r - \frac{d+\sqrt{d}}{2},\ r - \frac{d-\sqrt{d}}{2},\ \frac{(2r-d)^2-d}{4p}\right).$$

Но так как, по предположению, p не входит в d, то второй из этих идеальных множителей равен (1), ибо он содержит p и разность между третьим и вторым членами, т. е. $\sqrt{d}$, а значит, и пару взаимно простых чисел p, d. Отсюда получаем, наконец,

$$\mathfrak{p} = \left(p,\ r - \frac{d+\sqrt{d}}{2}\right),\quad \mathfrak{p}' = \left(p,\ r - \frac{d-\sqrt{d}}{2}\right).$$

Оба этих простых идеала различны и, значит, взаимно просты, ибо $(\mathfrak{p}, \mathfrak{p}')$ содержит пару взаимно простых чисел p, d.

Пусть теперь, обратно, x есть решение сравнения (45). Тогда, очевидно,

$$\omega = \frac{x+\sqrt{d}}{2}$$

есть целое число, число же $\frac{\omega}{p}$ — нецелое, так как $\left(\frac{\omega-\omega'}{p}\right)^2 = \frac{d}{p^2}$ нецелое. Поэтому число p, входящее в $\omega\omega'$, не входя ни в ω, ни в ω', не может порождать простой идеал и, следовательно, разлагается в $k(\sqrt{d})$ на два простых идеала, которые, в силу сказанного выше, различны между собой. Тем самым теорема полностью доказана.

Пусть теперь q — нечетный простой множитель дискриминанта d. Имеем

$$\mathfrak{q} = \left(q,\ \frac{d+\sqrt{d}}{2}\right) = \left(q,\ \frac{-d+\sqrt{d}}{2} + d\right) = \left(q,\ \frac{d-\sqrt{d}}{2}\right) = \mathfrak{q}',$$

$$\mathfrak{q}^2 = \mathfrak{q}\mathfrak{q}' = q\left(q,\ \frac{d+\sqrt{d}}{2},\ \frac{d-\sqrt{d}}{2},\ \frac{d(d-1)}{4q}\right).$$

$\frac{d(d-1)}{4q}$ наверное не делится на q, т. е. взаимно просто с q; поэтому второй идеальный множитель в правой части равен (1) и $\mathfrak{q}^2 = q$, так что $\mathfrak{q}$ есть единственный входящий в q простой идеал.

Наконец, если d четно, то также 2 есть квадрат некоторого простого идеала, а именно, квадрат идеала $\mathfrak{q}=(2, \sqrt{D})$ при $D\equiv 2 \pmod 4$ или квадрат идеала $\mathfrak{q}=(2, 1+\sqrt{D})$ при $D\equiv 3 \pmod 4$.

Замечая теперь, что так как $d\equiv 0$ или $1 \pmod 4$, то в силу § 14 разрешимость сравнения (45) для нечетного простого числа p равносильна разрешимости сравнения $y^2\equiv d \pmod p$, мы можем объединить полученные результаты в следующей теореме:

Теорема 90. *Если p — простое нечетное число, то в квадратичном поле с дискриминантом d*

p разлагается на два различных множителя первой степени, если $\left(\frac{d}{p}\right)=+1$;

p разлагается на два одинаковых множителя первой степени, если $\left(\frac{d}{p}\right)=0$;

p само есть простой идеал (второй степени), если $\left(\frac{d}{p}\right)=-1$.

Простое число 2 разлагается на два различных множителя, если d нечетно и является квадратичным вычетом $\bmod 8$; *2 есть само простой идеал, если d нечетно и является невычетом* $\bmod 8$; *2 есть квадрат при четном d.*

§ 30. Второй тип законов разложения для рациональных простых чисел: разложение в поле $K(e^{\frac{2\pi i}{m}})$

Мы исследуем теперь поле корней m-й степени из 1, где m — целое рациональное число >2. Корни m-й степени из 1 суть m корней уравнения $x^m-1=0$, следовательно, целые алгебраические числа.

Первообразными корнями m-й степени из 1 служат $\varphi(m)$ чисел $e^{\frac{2\pi i a}{m}}$, где $(a, m)=1$; они не являются корнями меньшей степени из 1.

Рассмотрим произведение

$$g(x)=\prod_{k=1}^{m-1}(x^k-1).$$

Корень полинома $g(x)$ тогда и только тогда будет корнем полинома $f(x)=x^m-1$, если он является непервообразным корнем m-й степени из 1. Следовательно,

$$F(x)=\frac{x^m-1}{d(x)}, \quad \text{где} \quad d(x)=(f(x), g(x)),$$

есть полином с целыми рациональными коэфициентами, имеющий корнями $\varphi(m)$ первообразных корней m-й степени из 1 и только их. Так как, наконец, среди первообразных корней m-й степени из 1 каждый есть степень любого другого, то поле $K(e^{\frac{2\pi i}{m}})$ есть поле Галуа, степень которого $h\leqslant\varphi(m)$. (То обстоятельство, что эта степень

в точности равна $\varphi(m)$ и, значит, $F(x)$ — неприводимый полином, — — в этом параграфе не будет использовано; оно будет получено как побочный результат из рассмотрений § 43.)

Положим $e^{\frac{2\pi i}{m}} = \zeta$ и заметим, что, как было выяснено при доказательстве теоремы 64, каждое целое число поля $K(\zeta)$ может быть единственным образом представлено в виде

$$\omega = r_0 + r_1\zeta + \ldots + r_{h-1}\zeta^{h-1},$$

где r_i — рациональные числа, знаменатели которых суть делители фиксированного целого числа D — дискриминанта $F(x)$.

Пусть теперь p — рациональное простое число, не входящее в D, и D' удовлетворяет сравнению $DD' \equiv 1 \pmod{p}$. Тогда в каждом классе вычетов $\bmod p$ в $K(\zeta)$ существуют числа, для которых все $r_0, r_1, \ldots, r_{h-1}$ целые рациональные, ибо для каждого целого ω имеем

$$\omega \equiv DD'\omega \pmod{p}$$

и $DD'r_i$, в силу сказанного выше, целые рациональные. Пользуясь этим обстоятельством, мы сможем при исследовании p обойтись без построения базиса поля.

Лемма. *Если простое число p не входит в Dm, то для каждого целого числа ω поля $K(\zeta)$ удовлетворяется сравнение*

$$\omega^{p^f} \equiv \omega \pmod{p},$$

где f — наименьший положительный показатель, для которого $p^f \equiv 1 \pmod{m}$.

Для доказательства примем, что ω есть то число в своем классе вычетов $\bmod p$, в представлении которого

$$\omega = a_0 + a_1\zeta + \ldots + a_{h-1}\zeta^{h-1}$$

все a_i целые рациональные. Тогда, как и при доказательстве формулы (44), для целочисленного в $k(1)$ полинома

$$Q(x) = a_0 + a_1x + \ldots + a_{h-1}x^{h-1}$$

удовлетворяется функциональное сравнение

$$Q(x)^p \equiv Q(x^p) \pmod{p}, \quad \text{вообще} \quad Q(x)^{p^f} \equiv Q(x^{p^f}) \pmod{p}.$$

Это функциальное сравнение при замене переменной x целым алгебраическим числом ζ дает верное числовое сравнение, которое и доказывает лемму.

Теорема 91. *Если простое число p не входит в Dm, то p не делится в $K(\zeta)$ на квадрат простого идеала.*

Действительно, пусть, в противоречие с утверждением теоремы, $\mathfrak{p}^2 \mid p$. Выберем целое число ω, делящееся на $\mathfrak{p}$, но не делящееся на $\mathfrak{p}^2$. В силу леммы, имеем тогда

$$\omega^{p^f} \equiv \omega \pmod{\mathfrak{p}^2},$$

откуда, так как $p^f \geqslant 2$ и поэтому $\omega^{p^f} \equiv 0 \pmod{\mathfrak{p}^2}$, получим

$$\omega \equiv 0 \pmod{\mathfrak{p}^2},$$

что противоречит предположению.

Теорема 92. *Если простое число p не входит в Dm и f есть наименьший положительный показатель, для которого $p^f \equiv 1 \pmod m$, то p разлагается в поле $K(\zeta)$ в произведение точно $e = \frac{h}{f}$ различных простых идеалов, каждый из которых имеет степень f.*

В самом деле, пусть $\mathfrak{p}$ — простой множитель p степени f_1. Тогда, согласно (43), для каждого целого числа ω поля $K(\zeta)$ имеет место сравнение

$$\omega^{p^{f_1}} \equiv \omega \pmod{\mathfrak{p}}, \tag{46}$$

причем это сравнение не будет уже выполняться для всех ω, если f_1 будет заменено меньшим числом. Поэтому, согласно лемме, $f_1 \leqslant f$. С другой стороны, полагая в (46) $\omega = \zeta$, получаем

$$\zeta^{p^{f_1}} \equiv \zeta \pmod{\mathfrak{p}}.$$

Но здесь должно быть $p^{f_1} \equiv 1 \pmod m$, ибо в противном случае $\zeta^{p^{f_1}}$ было бы отличным от ζ первообразным корнем m-й степени из 1, и тогда $\zeta^{p^{f_1}} - \zeta$, а следовательно, и $\mathfrak{p}$ входило бы множителем в дискриминант D полинома $F(x)$, в противоречие с предположением, что p не входит в D. Теперь, из $p^{f_1} \equiv 1 \pmod m$ и $f_1 \leqslant f$ вытекает, в силу определения показателя f, что $f_1 = f$.

Так как сопряженные простые идеалы, в силу теоремы 91, входят в p лишь в первой степени, то, согласно сделанному в § 29 замечанию, p распадается точно на $\frac{h}{f}$ множителей, что и завершает доказательство теоремы.

Этой теоремой устанавливается тесная связь поля $K(\zeta)$ с группой классов вычетов $\bmod m$ в поле $k(1)$. *Простые числа, принадлежащие одному и тому же классу вычетов* $\bmod m$, *разлагаются в $K(\zeta)$ одинаковым образом,* за конечным числом исключений. Позже, в § 43, мы покажем также, что поле $K(\zeta)$ имеет степень $\varphi(m)$, т. е. ту же степень, что и группа $\mathfrak{R}(m)$ в $k(1)$. Наконец, упомянем еще, что так называемая группа Галуа поля $K(\zeta)$ изоморфна группе $\mathfrak{R}(m)$.

Исходя из этих обстоятельств $K(\zeta)$ называют *полем классов,* соответствующим разбиению рациональных чисел на классы вычетов $\bmod m$.

Как известно из теории деления круга, $K(\zeta)$ содержит одно или несколько квадратичных полей и каждое квадратичное поле в свою очередь содержится в некотором $K(\zeta)$. Оказывается, что из законов разложения в $K(\zeta)$ можно вывести законы разложения для каждого его под-поля, и таким образом получается для квадратичных полей

закон разложения, совершенно отличный по форме от найденного в предыдущем параграфе. Сравнение обоих законов приводит тогда к доказательству сформулированного в § 16 *квадратичного закона взаимности* [1]).

§ 31. Дробные идеалы

Мы введем теперь дробные идеалы — системы чисел, которые могут содержать также нецелые числа поля, а если содержат лишь целые числа, то совпадают с рассматривавшимися до сих пор идеалами.

Систему S целых или дробных чисел поля мы будем, начиная с этого момента, называть идеалом, если

1) вместе с α и β к ней принадлежат также $\lambda\alpha + \mu\beta$ с произвольными целыми λ, μ из K;

2) существует отличное от 0 целое число ν такое, что произведение его на каждое число из S есть целое число.

Идеалы, содержащие лишь целые числа, мы будем называть *целыми* идеалами, остальные идеалы — *дробными* идеалами. Два идеала называются равными, если они содержат одни и те же числа.

Теорема 93. *Каждый идеал* $\mathfrak{g}$ *совпадает с совокупностью значений некоторой линейной формы*

$$\xi_1\rho_1 + \ldots + \xi_r\rho_r,$$

где $\rho_1, \ldots, \rho_r$ — *некоторые целые или дробные числа из* $\mathfrak{g}$, *а* ξ_i *пробегают все целые числа из* K. *Это мы запишем в виде*

$$\mathfrak{g} = (\rho_1, \ldots, \rho_r).$$

Действительно, если ν — число, обладающее свойством 2), то совокупность произведений числа ν на числа из $\mathfrak{g}$ образует, очевидно, целый идеал $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$, и тогда $\mathfrak{g} = \left(\frac{\alpha_1}{\nu}, \ldots, \frac{\alpha_r}{\nu}\right)$.

Если $\alpha_1, \ldots, \alpha_r$ — базис целого идеала $\mathfrak{a}$, то $\frac{\alpha_1}{\nu}, \ldots, \frac{\alpha_r}{\nu}$ есть, очевидно, базис идеала $\mathfrak{g}$, рассматриваемого как бесконечная абелева группа.

Произведение двух идеалов $\mathfrak{g} = (\gamma_1, \ldots, \gamma_r)$ и $\mathfrak{r} = (\rho_1, \ldots, \rho_s)$ определяется так же, как и в случае целых идеалов:

$$\mathfrak{g}\mathfrak{r} = (\ldots, \gamma_i\rho_k, \ldots),$$

причем это умножение также коммутативно и ассоциативно. Каждый идеал $\mathfrak{g} \neq (0)$ можно путем умножения на подходящие выбранный

---

[1]) Идея этого наиболее прозрачного доказательства квадратичного закона взаимности восходит к Кронекеру. См., например, изложение этого доказательства в гильбертовом отчете о теории алгебраических числовых полей, § 122. В настоящей книге это доказательство не приводится. Связь между обеими формами законов разложения видна в принципе уже при рассмотрении поля $K(\sqrt{-3})$ корней третьей степени из 1, где обе эти формы имеют место.

целый идеал (ν) превратить в целый идеал и, следовательно, также в главный идеал (ω).

Если $\mathfrak{g} \neq (0)$, *то из* $\mathfrak{g}\mathfrak{x} = \mathfrak{g}\mathfrak{y}$ *вытекает* $\mathfrak{x} = \mathfrak{y}$.

Доказывается дословно, как теорема 68.

Пусть $\mathfrak{g}_1$, $\mathfrak{g}_2$ — *произвольные идеалы, причем* $\mathfrak{g}_1 \neq (0)$. *Тогда существует точно один идеал* $\mathfrak{x}$, *обладающий тем свойством, что*

$$\mathfrak{g}_1\mathfrak{x} = \mathfrak{g}_2.$$

Пишут $\mathfrak{x} = \frac{\mathfrak{g}_1}{\mathfrak{g}_2}$ и называют $\mathfrak{x}$ *отношением* $\mathfrak{g}_2$ к $\mathfrak{g}_1$; это отношение имеет, следовательно, смысл лишь если $\mathfrak{g}_1 \neq (0)$.

Для доказательства сформулированного утверждения выберем $\mathfrak{a} \neq (0)$ так, чтобы $\mathfrak{a}\mathfrak{g}_1$ было главным идеалом, $\mathfrak{a}\mathfrak{g}_1 = (\omega)$ (так что $\omega \neq 0$); пусть при этом $\mathfrak{a}\mathfrak{g}_2 = (\rho_1, \ldots, \rho_r)$, и положим

$$\mathfrak{x} = \left(\frac{\rho_1}{\omega}, \ldots, \frac{\rho_r}{\omega}\right).$$

Тогда действительно $\mathfrak{a}\mathfrak{g}_2 = (\omega)\mathfrak{x} = \mathfrak{a}\mathfrak{g}_1\mathfrak{x}$ и $\mathfrak{g}_2 = \mathfrak{g}_1\mathfrak{x}$, причем, в силу предыдущего предложения, идеал $\mathfrak{x}$ определен однозначно.

Вследствие этого равенство $\frac{\mathfrak{a}}{\mathfrak{b}} = \frac{\mathfrak{c}}{\mathfrak{d}}$ совершенно равносильно равенству $\mathfrak{a}\mathfrak{d} = \mathfrak{b}\mathfrak{c}$, в частности, для каждого идеала $\mathfrak{m} \neq (0)$

$$\frac{\mathfrak{a}}{\mathfrak{b}} = \frac{\mathfrak{a}\mathfrak{m}}{\mathfrak{b}\mathfrak{m}}, \quad \frac{\mathfrak{a}}{(1)} = \mathfrak{a}, \quad \frac{\mathfrak{m}}{\mathfrak{m}} = (1).$$

Поэтому каждый идеал может быть представлен в виде отношения целых взаимно простых идеалов, которые мы, как и в случае обычных чисел, будем называть числителем и знаменателем. В частности, каждый дробный главный идеал ω может быть представлен в виде отношения целых идеалов:

$$\omega = \frac{\mathfrak{a}}{\mathfrak{b}}.$$

Также и для дробных идеалов мы будем говорить о *делимости*: „$\mathfrak{a} \mid \mathfrak{b}$“ или „$\mathfrak{b}$ делится на $\mathfrak{a}$“ будет означать, что $\mathfrak{b} \mid \mathfrak{a}$ — целый идеал. Если $\mathfrak{a}$ и $\mathfrak{b}$ — целые идеалы, то это определение совпадает с прежним определением делимости.

В силу этого определения число ω входит в идеал $\mathfrak{g}$ тогда и только тогда, когда (ω) делится на $\mathfrak{g}$, т. е. (ω) обладает разложением

$$(\omega) = \mathfrak{m}\mathfrak{g},$$

где $\mathfrak{m}$ — целый идеал. Таким образом число 1 входит во все те и только те идеалы, которые являются обратными к целому идеалу $\mathfrak{a}$, т. е. равны $\frac{(1)}{\mathfrak{a}}$.

Пусть $\mathfrak{g} = \frac{\mathfrak{a}}{\mathfrak{b}}$, где $\mathfrak{a}$, $\mathfrak{b}$ — взаимно простые идеалы. Норма идеала $\mathfrak{g}$ определяется тогда следующим образом:

$$N(\mathfrak{g}) = \frac{N(\mathfrak{a})}{N(\mathfrak{b})}.$$

Это равенство сохраняет силу и в том случае, когда $\mathfrak{a}$, $\mathfrak{b}$ не взаимно просты или даже являются дробными идеалами. Также и здесь

$$N(\mathfrak{g}_1\mathfrak{g}_2) = N(\mathfrak{g}_1)\,N(\mathfrak{g}_2).$$

Как и в случае целых идеалов, базис и норма связаны следующим соотношением:

Если $\alpha_1, \ldots, \alpha_n$ — *базис* $\mathfrak{g}$, *то*

$$N(\mathfrak{g}) = \left|\frac{\Delta(\alpha_1, \ldots, \alpha_n)}{\sqrt{d}}\right|. \tag{47}$$

Действительно, пусть целое число $\nu \neq 0$ выбрано так, чо $\nu\mathfrak{g}$ есть целый идеал $\mathfrak{b}$, и пусть $(\beta_1, \ldots, \beta_n)$ — базис $\mathfrak{b}$; тогда $\frac{\beta_1}{\nu}, \ldots, \frac{\beta_n}{\nu}$ есть базис $\mathfrak{g}$ и

$$N(\mathfrak{g}) = \frac{N(\mathfrak{b})}{N((\nu))} = \left|\frac{\Delta(\beta_1, \ldots, \beta_n)}{N(\nu)\sqrt{d}}\right| = \left|\frac{\Delta\left(\frac{\beta_1}{\nu}, \ldots, \frac{\beta_n}{\nu}\right)}{\sqrt{d}}\right|.$$

§ 32. Теорема Минковского о линейных формах

В дальнейшем развитии теории алгебраических чисел понятие величины снова начинает играть существенную роль, в отличие от предыдущего, когда все основывалось на понятии делимости и формальных алгебраических процессах. Важнейшим вспомогательным средством служит при этом одна теорема о разрешимости линейных неравенств в целых рациональных числах, восходящая к Дирихле и значительно расширенная и усиленная Минковским. Эта теорема, как и и ее доказательство, совершенно не зависит от предыдущих теорий. Она гласит следующее:

Теорема 94. *Пусть даны* n *линейных однородных выражений*

$$L_p(x) = \sum_{q=1}^{n} a_{pq}x_q \quad (p = 1, \ldots, n)$$

с вещественными коэфициентами a_{pq} *и определителем* $D = |a_{pq}|$, *отличным от нуля, и* n *положительных величин* $\varkappa_1, \ldots, \varkappa_n$, *удовлетворяющих условию*

$$\varkappa_1\varkappa_2 \ldots \varkappa_n \geqslant |D|.$$

Тогда всегда существуют n *целых рациональных чисел* $x_1, \ldots, x_n$, *не равных одновременно нулю, для которых выполняются неравенства*

$$|L_p(x)| \leqslant \varkappa_p \quad (p = 1, \ldots, n). \tag{48}$$

Эта теорема принадлежит разработанной Минковским геометрии чисел, и доказательство ее проводится геометрическим методом. Для доказательства теоремы мы изменяем постановку вопроса и спрашиваем, что следует для велечин $\varkappa$ из неразрешимости n неравенств (48)

в целых рациональных числах $x_q \neq 0$? Мы покажем, что в этом случае должно быть $\varkappa_1\varkappa_2\ldots\varkappa_n < |D|$.

Рассмотрим для этой цели в n-мерном пространстве с декартовыми координатами $x_1, \ldots, x_n$ параллелотоп

$$|L_p(x)| \leqslant \frac{\varkappa_p}{2} \quad (p = 1, \ldots, n)$$

и представим себе его последовательно параллельно смещенным так, чтобы его центр $(0, \ldots, 0)$ попал в каждую целую точку $(g_1, \ldots, g_n)$ (g_i независимо друг от друга пробегают все целые рациональные значения). Мы будем иметь тогда бесконечное множество параллелотопов $\Pi_{g_1,\ldots,g_n}$:

$$|L_p(x-g)| \leqslant \frac{\varkappa_p}{2} \quad (p = 1, \ldots, n).$$

Если неравенства (48) неразрешимы, то никакие два из этих параллелотопов не смогут иметь общей точки. В самом деле, если бы некоторая точка (x) принадлежала обоим параллелотопам $\Pi_{g_1,\ldots,g_n}$ и $\Pi_{g_1',\ldots,g_n'}$, то из неравенств

$$-\frac{\varkappa_p}{2} \leqslant L_p(x-g) \leqslant \frac{\varkappa_p}{2}$$

и

$$-\frac{\varkappa_p}{2} \leqslant L_p(x-g') \leqslant \frac{\varkappa_p}{2}$$

мы получили бы путем вычитания

$$|L_p(g-g')| \leqslant \varkappa_p,$$

т. е. неравенства (48) имели бы решение $x_q = g_q - g_q'$.

Вследствие этого сумма объемов всех Π, содержащихся в некотором определенном кубе $|x_q| \leqslant L$ $(q = 1, \ldots, n)$, будет меньше объема $(2L)^n$ этого куба. А отсюда, как мы сейчас покажем, уже вытекает наше утверждение. В самом деле, пусть c — некоторое число, удовлетворяющее тому условию, что координаты всех точек исходной фигуры $\Pi_{0,\ldots,0}$ не превосходят его по абсолютной величине. Тогда те $\Pi_{g_1,\ldots,g_n}$, для которых

$$|g_q| \leqslant L \quad (q = 1, \ldots, n),$$

во всяком случае содержатся в кубе $|x_q| \leqslant L + c$, ибо из $|L_q(x-g)| \leqslant \frac{\varkappa_p}{2}$ и $|g_q| \leqslant L$ следует $|x_q| = |x_q - g_q + g_q| \leqslant |x_q - g_q| + |g_q| \leqslant c + L$. Пусть L — целое положительное рациональное число, тогда существует $(2L+1)^n$ параллелотопов $\Pi_{g_1,\ldots,g_n}$, центры которых лежат в кубе $|g_q| \leqslant L$, и для их совокупного объема $(2L+1)^n J$, где J — объем каждого отдельного Π, в силу только что сказанного, должно иметь место неравенство

$$(2L+1)^n J < (2L+2c)^n.$$

Деля на L^n, беря $L \to \infty$ и переходя к пределу, получаем

$$J \leqslant 1.$$

Но, с другой стороны,

$$J = \int\limits_{|L_p(x)| \leqslant \frac{\varkappa_p}{2}} \dots \int dx_1 \dots dx_n = \frac{1}{|D|} \int\limits_{|y_p| \leqslant \frac{\varkappa_p}{2}} \dots \int dy_1 \dots dy_n = \frac{\varkappa_1 \varkappa_2 \dots \varkappa_n}{|D|}.$$

Таким образом, если неравенства (48) неразрешимы в целых числах, не равных одновременно нулю, то $\varkappa_1 \varkappa_2 \dots \varkappa_n \leqslant |D|$. При этом здесь необходимо должен стоять знак $<$; действительно, из неразрешимости неравенств (48) для данных значений $\varkappa_1, \dots, \varkappa_n$ вытекает по непрерывности также неразрешимость для достаточно близких бо́льших значений $\varkappa$, произведение которых, по доказанному, тоже должно быть $\leqslant |D|$, так что произведение прежних значений $\varkappa$ необходимо $< |D|$.

Но тем самым доказано, что если произведение величин $\varkappa$ равно или превосходит $|D|$, то неравенства (48) должны иметь решение в целых числах.

Будем теперь рассматривать линейные формы $L_p(x)$ с комплексными коэфициентами. Комплексно сопряженными мы будем называть линейные формы, у которых все соответственные коэфициенты суть комплексно сопряженные числа. Путем нетрудного видоизменения предыдущей теоремы получается

Теорема 95. *Пусть даны n линейных форм $L_p(x) = \sum\limits_{q=1}^{n} a_{pq} x_q$ $(p = 1, \dots, n)$ с вещественными или комплексными коэфициентами и определителем $D \neq 0$. Пусть при этом наряду с каждой невещественной формой среди данных n форм всегда находится и комплексно сопряженная с ней. Наконец, пусть $\varkappa_1, \dots, \varkappa_n$ — положительные величины, причем $\varkappa_\alpha = \varkappa_\beta$, если формы $L_\alpha(x)$ и $L_\beta(x)$ — комплексно сопряженные. Если тогда*

$$\varkappa_1 \varkappa_2 \dots \varkappa_n \geqslant |D|,$$

то существуют такие целые рациональные x_q, не обращающиеся одновременно в нуль, что

$$|L_p(x)| \leqslant \varkappa_p \quad (p = 1, \dots, n).$$

Для доказательства заменим систему форм $L_p(x)$ системой вещественных форм $L'(x)$, получающейся следующим образом: если $L_p(x)$ — вещественная форма, то полагаем $L'_p(x) = L_p(x)$; если $L_\alpha(x)$ и $L_\beta(x)$ — комплексно сопряженные формы и, скажем, $\alpha < \beta$, то полагаем

$$L'_\alpha(x) = \frac{L_\alpha(x) + L_\beta(x)}{2}, \quad L'_\beta(x) = \frac{L_\alpha(x) - L_\beta(x)}{2i}.$$

Одновременно положим $\varkappa'_p = \varkappa_p$ в первом случае и

$$\varkappa'_\alpha = \varkappa'_\beta = \frac{\varkappa_\alpha}{\sqrt{2}}$$

— во втором. Определитель D' системы вещественных форм L', очевидно, связан с определителем D системы форм D равенством

$$|D'| = 2^{-r_2}|D|,$$

где r_2 означает количество пар комплексно сопряженных среди форм $L_p(x)$. Так как, таким образом, $\varkappa'_1\varkappa'_2\ldots\varkappa'_n \geqslant |D'|$, то, в силу теоремы 94, существуют целые рациональные числа x_q, не равные одновременно нулю, для которых

$$|L'_p(x)| \leqslant \varkappa'_p \quad (p = 1, \ldots, n).$$

Тем самым теорема доказана, ибо для каждой невещественной формы $L_\alpha(x)$ выполняется неравенство

$$|L_\alpha(x)|^2 = L'^2_\alpha(x) + L'^2_\beta(x) \leqslant \varkappa'^2_\alpha + \varkappa'^2_\beta = \varkappa^2_\alpha.$$

§ 33. Классы идеалов и группы классов. Идеальные числа

Мы теперь в состоянии приступить к решению проблемы, поставленной в § 23 в начале построения теории идеалов, а именно, исследовать, можно ли всякий идеал представить некоторым алгебраическим числом (принадлежащим, возможно, другому полю). Для этой цели мы введем понятие эквивалентности идеалов поля K и, значит, соответствующее разбиение всех идеалов этого поля на классы.

Определение. Два целых или дробных идеала $\mathfrak{a}$, $\mathfrak{b}$ называются *эквивалентными*, в обозначениях:

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

если они отличаются лишь множителем, являющимся главным идеалом, т. е. если существует такой (целый или дробный) главный идеал $(\omega) \neq (0)$, что

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

Введенное здесь понятие эквивалентности, очевидно, обладает следующими тремя свойствами, обязательными для всякого понятия эквивалентности:

1. $\mathfrak{a} \sim \mathfrak{a}$.
2. Из $\mathfrak{a} \sim \mathfrak{b}$ вытекает $\mathfrak{b} \sim \mathfrak{a}$.
3. Из $\mathfrak{a} \sim \mathfrak{b}$ и $\mathfrak{b} \sim \mathfrak{c}$ вытекает $\mathfrak{a} \sim \mathfrak{c}$.

Кроме того:

4. Из $\mathfrak{a} \sim \mathfrak{b}$ вытекает $\mathfrak{ac} \sim \mathfrak{bc}$, а в случае $\mathfrak{c} \neq (0)$ — и обратно.

Совокупность всех идеалов, эквивалентных некоторому определенному идеалу $\mathfrak{a}$, образует *класс идеалов*. В частности, все главные идеалы ($\neq (0)$) эквивалентны друг другу. Они образуют *главный класс*.

Эти классы, в силу свойства 4, можно объединить в абелеву группу. Именно, для любых идеалов $\mathfrak{a}$, $\mathfrak{b}$, принадлежащих соответственно классам A, B, произведение $\mathfrak{ab}$, в силу свойства 4, принадлежит одному и тому же классу C, который, таким образом, определяется единственно классами A, B, независимо от выбора в них идеалов $\mathfrak{a}$ и $\mathfrak{b}$. Мы обозначаем класс, которому принадлежит $\mathfrak{ab}$, через AB и тем самым определяем некоторую композицию классов идеалов, относительно которой они образуют (конечную или бесконечную) абелеву группу — *группу классов поля* K. При этом единичным элементом служит главный класс.

Переход от идеалов к классам идеалов в точности соответствует переходу от чисел к классам вычетов по некоторому модулю. В самом деле, совокупность целых и дробных идеалов поля K, отличных от (0), образует, очевидно, если в качестве композиции рассматривать обыкновенное умножение, бесконечную абелеву группу (имеющую бесконечный базис, а именно, совокупность всех простых идеалов). Эта группа $\mathfrak{M}$ содержит в качестве подгруппы группу $\mathfrak{H}$ всех главных идеалов ($\neq (0)$). А определенная выше *группа классов есть, очевидно, факторгруппа* $\mathfrak{M}/\mathfrak{H}$, поскольку ее элементами служат различные смежные классы группы $\mathfrak{H}$, состоящие из идеалов, отличающихся друг от друга только множителем, содержащимся в $\mathfrak{H}$, т. е. главным идеалом.

Одной из основных проблем высшей арифметики является подробное исследование структуры группы классов, которая играет существенную роль почти во всех предложениях о числах поля K. Однако наши познания о структуре общих полей чрезвычайно бедны. Важнейшее из известных здесь общих предложений выражается следующей теоремой:

Теорема 96. *В каждом классе идеалов поля K содержится целый идеал, норма которого не превосходит $|\sqrt{d}|$, где d — дискриминант поля. Поэтому число классов идеалов поля K конечно.*

Действительно, пусть $\mathfrak{a}$ — целый идеал из класса B^{-1}, где B — произвольно заданный класс. Пусть $\alpha_1, \ldots, \alpha_n$ — базис $\mathfrak{a}$. Тогда, в силу теоремы 95, существуют такие целые рациональные $x_1, \ldots, x_n$, не равные одновременно нулю, что

$$|\omega^{(i)}| = \left|\sum_{k=1}^{n} \alpha_k^{(i)} x_k\right| \leqslant \left|\sqrt[n]{\Delta}\right| \quad (i = 1, \ldots, n),$$

где $\Delta = \Delta(\alpha_1, \ldots, \alpha_n)$ — определитель системы $\alpha_k^{(i)}$. Поэтому для произведения всех этих сопряженных $\omega^{(i)}$ имеем

$$|N(\omega)| \leqslant |\Delta| = N(\mathfrak{a})\,|\sqrt{d}|. \tag{49}$$

Но, по своему определению, ω есть отличное от нуля целое число, делящееся на $\mathfrak{a}$, т. е.

$$\omega = \mathfrak{a}\mathfrak{b},$$

где $\mathfrak{b}$ — некоторый отличный от нуля целый идеал, очевидно лежащий в обратном к B^{-1} классе B, ибо $\mathfrak{a}\mathfrak{b} \sim (1)$. Из (49) получаем тогда

$$N(\mathfrak{b}) \leqslant |\sqrt{d}|, \tag{50}$$

чем первая часть теоремы доказана.

Но существует лишь конечное множество целых идеалов, нормы которых имеют заданное значение z, ибо, в силу (42) (§ 27), эти идеалы являются делителями идеала (z). Следовательно, существует также лишь конечное множество целых идеалов, нормы которых не превосходят некоторого данного числа, ибо нормы суть целые рациональные числа. Таким образом существует лишь конечное множество целых идеалов $\mathfrak{b}$, удовлетворяющих условию (50), а так как, с другой стороны, по доказанному, такой идеал $\mathfrak{b}$ находится в каждом классе, то число различных классов идеалов поля K конечно.

Это *число классов* мы будем обозначать в дальнейшем через h. В качестве непосредственного следствия конечности h мы получаем из теоремы 21 следующее предложение:

Теорема 97. *h-я степень каждого идеала в K является главным идеалом.*

Вместе с тем мы можем, наконец, доказать высказанное в § 24 утверждение:

Теорема 98. *Для каждого идеала $\mathfrak{a}$ из K существует число* A, *вообще говоря не принадлежащее полю K, обладающее тем свойством, что числа идеала $\mathfrak{a}$ совпадают с теми числами поля K, которые делятся на* A.

В самом деле, по теореме 97 $\mathfrak{a}^h$ равно некоторому главному идеалу (ω). Тогда число $\mathrm{A} = \sqrt[h]{\omega}$ обладает требуемым свойством. Действительно, если α — число из $\mathfrak{a}$, то α^h содержится в $\mathfrak{a}^h$, значит, $\frac{\alpha^h}{\omega}$ есть целое число и, следовательно, также $\frac{\alpha}{\sqrt[h]{\omega}} = \frac{\alpha}{\mathrm{A}}$ — целое.

Обратно, если α — такое число поля K, что $\frac{\alpha}{\mathrm{A}}$ — целое, то также $\frac{\alpha^h}{\omega}$ — целое, т. е. $\frac{\alpha^h}{\mathfrak{a}^h}$ есть целый идеал; в силу основной теоремы теории идеалов, тогда и $\frac{\alpha}{\mathfrak{a}}$ есть целый идеал, т. е. α входит в $\mathfrak{a}$.

Числа A, необходимые для представления всех идеалов поля K, мы можем теперь, в силу группового свойства классов идеалов, выбрать так, чтобы они все принадлежали некоторому полю над K относительной степени h, а именно, следующим образом.

В случае $h > 1$ группа классов, как конечная абелева группа, обладает базисом, скажем состоящим из классов $B_1, \ldots, B_m$ соответственно порядков $c_1, \ldots, c_m$. Выберем из каждого базисного класса по идеалу $\mathfrak{b}_q$ $(q = 1, \ldots, m)$. Тогда по определению базиса каждый идеал $\mathfrak{a}$ поля K будет эквивалентен в точности одному произведению степеней

$$\mathfrak{b}_1^{x_1} \ldots \mathfrak{b}_m^{x_m} \quad (0 \leqslant x_q < c_q,\ q = 1, \ldots, m). \tag{51}$$

Иными словами, мы получим каждый (целый или дробный) идеал $\mathfrak{g}$ точно один раз, заставляя в

$$\mathfrak{g} = \rho \mathfrak{b}_1^{x_1} \ldots \mathfrak{b}_m^{x_m} \tag{52}$$

число ρ пробегать все неассоциированные числа поля, а числа x_q — независимо друг от друга все целые рациональные числа в пределах $0 \leqslant x_q < c_q$. Если поэтому мы для каждого $\mathfrak{b}_q$ определим по теореме 98 число B_q:

$$\mathrm{B}_q = \sqrt[c_q]{\beta_q}, \quad \mathfrak{b}_q^{c_q} = (\beta_q),$$

то каждому $\mathfrak{g}$ вида (52) будет соответствовать число

$$\Gamma = \rho \mathrm{B}_1^{x_1} \ldots \mathrm{B}_m^{x_m}, \tag{53}$$

обладающее, очевидно, тем свойством, что $\mathfrak{g}$ совпадает с совокупностью чисел поля, делящихся на это Γ. Заставляя в выражении (53) число ρ пробегать все числа поля, т. е. также и ассоциированные, а числа x_q — указанные выше значения, мы получим систему чисел, называемую *системой идельных чисел поля* K. Она распадается, соответственно классам идеалов, на h классов идеальных чисел. Каждый класс в отдельности содержит числа (53) с совпадающими системами показателей x_q, и совокупность чисел одного и того же класса (включая и 0) воспроизводится при сложении и вычитании, совокупность же всех идеальных чисел, отличных от нуля, воспроизводится при умножении и делении. В этой системе каждый идеал из K представим в смысле теоремы 98 настоящим числом.

Это представление оказалось особенно важным в новейших исследованиях по аналитической теории чисел. Отметим еще, что поле $K(\mathrm{B}_1, \ldots, \mathrm{B}_m)$, имеющее степень h относительно K, вообще говоря, не тождественно так называемому гильбертову полю классов.

§ 34. Единицы. Верхняя граница для числа основных единиц

Целью этого и следующего параграфов является доказательство формулируемой ниже фундаментальной теоремы Дирихле, описывающей структуру группы единиц, содержащихся в поле K. Существование, вообще говоря, бесконечного множества единиц является вторым, наряду с необходимостью введения понятия идеала, существенным признаком, отличающим алгебраические поля высших степеней от поля рациональных чисел.

Прежде всего совокупность всех единиц поля K образует, очевидно, абелеву группу относительно умножения. Обозначим эту группу через $\mathfrak{E}$. Она содержит в качестве подгруппы группу $\mathfrak{W}$ всех корней из 1, лежащих в K, насчитывающую по меньшей мере два элемента, именно ± 1.

Лемма а). *В поле K имеется не более конечного числа целых чисел, которые вместе со всеми своими сопряженными не превосходят по абсолютной величине данной константы. Если все сопряженные некоторого целого числа поля K имеют абсолютную величину 1, то это число есть корень из 1.*

В самом деле, если для целого числа α из K имеют место неравенства $|\alpha^{(i)}| \leqslant C$, $i = 1, \ldots, n$, то отсюда для элементарных симметрических функций чисел $\alpha^{(i)}$ получаются оценки, зависящие только от C и n. Но эти функции имеют целые рациональные значения и суть коэфициенты уравнения n-й степени с корнями $\alpha^{(i)}$; следовательно, для значений этих коэфициентов имеется лишь конечное число возможностей и, значит, существует лишь конечное число уравнений n-й степени, все корни которых являются целыми числами, не превосходящими по абсолютной величине C.

Далее, если α — целое число из K и $|\alpha^{(i)}| = 1$, $i = 1, \ldots, n$, то то же справедливо и для всего бесконечного множества степеней α^q ($q = 1, 2, \ldots$). В силу только что доказанного эти степени не могут быть тогда все различными, т. е. для некоторой степени имеем $\alpha^q = 1$, значит, α — корень из 1.

Теорема 99. *Группа $\mathfrak{W}$ всех корней из 1, содержащихся в K, конечна и является циклической группой порядка $w \geqslant 2$.*

В самом деле, так как все корни из 1 со всеми их сопряженными имеют абсолютную величину 1, то первое утверждение следует из леммы а). Пусть, далее, p — простое число, входящее в порядок w группы $\mathfrak{W}$. Так как число решений уравнения $x^p = 1$ равно p^1, то по теореме 28 группа $\mathfrak{W}$ действительно циклическая.

Для дальнейшего исследования мы введем определенную нумерацию сопряженных полей $K^{(p)}$. Пусть ϑ — какое-либо производящее число поля K и пусть среди n его сопряженных числа $\vartheta^{(1)}, \vartheta^{(2)}, \ldots, \vartheta^{(r_1)}$ вещественны, а остальные $2r_2$ чисел невещественны, причем $\vartheta^{(p+r_2)}$ комплексно сопряженно с $\vartheta^{(p)}$, $p = r_1 + 1, \ldots, r_1 + r_2$. Согласно § 19, эта нумерация распространяется на все числа из K, причем тогда для каждого числа α из K

$$\begin{aligned} &\alpha^{(1)}, \ldots, \alpha^{(r_1)} \text{ вещественны,} \\ &|\alpha^{(p+r_2)}| = |\alpha^{(p)}|, \quad p = r_1 + 1, \ldots, r_1 + r_2. \end{aligned} \tag{54}$$

Положим, наконец,

$$\begin{aligned} e_p &= 1 \quad \text{для} \quad p = 1, \ldots, r_1, \\ e_p &= 2 \quad \text{для} \quad p = r_1 + 1, \ldots, n, \end{aligned}$$

так что

$$\sum_{p=1}^{r_1+r_2} e_p = n.$$

Нашей целью является доказательство следующей фундаментальной теоремы Дирихле:

ТЕОРЕМА 100. *Группа $\mathfrak{E}$ всех единиц поля K обладает конечным базисом. Этот базис содержит точно $r = r_1 + r_2 - 1$ элементов бесконечного порядка, тогда как остальные базисные элементы суть корни из 1.*

Это означает, таким образом, следующее:

Существует $r+1$ единиц $\zeta, \eta_1, \ldots, \eta_r$, где ζ — корень w-й степени из 1, таких, что, заставляя в форме

$$\varepsilon = \zeta^a \eta_1^{a_1} \ldots \eta_r^{a_r}$$

числа $a_1, \ldots, a_r$ пробегать независимо друг от друга все целые рациональные значения, а число a — лишь значения $0, 1, 2, \ldots, w-1$, мы получим каждую единицу поля точно один раз. r единиц $\eta_1, \ldots, \eta_r$ называются *основными единицами* поля.

Для подготовки доказательства, которым мы будем заниматься в этом и следующем параграфах, заметим, что k единиц $\varepsilon_1, \ldots, \varepsilon_k$ бесконечного порядка (т. е. не принадлежащих к $\mathfrak{W}$) являются независимыми в групповом смысле, если соотношение

$$\varepsilon_1^{a_1} \varepsilon_2^{a_2} \ldots \varepsilon_k^{a_k} = 1 \tag{55}$$

с целыми рациональными a имеет место лишь при $a_1 = \ldots = a_k = 0$. Но одновременно с соотношением (55) имеют место и аналогичные соотношения для сопряженных чисел, следовательно, также

$$|\varepsilon_1^{(i)}|^{a_1} |\varepsilon_2^{(i)}|^{a_2} \ldots |\varepsilon_k^{(i)}|^{a_k} = 1 \quad (i = 1, \ldots, n)$$

или

$$\sum_{m=1}^{k} a_m \ln |\varepsilon_m^{(i)}| = 0 \quad (i = 1, \ldots, n) \tag{56}$$

(где берутся вещественные ветви логарифмов). Обратно, из наличия соотношений (56) с целыми рациональными a для всех $i = 1, \ldots, n$ вытекает, в силу леммы а), что $\varepsilon_1, \ldots, \varepsilon_k$ не могут быть независимыми, так как тогда $\varepsilon_1^{a_1} \ldots \varepsilon_k^{a_k}$, являясь целым числом из K, все сопряженные которого имеют абсолютную величину 1, есть корень w-й степени из 1, так что $\varepsilon_1^{wa_1} \ldots \varepsilon_k^{wa_k} = 1$.

Но из выполнения r равенств

$$\sum_{m=1}^{k} \gamma_m \ln |\varepsilon_m^{(i)}| = 0 \quad \text{для} \quad i = 1, 2, \ldots, r_1 + r_2 - 1 \tag{57}$$

(с произвольными γ) уже вытекает выполнение этих равенств и для остальных индексов $i = r_1 + r_2, \ldots, n$. В самом деле, так как ε_m — единица, то

$$\sum_{p=1}^{r_1+r_2} e_p \ln |\varepsilon_m^{(p)}| = 0 \quad (m = 1, \ldots, k),$$

следовательно,

$$e_{r_1+r_2} \sum_{m=1}^{k} \gamma_m \ln |\varepsilon_m^{(r_1+r_2)}| = - \sum_{p=1}^{r_1+r_2-1} e_p \sum_{m=1}^{k} \gamma_m \ln |\varepsilon_m^{(p)}| = 0,$$

т. е. (57) выполняется также для $i = r_1 + r_2$ и, значит, в силу (54), для $i = 1, \ldots, n$. Следовательно, k единиц $\varepsilon_1, \ldots, \varepsilon_k$ тогда и только тогда являются независимыми, когда r линейных однородных уравнений с k неизвестными $\gamma_1, \ldots, \gamma_k$

$$\sum_{m=1}^{k} \gamma_m \ln |\varepsilon_m^{(i)}| = 0 \quad (i = 1, \ldots, r) \tag{58}$$

не имеют решений в целых рациональных γ, не равных одновременно нулю.

Верхняя граница для числа k независимых единиц дается теперь следующей леммой:

Лемма b). *Если между k единицами $\varepsilon_1, \ldots, \varepsilon_k$ имеют место соотношения* (58) *с какими-либо вещественными γ_m, не равными одновременно нулю, то такие же соотношения всегда имеют место и с некоторыми целыми рациональными γ_m, не равными одновременно нулю.*

Очевидно, это предложение достаточно доказать для единиц, не являющихся корнями из 1. Пусть теперь q — такое число, что между единицами $\varepsilon_1, \ldots, \varepsilon_{q-1}$ может иметь место r соотношений

$$\sum_{m=1}^{q-1} \alpha_m \ln |\varepsilon_m^{(i)}| = 0 \quad (i = 1, \ldots, r)$$

лишь при $\alpha_1 = \ldots = \alpha_{q-1} = 0$, тогда как для q единиц $\varepsilon_1, \ldots, \varepsilon_q$ существует система соотношений

$$\sum_{m=1}^{q} \beta_m \ln |\varepsilon_m^{(i)}| = 0 \quad (i = 1, \ldots, r) \tag{59}$$

с вещественными $\beta_1, \ldots, \beta_q$, не равными одновременно нулю. Для $q = 1$ утверждение теоремы тривиально. Поэтому мы можем считать, что $2 \leqslant q \leqslant k$. В силу предположения относительно q тогда необходимо $\beta_q \neq 0$, так что $q - 1$ отношений $\frac{\beta_1}{\beta_q}, \ldots, \frac{\beta_{q-1}}{\beta_q}$ вполне определены. Лемма b) будет доказана, если мы покажем, что эти $q - 1$ отношений $\frac{\beta_m}{\beta_q}$ $(m = 1, 2, \ldots, q-1)$ суть рациональные числа.

Полагая

$$\frac{\beta_m}{\beta_q} = -\alpha_m \quad (m = 1, \ldots, q-1),$$

мы получаем n равенств

$$\ln|\varepsilon_q^{(i)}| = \sum_{m=1}^{q-1} \alpha_m \ln|\varepsilon_m^{(i)}| \quad (i = 1, \ldots, n). \tag{60}$$

Рассмотрим теперь все вообще единицы η, логарифмы абсолютных величин которых представимы в форме

$$\ln|\eta^{(i)}| = \sum_{m=1}^{q-1} \rho_m \ln|\varepsilon_m^{(i)}| \quad (i = 1, 2, \ldots, n) \tag{61}$$

с вещественными ρ_m. Если такое представление вообще возможно, то, в силу предположения относительно q, коэфициенты ρ_m однозначно определяются числом η. Но среди систем значений $\rho_1, \ldots, \rho_{q-1}$, для которых имеют место соотношения вида (61), существует лишь конечное число систем, все элементы которых по абсолютной величине меньше чем 1, ибо для соответствующих η имеем

$$|\ln|\eta^{(i)}|| \leqslant \sum_{m=1}^{q-1} |\ln|\varepsilon_m^{(i)}|| \quad (i = 1, \ldots, n),$$

а по лемме a) подобному условию может удовлетворять лишь конечное количество целых чисел поля. Пусть H — число различных систем $(\rho_1, \ldots, \rho_{q-1})$, где $|\rho_m| < 1$ $(m = 1, \ldots, q-1)$.

Множество всех систем $(\rho_1, \ldots, \rho_{q-1})$ вида (61) обладает тем свойством, что вместе с $(\rho_1, \ldots, \rho_{q-1})$ в это множество входят также все системы

$$(N\rho_1 - n_1, N\rho_2 - n_2, \ldots, N\rho_{q-1} - n_{q-1}),$$

где N, n_1, n_2, $\ldots$, n_{q-1} — произвольные целые рациональные числа. Но теперь для каждого N можно подобрать n_1, n_2, $\ldots$, n_{q-1} таким образом, чтобы для всех чисел $N\rho_m - n_m$ выполнялось неравенство $|N\rho_m - n_m| \leqslant \frac{1}{2}$. Если бы какое-либо ρ_m было иррациональным, то числа $N\rho_m - n_m$ имели бы различные значения для различных значений N и, таким образом, получилось бы бесконечное множество систем $(\rho_1, \ldots, \rho_{q-1})$, все элементы которых по абсолютной величине меньше 1, в противоречие с доказанным выше. Таким образом все ρ_m, а значит, и все α_m в (60), рациональны, и лемма b) доказана.

Из этой леммы непосредственно следует, что число k независимых единиц бесконечного порядка не превосходит r. В самом деле, при $k > r$ r линейных уравнений (58) относительно неизвестных $\gamma_1, \ldots, \gamma_k$ всегда имеют вещественные решения, не равные одновременно нулю, а тогда, в силу леммы b), они имеют и целые рациональные решения, т. е. единицы $\varepsilon_m^{(i)}$ $(i = 1, \ldots, k)$ зависимы.

Коэфициенты ρ_m в (61) не могут быть произвольными рациональными числами: существует такое целое рациональное $M \neq 0$, завися-

щее только от $\varepsilon_1, \ldots, \varepsilon_{q-1}$, но не от η, что все $M\rho_m$ суть целые рациональные числа. Действительно, пусть, например, ρ_1 представляется в виде несократимой дроби $\frac{a}{b}$ (a, b — целые рациональные, $b > 0$); тогда среди чисел $|N\rho_1 - n_1|$ имеется точно b различных и меньших чем 1, именно $0, \frac{1}{b}, \ldots, \frac{b-1}{b}$, и потому b не превосходит определенного выше числа H всех систем $(\rho_1, \ldots, \rho_{q-1})$ с $|\rho_m| < 1$ $(m = 1, \ldots, q-1)$. Таким образом $H!\rho_m$ — целое для всех m, и в качестве M мы можем взять $M = H!$ Тем самым доказана

Лемма c). *Если* $\varepsilon_1, \ldots, \varepsilon_k$ — *такие единицы, что* r *равенств*

$$\sum_{m=1}^{k} \gamma_m \ln |\varepsilon_m^{(i)}| = 0 \quad (i = 1, \ldots, r)$$

с вещественными γ_m *могут удовлетворяться лишь когда все* γ_m *равны нулю, то существует такое фиксированное целое рациональное* $M \neq 0$, *что* n *выражений*

$$\sum_{m=1}^{k} \rho_m \ln |\varepsilon_m^{(i)}|$$

лишь тогда могут представлять соответственно $\ln |\eta^{(i)}|$ $(i = 1, \ldots, n)$, *где* η — *единица поля* K, *когда все* $M\rho_m$ — *целые рациональные числа.*

Из леммы c) следует далее

Лемма d). *Группа* $\mathfrak{E}$ *всех единиц поля* K *имеет конечный базис, причем число* k *базисных элементов бесконечного порядка не превосходит* r.

В самом деле, пусть $\varepsilon_1, \ldots, \varepsilon_k$ суть k независимых единиц бесконечного порядка, причем всякие $k+1$ единиц бесконечного порядка уже зависимы. Тогда для каждой единицы η поля K имеем в силу лемм b) и c) систему равенств

$$\ln |\eta^{(i)}| = \sum_{m=1}^{k} \frac{g_m}{M} \ln |\varepsilon_m^{(i)}| \quad (i = 1, \ldots, n)$$

с целыми рациональными g_m и некоторым, одним и тем же для всех η, целым рациональным положительным M. Отсюда, в силу леммы a), имеем

$$\eta^M = \varepsilon_1^{g_1} \ldots \varepsilon_k^{g_k} \zeta,$$

где ζ есть некоторый корень из 1, лежащий в K, т. е. корень w-й степени из 1. Поэтому

$$\eta = \varepsilon_1^{\frac{g_1}{M}} \varepsilon_2^{\frac{g_2}{M}} \ldots \varepsilon_k^{\frac{g_k}{M}} \zeta_0^x,$$

где $\zeta_0 = e^{\frac{2\pi i}{M\omega}}$ и x — целое рациональное число. Рассмотрим теперь [1]) совокупность всех произведений степеней $k+1$ чисел

$$H_1 = \varepsilon_1^{\frac{1}{M}}, \ldots, \quad H_k = \varepsilon_k^{\frac{1}{M}}, \quad H_{k+1} = \zeta_0,$$

где взяты произвольные, но фиксированные значения корней. Совокупность этих произведений образует (смешанную) абелеву группу, с базисом $H_1, \ldots, H_k, H_{k+1}$. Как вытекает из сказанного выше, группа $\mathfrak{E}$ всех единиц поля K содержится в этой группе в качестве подгруппы и притом конечного индекса, так как M-я степень каждого элемента группы содержится в $\mathfrak{E}$. Поэтому, в силу теоремы 34, также $\mathfrak{E}$ имеет конечный базис, причем число базисных элементов бесконечного порядка в группе $\mathfrak{E}$ не превосходит k. Среди произведений степеней этих базисных элементов бесконечного порядка содержатся во всяком случае w-е степени всех единиц, в частности, $\varepsilon_1^w, \ldots, \varepsilon_k^w$, т. е. k независимых единиц, следовательно, число этих базисных элементов есть k. Но выше было показано, что $k \leqslant r$; тем самым лемма d) доказана.

§ 35. Теорема Дирихле о точном числе основных единиц

Для завершения доказательства теоремы 100 Дирихле мы должны еще показать, что число k в точности равно $r = r_1 + r_2 - 1$.

Так как $n = r_1 + 2r_2$, то $r = \frac{n + r_1}{2} - 1$, и, следовательно, r равно нулю лишь, если $n + r_1 = 2$, т. е. либо $n = 2$, $r_1 = 0$, либо $n = 1$, $r_1 = 1$, иначе говоря, r равно нулю только для мнимых квадратичных полей и поля рациональных чисел.

Лемма a). *Если $r = 0$, то группа $\mathfrak{E}$ совпадает с конечной группой $\mathfrak{W}$ корней из 1, лежащих в K.*

В самом деле, в мнимом квадратичном поле из $N(\varepsilon) = \pm 1$ вытекает сразу $\varepsilon^{(1)}\varepsilon^{(2)} = +1$, и так как $|\varepsilon^{(1)}| = |\varepsilon^{(2)}|$, то ε — единицы, равные по абсолютной величине 1, т. е. корни из 1.

Случай поля рациональных чисел тривиален.

Лемма b). *Если $r > 0$, то для каждой системы вещественных чисел $c_1, \ldots, c_r$, не равных одновременно нулю, существует такая единица ε, что*

$$L(\varepsilon) = c_1 \ln|\varepsilon^{(1)}| + \ldots + c_r \ln|\varepsilon^{(r)}| \neq 0.$$

Этот второй существенный пункт в ходе доказательства теоремы Дирихле основывается на теореме 95 Минковского.

---

[1]) Напомним, что аналогичный прием был применен нами в § 22 при доказательстве существования базиса поля.

Пусть $\varkappa_1, \ldots, \varkappa_n$ — такие n положительных величин, что

$$\varkappa_1 \ldots \varkappa_n = |\sqrt{d}|,$$

$$\varkappa_{p+r_2} = \varkappa_p \quad \text{для} \quad p = r_1 + 1, \ldots, r_1 + r_2,$$

где d — дискриминант поля. В силу теоремы 95 существует целое число α поля K, отличное от нуля (норма которого, следовательно, по абсолютной величине не меньше чем 1) и такое, что

$$|\alpha^{(i)}| \leqslant \varkappa_i \quad \text{для} \quad i = 1, 2, \ldots, n,$$

значит,

$$1 \leqslant |N(\alpha)| \leqslant |\sqrt{d}|.$$

Отсюда

$$|\alpha^{(i)}| \geqslant \frac{1}{|\alpha^{(1)}| \ldots |\alpha^{(i-1)}| |\alpha^{(i+1)}| \ldots |\alpha^{(n)}|} \geqslant \frac{\varkappa_i}{\varkappa_1 \ldots \varkappa_n} = \frac{\varkappa_i}{|\sqrt{d}|}.$$

(Это, между прочим, показывает, что $|d| > 1$, так как при $|d| = 1$ в этих неравенствах всюду должен был бы стоять знак равенства, тогда как $\varkappa_i$ — в достаточной степени произвольные числа.) Образованное для этого числа α выражение

$$L(\alpha) = \sum_{m=1}^{r} c_m \ln |\alpha^{(m)}|$$

удовлетворяет неравенству

$$\left| L(\alpha) - \sum_{m=1}^{r} c_m \ln \varkappa_m \right| \leqslant \sum_{m=1}^{r} |c_m| \ln |\sqrt{d}| < A,$$

где A можно считать не зависящим от α и величин $\varkappa$. Но среди $\varkappa_1, \ldots, \varkappa_n$ первые r величин $\varkappa_1, \ldots, \varkappa_r$ могут быть выбраны совершенно произвольно. Поэтому мы можем найти последовательность систем $\varkappa_1^{(h)}, \ldots, \varkappa_r^{(h)}$ $(h = 1, 2, \ldots)$, для которых

$$\sum_{m=1}^{r} c_m \ln \varkappa_m^{(h)} = 2Ah \quad (h = 1, 2, \ldots).$$

Для соответствующих α_h имеем

$$|L(\alpha_h) - 2Ah| < A,$$

$$A(2h-1) < L(\alpha_h) < A(2h+1),$$

и, значит,

$$L(\alpha_1) < L(\alpha_2) < L(\alpha_3) < \ldots, \tag{62}$$

причем одновременно

$$|N(\alpha_h)| \leqslant |\sqrt{d}|.$$

Но главные идеалы (α_h), число которых бесконечно, а нормы не превосходят $|\sqrt{d}|$, не могут быть все различны между собой. Поэтому для некоторых двух различных индексов h и m будет выполняться равенство

$$(\alpha_h) = (\alpha_m), \quad \text{следовательно,} \quad \alpha_m = \varepsilon \alpha_h,$$

где ε — некоторая единица поля K. Таким образом мы имеем

$$L(\alpha_h) \neq L(\alpha_m) = L(\varepsilon\alpha_h),$$

$$L(\varepsilon) = L(\varepsilon\alpha_h) - L(\alpha_h) \neq 0,$$

чем лемма b) доказана. Из нее вытекает

Лемма c). *Если $r > 0$, то число k независимых единиц бесконечного порядка поля K точно равно r.*

Действительно, в силу леммы b) существует единица ε_1, для которой

$$\ln|\varepsilon_1^{(1)}| \neq 0.$$

Если при этом $r > 1$, то существует точно так же единица ε_2, для которой

$$\begin{vmatrix} \ln|\varepsilon_1^{(1)}| & \ln|\varepsilon_2^{(1)}| \\ \ln|\varepsilon_1^{(2)}| & \ln|\varepsilon_2^{(2)}| \end{vmatrix} \neq 0,$$

и т. д. Таким образом мы заключаем из леммы b), что существуют r единиц $\varepsilon_1, \ldots, \varepsilon_r$, для которых

$$\begin{vmatrix} \ln|\varepsilon_1^{(1)}| & \ldots & \ln|\varepsilon_r^{(1)}| \\ \ln|\varepsilon_1^{(2)}| & \ldots & \ln|\varepsilon_r^{(2)}| \\ \ldots & \ldots & \ldots \\ \ln|\varepsilon_1^{(r)}| & \ldots & \ln|\varepsilon_r^{(r)}| \end{vmatrix} \neq 0.$$

Из необращения этого определителя в нуль вытекает, что ни одна из единиц $\varepsilon_1, \ldots, \varepsilon_r$ не есть корень из 1 и что r линейных однородных уравнений относительно $\gamma_1, \ldots, \gamma_r$:

$$\sum_{m=1}^{r} \gamma_m \ln|\varepsilon_m^{(i)}| = 0 \quad (i = 1, \ldots, r),$$

имеют единственное решение $\gamma_1 = \gamma_2 = \ldots = \gamma_r = 0$. Тем самым, в силу доказанного в предыдущем параграфе, число k независимых единиц бесконечного порядка в точности равно r; в соединении с леммой d) предыдущего параграфа это завершает доказательство теоремы Дирихле о единицах поля.

В силу теоремы 38 (§ 11) две системы основных единиц поля K: $\eta_1, \ldots, \eta_r$ и $\varepsilon_1, \ldots, \varepsilon_r$, связаны соотношениями

$$\eta_m = \zeta_m \varepsilon_1^{a_{m1}} \varepsilon_2^{a_{m2}} \ldots \varepsilon_r^{a_{mr}} \quad (m = 1, \ldots, r),$$

где ζ_m — корни из 1, а a_{mk} — целые рациональные числа с определителем ± 1. Поэтому абсолютная величина определителя

$$\begin{vmatrix} \ln|\eta_1^{(1)}| \dots \ln|\eta_r^{(1)}| \\ \dots\dots\dots\dots \\ \ln|\eta_1^{(r)}| \dots \ln|\eta_r^{(r)}| \end{vmatrix}$$

для всех систем $\eta_1, \dots, \eta_r$ основных единиц сохраняет одно и то же, отличное от нуля значение, являющееся, таким образом, константой поля.

Абсолютная величина R определителя

$$\begin{vmatrix} e_1 \ln|\eta_1^{(1)}| \dots e_1 \ln|\eta_r^{(1)}| \\ \dots\dots\dots\dots \\ e_r \ln|\eta_1^{(r)}| \dots e_r \ln|\eta_r^{(r)}| \end{vmatrix} = \pm R$$

называется *регулятором* R поля K.

§ 36. Дифференты и дискриминанты

В этом параграфе мы будем рассматривать более глубокие свойства дискриминанта d поля K. До сих пор d был определен формально, как определитель базиса поля; нашей целью будет теперь дать определение дискриминанта d, основывающееся на его внутренних свойствах; оно будет иметь и то преимущество, что его окажется возможным перенести на относительные поля (§ 38).

Мы определим прежде всего как *дифференту числа* $\alpha^{(p)}$ *в поле* $K^{(p)}$ число

$$\delta(\alpha^{(p)}) = \prod_{h \neq p} (\alpha^{(p)} - \alpha^{(h)}).$$

Очевидно,

$$\delta(\alpha) = F'(\alpha), \tag{63}$$

где $F(x)$ — полином n-й степени с рациональными коэфициентами и старшим коэфициентом 1, имеющий корнями n величин $\alpha^{(1)}, \dots, \alpha^{(n)}$. Поэтому $\delta(\alpha^{(p)})$ есть число поля $K^{(p)}$. В силу теоремы 54 оно обращается в нуль тогда и только тогда, когда степень α меньше, чем n. Для дискриминанта числа α мы имеем выражение

$$d(\alpha) = \prod_{n \geqslant i > k \geqslant 1} (\alpha^{(i)} - \alpha^{(k)})^2 = (-1)^{\frac{n(n-1)}{2}} N(\delta(\alpha)).$$

Пусть теперь задан произвольный идеал $\mathfrak{a} \neq 0$ поля K и $\alpha_1, \dots, \alpha_n$ — его базис.

Теорема 101. *Совокупность чисел* λ *поля* K, *обладающих тем свойством, что для каждого числа* α *из* $\mathfrak{a}$

$$\text{след } S(\lambda\alpha) = \sum_{p=1}^{n} \lambda^{(p)}\alpha^{(p)} \text{ есть целое число,} \tag{64}$$

образует идеал $\mathfrak{m}$. *При этом* $\mathfrak{m}\mathfrak{a}$ *есть не зависящий от* $\mathfrak{a}$, *определенный лишь полем* K, *идеал, являющийся обратным к некоторому целому идеалу* $\mathfrak{d}$. n *чисел* $\beta_1, \ldots, \beta_n$, *определенных вместе с их сопряженными уравнениями*

$$S(\beta_i\alpha_k) = e_{ik} \quad (i, k = 1, \ldots, n), \tag{65}$$

где $e_{ik} = 1$, *если* $i = k$, *и* $e_{ik} = 0$, *если* $i \neq k$, *образуют базис идеала* $\mathfrak{m}$.

Доказательство. Прежде всего, числа λ, обладающие свойством (64), не могут иметь, в приведенном виде, произвольно больших идеальных знаменателей. В самом деле, каждое λ удовлетворяет системе n уравнений

$$S(\lambda\alpha_k) = g_k \quad (k = 1, \ldots, n)$$

с некоторыми целыми рациональными g_k; из этих n линейных уравнений относительно $\lambda^{(1)}, \ldots, \lambda^{(n)}$ каждое $\lambda^{(i)}$ определяется как отношение двух определителей, причем знаменателем служит один и тот же для всех $\lambda^{(i)}$ определитель из $\alpha_k^{(i)}$, равный по абсолютной величине $N(\mathfrak{a})\,|\sqrt{d}|$, а числитель есть целочисленный полином относительно $\alpha_k^{(i)}$. Таким образом существует целое число ω, зависящее только от α, такое, что $\omega\lambda$ есть целое число. Далее, если λ_1 и λ_2 принадлежат рассматриваемой совокупности чисел λ, то для любых целых ξ_1, ξ_2 также

$$S((\lambda_1\xi_1 + \lambda_2\xi_2)\alpha) = S(\lambda_1\xi_1\alpha) + S(\lambda_2\xi_2\alpha)$$

есть целое число, ибо одновременно с α также $\xi_1\alpha$ и $\xi_2\alpha$ принадлежат идеалу $\mathfrak{a}$. Таким образом вместе с λ_1 и λ_2 в совокупности чисел λ содержится также $\lambda_1\xi_1 + \lambda_2\xi_2$. Следовательно, эта совокупность представляет собой (§ 31) идеал. Обозначим этот идеал, зависящий от $\mathfrak{a}$, через $\mathfrak{m} = \mathfrak{m}(\mathfrak{a})$. Нетрудно убедиться в том, что $\mathfrak{a}\mathfrak{m}(\mathfrak{a}) = \mathfrak{m}(1)$, т. е. не зависит от $\mathfrak{a}$. В самом деле, если λ принадлежит $\mathfrak{m}(\mathfrak{a})$, то для каждого целого ξ также $S(\lambda\alpha_k\xi)$ — целое, т. е. $\lambda\alpha_k$ принадлежит $\mathfrak{m}(1)$. Обратно, если μ принадлежит $\mathfrak{m}(1)$ и $\rho_1, \ldots, \rho_n$ — базис идеала $\frac{1}{\mathfrak{a}}$, то $\alpha\rho_k$ есть целое число и поэтому $S(\mu\rho_k\alpha)$ — целое, т. е. произведение μ на каждое число из $\frac{1}{\mathfrak{a}}$ принадлежит $\mathfrak{m}(\mathfrak{a})$ и, значит, μ принадлежит $\mathfrak{a}\mathfrak{m}(\mathfrak{a})$.

Далее, $\mathfrak{m}(1)$ является обратным к некоторому целому идеалу $\mathfrak{d}$, так как, очевидно, число 1 принадлежит $\mathfrak{m}(1)$. Таким образом

$$\mathfrak{m} = \mathfrak{m}(\mathfrak{a}) = \frac{1}{\mathfrak{a}\mathfrak{d}},$$

где $\mathfrak{d}$ — целый идеал, не зависящий от $\mathfrak{a}$.

Наконец, определим n^2 чисел $\beta_i^{(p)}$ однозначно разрешимыми уравнениями

$$\sum_{p=1}^{n} \beta_i^{(p)} \alpha_k^{(p)} = e_{ik} \quad (i, k = 1, \ldots, n). \tag{65}$$

Полагая, для λ, удовлетворяющего условию (64),

$$S(\lambda\alpha_k) = g_k \quad (k = 1, \ldots, n),$$

мы будем также для

$$\lambda_0 = g_1\beta_1 + \ldots + g_n\beta_n$$

иметь

$$S(\lambda_0\alpha_k) = g_k;$$

а в силу однозначной разрешимости системы уравнений $S(\lambda\alpha_k) = g_k$ мы получим тогда

$$\lambda = \lambda_0 = g_1\beta_1 + \ldots + g_n\beta_n.$$

Таким образом, чтобы убедиться в том, что числа $\beta_1, \ldots, \beta_n$ образуют базис идеала $\mathfrak{m}(\mathfrak{a})$, остается еще показать, что они принадлежат полю K. В последнем убеждаемся либо непосредственно из детерминантного представления решений уравнений (65), либо следующим образом: умножением на $\alpha_i^{(q)}$ и суммированием по i мы получаем из (65) равносильную систему уравнений

$$\sum_p \alpha_k^{(p)} \sum_i \beta_i^{(p)} \alpha_i^{(q)} = \sum_i e_{ik}\alpha_i^{(q)} = \alpha_k^{(q)} = \sum_p e_{pq}\alpha_k^{(p)},$$

откуда

$$\sum_i \beta_i^{(p)} \alpha_i^{(q)} = e_{pq}, \quad \sum_i \beta_i^{(p)} \sum_q \alpha_i^{(q)} \alpha_k^{(q)} = \sum_q e_{pq}\alpha_k^{(q)}$$

или

$$\sum_{i=1}^{n} \beta_i^{(p)} S(\alpha_i\alpha_k) = \alpha_k^{(p)};$$

так как здесь коэфициенты в левой части рациональны, то мы видим, что $\beta_i^{(p)}$ действительно суть числа из $K^{(p)}$. Тем самым доказательство теоремы 101 закончено.

Имея в виду последующее применение (в гл. VIII), мы отметим еще, в частности, следующее предложение:

Теорема 102. *Если* $\alpha_1, \ldots, \alpha_n$ — *базисные числа идеала* $\mathfrak{a}$, *то* n *систем чисел* $\beta_1^{(p)}, \ldots, \beta_n^{(p)}$ $(p = 1, \ldots, n)$, *определенные из уравнений* (65), *являются сопряженными в* K, *и числа* $\beta_1, \ldots, \beta_n$ *образуют базис идеала* $\frac{1}{\mathfrak{a}\mathfrak{d}}$.

Так как, в силу (65) и (47),

$$\Delta^2(\beta_1, \ldots, \beta_n) = \frac{1}{\Delta^2(\alpha_1, \ldots, \alpha_n)} = \frac{1}{dN^2(\mathfrak{a})},$$

а в силу (47) и равенства $\mathfrak{m}=\frac{1}{\mathfrak{ab}}$,

$$\Delta^2(\beta_1, \ldots, \beta_n)=N^2(\mathfrak{m})\,d=\frac{d}{N^2(\mathfrak{ab})}=\frac{d}{N^2(\mathfrak{a})\,N^2(\mathfrak{b})},$$

мы получаем следующую теорему:

Теорема 103. $N(\mathfrak{d})=|d|$.

Идеал $\mathfrak{d}$, определенный теоремой 101, называется *дифферентой* или *основным идеалом* поля K.

Для вывода фундаментального соотношения, связывающего эту дифференту поля K и определенные выше дифференты чисел из K, мы исследуем теперь совокупность чисел из K, представимых в виде

$$G(\vartheta)=a_0+a_1\vartheta+a_2\vartheta^2+\ldots+a_{n-1}\vartheta^{n-1},$$

с целыми рациональными a_i. Пусть ϑ — целое производящее число поля K. Совокупность чисел $G(\vartheta)$ с целыми рациональными a_i называется *числовым кольцом* или *областью целостности* и обозначается через $R(\vartheta)$. Числа этого кольца, во-первых, образуют модуль с n базисными элементами $1, \vartheta, \vartheta^2, \ldots, \vartheta^{n-1}$, во-вторых, воспроизводятся еще при умножении.

Лемма а). *Каждое число α поля K, для которого $\mathfrak{d}\alpha$ — целый идеал, представимо в форме*

$$\alpha=\frac{\rho}{F'(\vartheta)},$$

где ρ — некоторое число кольца $R(\vartheta)$ и $F'(\vartheta)$, как в (63), — дифферента числа ϑ.

Для доказательства рассмотрим полином относительно x

$$G(x)=\sum_{i=1}^{n}\alpha^{(i)}\frac{F(x)}{x-\vartheta^{(i)}}, \tag{66}$$

где

$$F(x)=\prod_{i=1}^{n}(x-\vartheta^{(i)})=c_0+c_1x+\ldots+c_{n-1}x^{n-1}+c_nx^n.$$

$G(x)$ есть полином с целыми рациональными коэфициентами. В самом деле,

$$\frac{F(x)}{x-\vartheta}=\frac{F(x)-F(\vartheta)}{x-\vartheta}=\sum_{h=1}^{n}c_h\sum_{0\leqslant r\leqslant h-1}x^r\vartheta^{h-r-1},$$

поэтому

$$G(x)=\sum_{h=1}^{n}c_h\sum_{0\leqslant r\leqslant h-1}x^rS(\alpha\vartheta^{h-r-1}),$$

и так как, по предположению, $\alpha\mathfrak{d}$ — целое, то, в обозначениях и в силу теоремы 101, идеал $\mathfrak{m}((\alpha))$ есть обратная величина целого

идеала, следовательно, содержит все целые числа поля, в частности, числа ϑ^{h-r-1}, и, значит, $S(\alpha\vartheta^{h-r-1})$ суть целые рациональные числа. Полагая в (66) $x=\vartheta$, мы получим

$$\alpha=\frac{G(\vartheta)}{F'(\vartheta)},$$

причем, по доказанному, $G(\vartheta)$ действительно есть число кольца. Тем самым лемма доказана.

Из нее вытекает, что для всякого α такого, что $\mathfrak{d}\alpha$ есть целый идеал, $F'(\vartheta)\alpha$ будет целым числом. Нетрудно видеть, что такое положение может иметь место лишь если $F'(\vartheta)$ делится на $\mathfrak{d}$. Таким образом $F'(\vartheta)$ допускает разложение

$$F'(\vartheta)=\mathfrak{d}\mathfrak{f}, \tag{67}$$

где $\mathfrak{f}$ есть целый идеал.

Лемма b). *Для каждого* ρ, *принадлежащего кольцу* $R(\vartheta)$, $S\left(\frac{\rho}{F'(\vartheta)}\right)$ *есть целое число.*

Очевидно, достаточно доказать это утверждение для $\rho=1, \vartheta, \ldots, \vartheta^{n-1}$; а для этих чисел оно непосредственно вытекает из так называемых эйлеровых формул

$$\sum_{i=1}^{n}\frac{\vartheta^{(i)k}}{F'(\vartheta^{(i)})}=\begin{cases}0 \text{ для } k=0,\ 1,\ 2,\ \ldots,\ n-2,\\ 1 \text{ для } k=n-1.\end{cases}$$

Для полноты изложения укажем, что эти формулы можно получить из интерполяционных формул Лагранжа

$$\sum_{i=1}^{n}\frac{\vartheta^{(i)k+1}}{F'(\vartheta^{(i)})}\frac{F(x)}{x-\vartheta^{(i)}}=\begin{cases}x^{k+1} & \text{для } k=0,\ 1,\ \ldots,\ n-2,\\ x^n-F(x) & \text{для } k=n-1,\end{cases}$$

полагая $x=0$) либо также путем разложения по степеням $\frac{1}{x}$ после деления на $F(x)$).

Теорема 104. *Все числа идеала* $\mathfrak{f}=\frac{F'(\vartheta)}{\mathfrak{d}}$ *принадлежат кольцу* $R(\vartheta)$, *и всякий идеал* $\mathfrak{a}$, *все числа которого принадлежат кольцу* $R(\vartheta)$, *делится на* .

Действительно, если $\omega\equiv 0 \pmod{\mathfrak{f}}$, то $\alpha=\frac{\omega}{F'(\vartheta)}$ имеет знаменатель $\mathfrak{d}$, и по лемме a) $\omega=\alpha F'(\vartheta)$ должно быть числом кольца $R(\vartheta)$, чем первое утверждение теоремы доказано.

Обратно, если все числа идеала $\mathfrak{a}$ принадлежат кольцу $R(\vartheta)$, то по лемме b) $S\left(\frac{\alpha}{F'(\vartheta)}\right)$ есть целое число для всех α из $\mathfrak{a}$. Следовательно, по теореме 101, $\frac{1}{F'(\vartheta)}$ есть число идеала $\mathfrak{m}(\mathfrak{a})=\frac{1}{\mathfrak{a}\mathfrak{d}}$, т. е. $F'(\vartheta)=\mathfrak{d}\mathfrak{f}$ делит $\mathfrak{a}\mathfrak{d}$ или $\mathfrak{f}\mid\mathfrak{a}$, чем доказано и второе утверждение.

Этой теоремой дается, таким образом, новое определение идеала $\mathfrak{f}$: $\mathfrak{f}$ есть наибольший общий делитель всех идеалов поля K, содержащих лишь числа кольца $R(\vartheta)$. $\mathfrak{f}$ называется *ведущим идеалом* кольца.

Лемма c). *В поле K всегда существует кольцо $R(\vartheta)$, ведущий идеал которого $\mathfrak{f}$ не делится на произвольно заданный простой идеал $\mathfrak{p}$.*

Пусть, в самом деле, ω — целое число, делящееся на $\mathfrak{p}$, но не делящееся на $\mathfrak{p}^2$. Выражение

$$\gamma_0 + \gamma_1\omega + \gamma_2\omega^2 + \ldots + \gamma_h\omega^h \tag{68}$$

(где h — любое) представляет все классы вычетов $\bmod \mathfrak{p}^{h+1}$, когда $\gamma_0, \ldots, \gamma_h$ независимо друг от друга пробегают полные системы вычетов $\bmod \mathfrak{p}$. Пусть теперь ϑ — такое первообразное число $\bmod \mathfrak{p}$, что делящееся на $\mathfrak{p}$ число

$$\omega = \vartheta^{N(\mathfrak{p})} - \vartheta$$

(см. (43)) не делится на $\mathfrak{p}^2$. (Если ϑ не обладает этим свойством, то $\vartheta + \pi$, где π — произвольное число, делящееся на $\mathfrak{p}$, но не делящееся на $\mathfrak{p}^2$, очевидно, будет обладать этим свойством.) Смещением $\bmod \mathfrak{p}^2$ мы можем при этом добиться того, чтобы ϑ было отлично от всех своих сопряженных и, кроме того, удовлетворяло условию

$$\vartheta \equiv 0 \pmod{\mathfrak{a}}, \quad \mathfrak{a} = \frac{\mathfrak{p}}{\mathfrak{p}^e}, \quad (\mathfrak{a}, \mathfrak{p}) = 1, \tag{69}$$

где p — рациональное простое число, делящееся на $\mathfrak{p}$.

Придавая теперь числам γ_i в (68) независимо друг от друга $N(\mathfrak{p})$ несравнимых $\bmod \mathfrak{p}$ значений

$$0, \vartheta, \vartheta^2, \ldots, \vartheta^{N(\mathfrak{p})-1},$$

мы видим, что каждый класс вычетов $\bmod \mathfrak{p}^h$ может быть представлен числом кольца $R(\vartheta)$. Но тогда, при выполнении условия (69), ведущий идеал $\mathfrak{f}$ кольца не может делиться на $\mathfrak{p}$. В самом деле, пусть

$$N(\mathfrak{d}\mathfrak{f}) = p^k a, \quad (a, p) = 1;$$

по только что доказанному для каждого целого ω существует число ρ кольца такое, что

$$\pi = \omega - \rho \equiv 0 \pmod{\mathfrak{p}^{ek}}.$$

Теперь, число $\pi a \vartheta^k$ делится на $F'(\vartheta) = \mathfrak{d}\mathfrak{f}$, в чем убеждаемся, принимая во внимание (69), из разложения

$$\frac{\pi a \vartheta^k}{F'(\vartheta)} = \frac{\pi \vartheta^k N(\mathfrak{d}\mathfrak{f})}{\mathfrak{d}\mathfrak{f} \cdot p^k} = \frac{N(\mathfrak{d}\mathfrak{f})}{\mathfrak{d}\mathfrak{f}} \frac{\pi}{p^{ek}} \frac{\vartheta^k}{a^k}.$$

Следовательно, по лемме a),

$$\frac{\pi a \vartheta^k}{F'(\vartheta)} = \frac{\rho_1}{F'(\vartheta)},$$

где ρ_1 — число из $R(\vartheta)$, откуда

$$\pi = -\frac{\rho_1}{a\vartheta^k}.$$

Но тогда

$$a\vartheta^k\omega = a\vartheta^k(\rho + \pi) = a\vartheta^k\rho + \rho_1$$

также является числом кольца $R(\vartheta)$. Таким образом идеал $a\vartheta^k$ (не делящийся на $\mathfrak{p}$) содержит лишь числа кольца $R(\vartheta)$ и, значит, в силу теоремы 104, делится на $\mathfrak{f}$; тем самым и $\mathfrak{f}$ не делится на $\mathfrak{p}$.

Из леммы c) и формул (63) и (67) непосредственно вытекает основная теорема излагаемой теории:

Теорема 105. *Наибольший общий делитель диферент* $\delta(\vartheta)$ *всех целых чисел поля* K *равен диференте* $\mathfrak{d}$ *поля.*

Интересно, что, в противоположность диференте, дискриминант d поля, будучи общим делителем дискриминантов $d(\vartheta)$ всех целых чисел ϑ поля, не обязательно является их наибольшим общим делителем [1]).

§ 37. Относительные поля.

Связь между идеалами в различных полях

Мы обращаемся теперь к вопросу о том, какие изменения претерпевают развитые в течение предыдущего изложения понятия, если поле K рассматривается не относительно $k(1)$, а относительно произвольного алгебраического поля k, содержащегося в K. Разумеется, к k, как и к K, применима развитая выше теория идеалов. Возникает вопрос: можно ли установить связь между идеалами в K и в k?

Условимся элементы (числа или идеалы) из K обозначать большими буквами, а элементы из k — малыми. Пусть K имеет степень m относительно k (см. § 20, теорему 59), а степени K и k относительно поля рациональных чисел равны соответственно N и n, так что

$$N = nm.$$

Любые q чисел $\alpha_1, \ldots, \alpha_q$ из k определяют идеал $(\alpha_1, \ldots, \alpha_q)$ в k и идеал $(\alpha_1, \ldots, \alpha_q)$ в K, которые мы будем обозначать, для различия, через

$$\mathfrak{a} = (\alpha_1, \ldots, \alpha_q)_k \quad \text{и} \quad \mathfrak{A} = (\alpha_1, \ldots, \alpha_q)_K. \tag{70}$$

Число β, принадлежащее $\mathfrak{a}$, очевидно, принадлежит также $\mathfrak{A}$; но имеет место и обратное утверждение.

Лемма a). *Если* β *принадлежит идеалу* $\mathfrak{A} = (\alpha_1, \ldots, \alpha_q)_K$, *то* β *принадлежит также идеалу* $(\alpha_1, \ldots, \alpha_q)_k$.

---

[1]) R. Dedekind, Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen и Über die Diskriminanten endlicher Körper, Abh. d. K. Ges. d. Wiss. zu Göttingen, 1878 и 1882; см. также последующие работы Hensel'я в Crelles Journal, Bd. 105 (1889) и Bd. 113 (1894).

Действительно, одновременно с равенством

$$\beta = \sum_h \Gamma_h \alpha_h$$

с целыми Γ_h из K имеют место равенства

$$\beta = \sum_h \Gamma_h^{(i)} \alpha_h \quad (i = 1, \ldots, m)$$

с относительно сопряженными $\Gamma_h^{(i)}$. Перемножением их получаем

$$\beta^m = \prod_{i=1}^{m} \Big(\sum_h \Gamma_h^{(i)} \alpha_h \Big).$$

Но выражение

$$\prod_{i=1}^{m} \Big(\sum_{h=1}^{q} \Gamma_h^{(i)} x_h \Big) = \sum_{n_1, \ldots, n_q} \gamma_{n_1 n_2 \ldots n_q} x_1^{n_1} x_2^{n_2} \ldots x_q^{n_q} \tag{71}$$

есть однородный полином измерения m относительно переменных $x_1, \ldots, x_q$,

$$n_1 + n_2 + \ldots + n_q = m,$$

коэфициенты которого, как целые симметрические выражения относительно $\Gamma_h^{(i)}$, являются целыми числами из k. Поэтому при $x_h = \alpha_h$ $(h = 1, \ldots, q)$ (71) есть число идеала $\mathfrak{a}^m$, следовательно, $\frac{\beta^m}{\mathfrak{a}^m}$ и, значит, также $\frac{\beta}{\mathfrak{a}}$ — целый идеал, т. е. β содержится в $\mathfrak{a}$.

Таким образом, если дана другая пара соответственных идеалов:

$$\mathfrak{b} = (\beta_1, \ldots, \beta_s)_k \quad \text{и} \quad \mathfrak{B} = (\beta_1, \ldots, \beta_s)_K,$$

то имеет место

Лемма b). *Если* $\mathfrak{a} = \mathfrak{b}$, *то* $\mathfrak{A} = \mathfrak{B}$, *и обратно.*

Первая половина леммы очевидна. Но если $\mathfrak{A} = \mathfrak{B}$, то каждое β из $\mathfrak{B}$ принадлежит $\mathfrak{A}$, значит, по лемме a) также к $\mathfrak{a}$, и точно так же каждое α из $\mathfrak{A}$ принадлежит $\mathfrak{b}$, откуда и следует, что $\mathfrak{a} = \mathfrak{b}$.

Отнесем теперь каждому идеалу $\mathfrak{a}$ из k идеал $\mathfrak{A}$ из K по следующему правилу: если $\mathfrak{a} = (\alpha_1, \ldots, \alpha_q)_k$, то в качестве $\mathfrak{A}$ возьмем $\mathfrak{A} = (\alpha_1, \ldots, \alpha_q)_K$. Это правило, в силу леммы b), дает вполне определяемый идеалом $\mathfrak{a}$ (независимо от представления $\mathfrak{a}$) идеал $\mathfrak{A}$, и притом мы получим таким путем каждый идеал из K, являющийся наибольшим общим делителем каких-либо чисел основного поля k. Это соответствие является тогда, в силу леммы b), взаимно однозначным; мы будем символически записывать его так:

$$\mathfrak{a} \leftrightarrows \mathfrak{A}. \tag{72}$$

Таким образом имеет место

Теорема 106. *С помощью соотношения* (72) *между всеми идеалами из* k, *с одной стороны, и всеми теми идеалами из* K, *которые являются наибольшими общими делителями каких-либо чисел из* k, *с другой стороны, устанавливается взаимно однозначное соответствие, такое, что утверждения*

„α принадлежит $\mathfrak{a}$“ и „α принадлежит $\mathfrak{A}$“,

где $\mathfrak{a}$ *и* $\mathfrak{A}$ *связаны соотношением* (72), *верны лишь одновременно; кроме того, если* $\mathfrak{a} \leftrightarrows \mathfrak{A}$ *и* $\mathfrak{b} \leftrightarrows \mathfrak{B}$, *то также*

$$\mathfrak{ab} \leftrightarrows \mathfrak{AB}.$$

Определение. Два идеала, связанные соотношением (72), мы будем называть равными друг другу и говорить, что идеал $\mathfrak{A}$ из K лежит в поле k.

Поскольку соотношение „$=$“ между идеалами различных полей еще не было определено, сформулированное только что определение не стоит ни в каком противоречии с полученными ранее результатами. В силу теоремы 106, имеют место следующие правила:

1. Из $\mathfrak{a} = \mathfrak{A}$ и $\mathfrak{a} = \mathfrak{b}$ следует $\mathfrak{b} = \mathfrak{A}$.
2. Из $\mathfrak{a} = \mathfrak{A}$ и $\mathfrak{b} = \mathfrak{A}$ следует $\mathfrak{a} = \mathfrak{b}$.
3. Из $\mathfrak{a} = \mathfrak{A}$ и $\mathfrak{A} = \mathfrak{B}$ следует $\mathfrak{a} = \mathfrak{B}$.
4. Из $\mathfrak{a} = \mathfrak{A}$ и $\mathfrak{b} = \mathfrak{B}$ следует $\mathfrak{ab} = \mathfrak{AB}$.
5. Из $\mathfrak{a}^p = \mathfrak{A}^p$ следует $\mathfrak{a} = \mathfrak{A}$ (p — целое рациональное).

Эти правила в совокупности означают, что установленное нами соотношение „$=$“ между идеалами в различных полях является обобщением ранее определенного и записываемого тем же знаком „$=$“ соотношения между идеалами одного и того же поля.

Сформулированным выше определением устанавливается, таким образом, можно ли два данных символа

$$(\alpha_1, \ldots, \alpha_q) \text{ из } k, \quad (\mathrm{A}_1, \ldots, \mathrm{A}_s) \text{ из } K$$

обозначить как равные или нельзя. При этом K мыслится как поле над k. Но при некоторых обстоятельствах оба символа могут иметь смысл уже в некотором под-поле K' поля K, и возникает вопрос, можно ли из равенства в одном поле заключить о равенстве также в другом.

Этот вопрос решается утвердительно. В самом деле, если K' над-поле относительно k и вместе с тем под-поле относительно K и если A принадлежит K', то из равенства

$$(\alpha_1, \ldots, \alpha_q)_{K'} = (\mathrm{A}_1, \ldots, \mathrm{A}_s)_{K'} \tag{73}$$

очевидно, сразу следует равенство

$$(\alpha_1, \ldots, \alpha_q)_K = (\mathrm{A}_1, \ldots, \mathrm{A}_s)_K.$$

Обратно, если последнее равенство справедливо, то по второй части леммы b), примененной к над-полю K поля K', справедливо также равенство (73) в K'.

Таким образом символ $(\alpha_1, \ldots, \alpha_q)$ определяет во всех полях, где он вообще имеет смысл, один и тот же идеал. И мы можем теперь говорить о равенстве или неравенстве двух идеалов $\mathfrak{a}_1$, $\mathfrak{a}_2$, определенных соответственно как наибольшие общие делители чисел произвольных полей k_1, k_2. Для этого нужно лишь перейти к любому полю K, содержащему одновременно k_1 и k_2, и установить, равны или не равны в смысле нашего первоначального определения (§ 24) эти наибольшие общие делители в поле K; результат будет один и тот же для всех таких полей K. Поэтому мы можем не указывать в обозначении $\mathfrak{a} = (\alpha_1, \ldots, \alpha_q)$ определенного поля, к которому оно относится. В силу правила 4, произведение двух идеалов $\mathfrak{a}$, $\mathfrak{b}$ также есть вполне определенный идеал, определяемый единственно лишь идеалами $\mathfrak{a}$ и $\mathfrak{b}$; то же справедливо для отношения и наибольшего общего делителя.

Таким образом, в частности, выражение „целые алгебраические числа $\alpha_1, \ldots, \alpha_q$ взаимно просты (имеют наибольший общий делитель (1))“ имеет смысл безотносительно к какому-либо специальному числовому полю и равносильно утверждению о существовании целых алгебраических чисел $\lambda_1, \ldots, \lambda_q$, для которых

$$\lambda_1\alpha_1 + \ldots + \lambda_q\alpha_q = 1.$$

Замечательным фактом, непосредственно вытекающим из наших рассмотрений, является при этом то, что если вообще существуют целые числа λ, обладающие указанным свойством, то они всегда будут существовать и в поле, порожденном числами $\alpha_1, \ldots, \alpha_q$.

Однако следует подчеркнуть, что идеалы, вообще говоря, не лежат, в смысле данного выше определения, одновременно во всех числовых полях. Так, например,

$$\mathfrak{a} = (5, \sqrt{10}) = (\sqrt{5}),$$

ибо квадраты обоих стоящих справа идеалов равны, в смысле введенного выше определения, идеалу (5). Таким образом $\mathfrak{a}$ лежит в обоих квадратичных полях $k(\sqrt{10})$ и $k(\sqrt{5})$; но $\mathfrak{a}$ не лежит в поле $k(1)$.

Свойство быть простым идеалом принадлежит идеалу лишь по отношению к некоторому определенному полю.

Сопоставляя теперь введенные понятия с теоремами § 33 об идеальных числах, мы получаем следующее: Если $\mathfrak{a}$ — идеал в k и $\mathfrak{a}^h$ есть главный идеал (ω) в k, то равенство

$$\mathfrak{a} = (\sqrt[h]{\omega}),$$

имеющее смысл в силу наших теперешних определений, является верным равенством. Если, далее, идеалу $\mathfrak{a}$ поля k соответствует число A из системы идеальных чисел этого поля, то точно так же $\mathfrak{a} = (\mathrm{A})$. Совокупность идеальных чисел поля k принадлежит некоторому полю степени h относительно k; этот факт мы можем теперь выразить следующим образом: Если h — число классов поля k, то суще-

ствует относительное поле над k относительной степени h, в котором все идеалы поля k являются главными идеалами. Впрочем, этим требованием относительное поле не определяется однозначно. Кроме того, число его классов может быть и не равно 1.

§ 38. Относительные нормы чисел и идеалов. Относительные диференты и относительные дискриминанты

Пусть A — любое число из K и $A^{(i)}$ $(i = 1, \ldots, m)$ — его сопряженные относительно k. Числа

$$S_k(A) = A^{(1)} + A^{(2)} + \ldots + A^{(m)},$$
$$N_k(A) = A^{(1)}A^{(2)} \ldots A^{(m)}$$

называются соответственно *относительным следом* и *относительной нормой* числа A (относительно k). Они содержатся в k. Если S и s — следы в K и в k относительно $k(1)$, а N и n — нормы в K и в k, то по теореме 59

$$S(A) = s(S_k(A)), \quad N(A) = n(N_k(A)). \tag{74}$$

Число

$$\delta_k(A^{(q)}) = \prod_{i=1,\ i \neq q}^{m} (A^{(q)} - A^{(i)})$$

называется *относительной диферентой* числа $A^{(q)}$ в поле $K^{(q)}$ относительно поля k; оно есть число поля $K^{(q)}$. Имеем

$$\delta_k(A) = \Phi'(A),$$

где

$$\Phi(x) = \prod_{i=1}^{m} (x - A^{(i)}) = x^m + \alpha_1 x^{m-1} + \ldots + \alpha_{m-1}x + \alpha_m$$

(α_i суть, очевидно, числа из k). Произведение

$$d_k(A) = \prod_{1 \leqslant i < q \leqslant m} (A^{(i)} - A^{(q)})^2 = (-1)^{\frac{m(m-1)}{2}} \prod_{i=1}^{m} \Phi'(A^{(i)}) =$$
$$= (-1)^{\frac{m(m-1)}{2}} N_k(\delta_k(A))$$

называется *относительным дискриминантом* числа A; оно есть число из k.

Пусть $\mathfrak{A}$ — идеал в K. Относительно сопряженные идеалы $\mathfrak{A}^{(i)}$ получатся, если заменить каждое его число A через $A^{(i)}$. Очевидно,

$$(\mathfrak{AB})^{(i)} = \mathfrak{A}^{(i)}\mathfrak{B}^{(i)}.$$

Определение. *Относительной нормой* идеала $\mathfrak{A}$ относительно поля k называется идеал

$$N_k(\mathfrak{A}) = \mathfrak{A}^{(1)}\mathfrak{A}^{(2)} \ldots \mathfrak{A}^{(m)}.$$

Имеем $N_k(\mathfrak{AB}) = N_k(\mathfrak{A})\, N_k(\mathfrak{B})$.

Теорема 107. *$N_k(\mathfrak{A})$ есть идеал в k. Если k — поле рациональных чисел, то $N_k(\mathfrak{A}) = (N(\mathfrak{A}))$.*

В самом деле, пусть сначала мы имеем целый идеал $\mathfrak{A} = (\mathrm{A}_1, \ldots, \mathrm{A}_s)$, где A — числа из K. По § 28, содержание сопряженного полинома относительно произвольных переменных $u_1, \ldots, u_s$

$$F^{(i)}(u) = \mathrm{A}_1^{(i)} u_1 + \ldots + \mathrm{A}_s^{(i)} u_s$$

равно $\mathfrak{A}^{(i)}$. В силу теоремы 87, мы имеем поэтому

$$\mathfrak{A}^{(1)} \ldots \mathfrak{A}^{(m)} = I(F^{(1)}) \ldots I(F^{(m)}) = I(F^{(1)} \ldots F^{(m)}).$$

Но

$$Q(u) = F^{(1)} \ldots F^{(m)}$$

есть, очевидно, полином в k, следовательно, $I(Q)$ есть идеал в k. Так как каждый идеал представим в виде отношения двух целых идеалов и, в силу определения,

$$N_k\left(\frac{\mathfrak{A}}{\mathfrak{B}}\right) = \frac{N_k(\mathfrak{A})}{N_k(\mathfrak{B})},$$

то первая часть теоремы доказана.

Пусть теперь h — число классов поля K. Тогда $\mathfrak{A}^h = (\mathrm{A})$, где A — некоторое число из K. Если k — поле рациональных чисел, то имеем

$$N_k(\mathfrak{A})^h = N_k(\mathfrak{A}^h) = N((\mathrm{A})) = (N(\mathrm{A})).$$

Так как

$$\pm N(\mathrm{A}) = N(\mathfrak{A}^h) = N(\mathfrak{A})^h,$$

то мы получаем

$$N_k(\mathfrak{A})^h = (N(\mathfrak{A}))^h, \quad N_k(\mathfrak{A}) = (N(\mathfrak{A})),$$

чем доказана и вторая часть теоремы.

Тем самым теорема 88 из § 29, сформулированная для полей Галуа, оказывается верной для всех полей, и вместе с тем обосновывается название „норма идеала $\mathfrak{A}$“ для числа классов вычетов mod $\mathfrak{A}$.

Теорема 108. *Для каждого простого идеала $\mathfrak{P}$ из K существует точно один простой идеал $\mathfrak{p}$ из k, делящийся на $\mathfrak{P}$. При этом*

$$N_k(\mathfrak{P}) = \mathfrak{p}^{f_1},$$

где f_1 — натуральное число, не превосходящее n. f_1 называется относительной степенью $\mathfrak{P}$ (относительно k). $\mathfrak{p}$ распадается в K не более чем на n множителей.

В самом деле, по теореме 107 $N_k(\mathfrak{P})$ есть идеал в k; при этом он по своему определению делится на $\mathfrak{P}$. По основной теореме теории идеалов, $\mathfrak{P}$ должен делить по крайней мере один из простых идеалов в k, на которые раскладывается $N_k(\mathfrak{P})$. Если бы $\mathfrak{P}$ делил два различных простых идеала $\mathfrak{p}_1$, $\mathfrak{p}_2$ в k, то он делил бы и их наибольший

общий делитель $(\mathfrak{p}_1, \mathfrak{p}_2) = 1$, чего, однако, быть не может. Таким образом существует точно один простой идеал в k, делящийся на $\mathfrak{P}$. Пусть теперь

$$\mathfrak{p} = \mathfrak{P}_1 \mathfrak{P}_2 \dots \mathfrak{P}_v$$

— разложение $\mathfrak{p}$ на простые идеалы в K. Тогда для относительных норм имеем

$$N_k(\mathfrak{P}_1) N_k(\mathfrak{P}_2) \dots N_k(\mathfrak{P}_v) = N_k(\mathfrak{p}) = \mathfrak{p}^m.$$

Каждый множитель в левой части равенства есть по предыдущей теореме идеал в k и, следовательно, в силу этого равенства, является некоторой степенью $\mathfrak{p}$:

$$N_k(\mathfrak{P}_i) = \mathfrak{p}^{f_i};$$

при этом $f_1 + \dots + f_v = m$, следовательно,

$$f_i \leqslant m \quad \text{и} \quad v \leqslant m.$$

Теорема 109. *Для каждого идеала $\mathfrak{A}$ в K*

$$N(\mathfrak{A}) = n(N_k(\mathfrak{A})),$$

где N означает норму идеала в K и n — норму в k.

Действительно, в силу (74), это утверждение верно для каждого числа A из K. Путем рассмотрения главного идеала $\mathfrak{A}^h$ мы убеждаемся в справедливости его и для каждого идеала из K.

Теорема 110. *Если относительная степень простого идеала $\mathfrak{P}$ равна 1, то каждое число из K сравнимо по модулю $\mathfrak{P}$ с некоторым числом из k.*

В самом деле, в силу теорем 108 и 109, $N(\mathfrak{P}) = n(\mathfrak{p})^{f_1}$. Поэтому при $f_1 = 1$ число классов вычетов mod $\mathfrak{P}$ в K равно числу классов вычетов mod $\mathfrak{p}$ в k. Но если число α из k делится на $\mathfrak{P}$, то $(\alpha, \mathfrak{p})$ делится по крайней мере на $\mathfrak{P}$, следовательно, $\neq (1)$ и потому $(\alpha, \mathfrak{p})$ как идеал в k необходимо равно $\mathfrak{p}$. Тем самым система чисел из k, несравнимых mod $\mathfrak{p}$, будет также системой чисел, несравнимых mod $\mathfrak{P}$. Таким образом существует $n(\mathfrak{p}) = N(\mathfrak{P})$ чисел из k, несравнимых mod $\mathfrak{P}$, что и доказывает теорему.

Отметим еще особо следующий факт. Если число A из K совпадает со всеми своими относительно сопряженными, то по теореме 56 оно есть число из k; но соответствующее утверждение для идеалов неверно. Например, в $k(\sqrt{5})$ идеал $(\sqrt{5})$ совпадает с его сопряженным относительно $k(1)$ и однако, он не является идеалом в $k(1)$.

Наконец, укажем еще, что введенные в § 36 понятия могут быть перенесены на относительные поля; мы приходим при этом к следующему определению относительной диференты:

Определение. Совокупность чисел A из K, обладающих тем свойством, что для каждого целого числа A из K относительный

след $S_k(\Delta A)$ есть целое число, состоит из чисел некоторого идеала $\mathfrak{M}$ из K. При этом

$$\frac{1}{\mathfrak{M}} = \mathfrak{D}_k$$

есть целый идеал и называется *относительной дифферентой* поля K относительно поля k.

Доказательство содержащихся в этом определении утверждений проводится аналогично доказательству теоремы 101.

Теорема 111. *Относительная дифферента $\mathfrak{D}_k$ поля K связана с дифферентами $\mathfrak{D}$ и $\mathfrak{d}$ полей K и k соотношением*

$$\mathfrak{D} = \mathfrak{D}_k\mathfrak{d}. \tag{75}$$

Доказательство. Пусть Δ — такое число из K, что $\Delta\mathfrak{D}_k\mathfrak{d}$ есть целый идеал. Тогда, по определению $\mathfrak{D}_k$, для каждого целого A из K

$$\mathfrak{d}S_k(\Delta A) \text{ целый идеал,} \tag{76}$$

так как для каждого числа ξ из k, делящегося на $\mathfrak{d}$,

$$S_k(\Delta A\xi) = \xi S_k(\Delta A)$$

есть целое число. В силу (76) и определения $\mathfrak{d}$, $s(S_k(\Delta A))$ есть целое число. Следовательно, $S(\Delta A)$ — целое и потому $\mathfrak{D}\Delta$ — целый идеал, если $\mathfrak{D}_k\mathfrak{d}\Delta$ — целый идеал.

Обратно, пусть $\mathfrak{D}\Delta$ — целый идеал, тогда для каждого целого A из K и каждого целого ξ из k также $S(\Delta A\xi)$ — целое, следовательно, $s(S_k(\Delta A\xi)) = s(\xi S_k(\Delta A))$ — целое, значит, $\mathfrak{d}S_k(\Delta A)$ есть целый идеал, т. е. $S_k(\rho\Delta A)$ есть целое число для любого ρ из k, входящего в $\mathfrak{d}$, поэтому $\rho\Delta\mathfrak{D}_k$ есть целый идеал; но отсюда следует, что $\mathfrak{D}_k\mathfrak{d}\Delta$ — целый идеал, если $\mathfrak{D}\Delta$ — целый.

В соединении с доказанным выше обратным утверждением это завершает доказательство теоремы 111.

Значение относительной дифференты, обнаруживаемое доказанным только что простым равенством (75), становится еще более очевидным в свете следующего предложения, могущего также служить определением для $\mathfrak{D}_k$:

Теорема 112. *Относительная дифферента поля K есть наибольший общий делитель дифферент всех целых чисел из K относительно поля k.*

Доказательство этой теоремы проводится в основных чертах тем же путем, что и доказательство теоремы 105 из § 36.

Пусть Θ — целое производящее число поля K. Под *относительным кольцом* $R_k(\Theta)$ мы будем понимать совокупность чисел

$$\alpha_0 + \alpha_1\Theta + \ldots + \alpha_{m-1}\Theta^{m-1},$$

где $\alpha_0, \ldots, \alpha_{m-1}$ пробегают все целые числа из k. Пусть $\Phi(x)$ — неприводимый в k полином со старшим коэфициентом 1, имеющий кор-

нем Θ. Тогда справедливы следующие предложения, доказываемые как в § 36.

Лемма a). *Каждое число* A *из* K, *для которого* $A\mathfrak{D}_k$ — *целый идеал, представимо в форме*

$$A = \frac{B}{\Phi'(\Theta)},$$

где B — *некоторое число из* $R_k(\Theta)$. *Следовательно,* $\Phi'(\Theta)$ *делится на* $\mathfrak{D}_k$.

Лемма b). *Для каждого* B *из* $R_k(\Theta)$, $S_k\left(\frac{B}{\Phi'(\Theta)}\right)$ *есть целое число.*

Теорема 113. *Наибольший общий делитель* $\mathfrak{F}$ *всех идеалов в* K, *содержащих лишь числа из* $R_k(\Theta)$, *равен* $\frac{\Phi'(\Theta)}{\mathfrak{D}_k}$.

Лемма c). *Для каждого простого идеала* $\mathfrak{P}$ *из* K *существует такое относительное кольцо* $R_k(\Theta)$, *что* $\mathfrak{P}$ *не делит* $\mathfrak{F} = \frac{\Phi'(\Theta)}{\mathfrak{D}_k}$.

В самом деле, пусть $\mathfrak{p}$ — простой идеал в k, делящийся на $\mathfrak{P}$,

$$\mathfrak{p} = \mathfrak{P}^e\mathfrak{A}, \quad (\mathfrak{A}, \mathfrak{P}) = 1.$$

Пусть, далее, A — такое первообразное число mod $\mathfrak{P}$, что каждое целое число из K по любой степени $\mathfrak{P}$ сравнимо с некоторым числом из $R_k(A)$, и притом

$$A \equiv 0 \pmod{\mathfrak{A}}.$$

Наконец, пусть β — число из k, делящееся на $\Phi'(A) = \mathfrak{D}_k\mathfrak{F}$, и $\mathfrak{p}^b$ — наивысшая входящая в $\mathfrak{b}$ степень $\mathfrak{p}$. Тогда некоторая степень $\alpha = \beta^h$ числа β допускает разложение на два числовых множителя в k:

$$\alpha = \pi\mu, \text{ где } \pi = \mathfrak{p}^{hb}, \ (\mu, \mathfrak{p}) = 1;$$
$$\alpha \equiv 0 \pmod{\mathfrak{F}\mathfrak{D}_k}.$$

Пусть теперь Δ — произвольно заданное целое число из K, и Γ — число из $R_k(A)$ такое, что

$$\Delta \equiv \Gamma \pmod{\mathfrak{P}^{eh b}}.$$

Тогда число $B\mu A^{hb} = (\Delta - \Gamma)\mu A^{hb}$ делится на $\mathfrak{D}_k\mathfrak{F} = \Phi'(A)$, ибо

$$\frac{B\mu A^{hb}}{\Phi'(A)} = \frac{\pi\mu}{\mathfrak{D}_k\mathfrak{F}} \frac{BA^{hb}}{\pi} = \frac{\alpha}{\mathfrak{D}_k\mathfrak{F}} \frac{BA^{hb}}{\mathfrak{P}^{ehb}\mathfrak{A}^{hb}}$$

— целое число. Применяя лемму a), мы получаем поэтому, что

$$\Delta\mu A^{hb} \text{ есть число из } R_k(A),$$

откуда по теореме 113 заключаем, что идеал μA^{hb} делится на $\mathfrak{F}$. А так как μA^{hb} не делится на $\mathfrak{P}$, то и $\mathfrak{F}$ не делится на $\mathfrak{P}$, что и завершает доказательство леммы, а вместе с нею и теоремы 112.

Под *дискриминантом поля K относительно k* мы будем понимать теперь, по определению, относительную норму относительной диференты поля K. В силу теоремы 103, определенный таким образом дискриминантный идеал относительно $k(1)$ будет совпадать с идеалом (d), где d — дискриминант поля K. Мы, однако, должны различать дискриминант поля, представляющий собой некоторое совершенно определенное число d, и относительный дискриминант этого же поля относительно поля $k(1)$, являющийся идеалом, именно (d).

В завершение исследований, относящихся к диферентам, докажем, наконец, следующую теорему, примыкающую, в применении к основному полю $k = k(1)$, к общей постановке вопроса в начале § 29.

Теорема 114. *Если простой идеал $\mathfrak{P}$ из K входит множителем в простой идеал $\mathfrak{p}$ из k выше чем в первой степени, то $\mathfrak{P}$ является множителем относительной диференты поля K. Таким образом простых идеалов $\mathfrak{P}$, обладающих подобным свойством, может существовать лишь конечное множество.*

В самом деле, пусть

$$\mathfrak{p} = \mathfrak{P}^e\mathfrak{A}, \text{ где } (\mathfrak{A}, \mathfrak{P}) = 1, \quad e \geqslant 2,$$

— разложение $\mathfrak{p}$ на множители в поле K, и пусть p — рациональное простое число, делящееся на $\mathfrak{p}$. В силу неоднократно применявшегося свойства биномиальных коэфициентов $\binom{p}{n}$, имеем для каждого целого числа A из K

$$S_k(\mathrm{A})^p \equiv S_k(\mathrm{A}^p) \pmod{p, \text{ значит и } \mathfrak{p}}. \tag{77}$$

Выберем теперь

$$\mathrm{A} \equiv 0 \pmod{\mathfrak{P}^{e-1}\mathfrak{A}};$$

в силу условия $e \geqslant 2$, имеем тогда

$$\mathrm{A}^p \equiv 0 \pmod{\mathfrak{p}}, \quad S_k(\mathrm{A}^p) \equiv 0 \pmod{\mathfrak{p}}. \tag{78}$$

Отсюда, в силу (77), мы получаем, что

$$S_k(\mathrm{A}) \equiv 0 \pmod{\mathfrak{p}}, \quad \text{если} \quad \mathrm{A} \equiv 0 \pmod{\mathfrak{P}^{e-1}\mathfrak{A}}. \tag{79}$$

Пусть теперь α — нецелое число из k, которое, рассматриваемое как дробный идеал, имеет знаменатель $\mathfrak{p}$:

$$\alpha = \frac{\mathfrak{a}}{\mathfrak{p}}, \quad (\mathfrak{a}, \mathfrak{p}) = 1.$$

Тогда вследствие (79) $\alpha S_k(\mathrm{A}) = S_k(\alpha\mathrm{A})$ есть целое число для всех A из $\mathfrak{P}^{e-1}\mathfrak{A}$, т. е. для всех αA из $\frac{\mathfrak{a}}{\mathfrak{P}}$. Следовательно, по определению относительной диференты, $\mathfrak{P}$ входит множителем в относительную диференту $\mathfrak{D}_k$.

Обращение теоремы 114 также верно, однако, доказывается труднее. Мы ограничимся здесь рассмотрением специального случая относительных полей Галуа.

Теорема 115. *Пусть K совпадает со всеми своими сопряженными относительно k (т. е. является относительным полем Галуа). Тогда относительная дифферента $\mathfrak{D}_k$ поля K делится лишь на такие простые идеалы из K, которые входят множителями в некоторый простой идеал из k выше чем в первой степени.*

Действительно, пусть $\mathfrak{p}$ — простой идеал в k и $\mathfrak{P}$ — простой множитель $\mathfrak{p}$ в K, квадрат которого уже не делит $\mathfrak{p}$. Тогда и относительно сопряженные простые идеалы $\mathfrak{P}^{(i)}$ входят в $\mathfrak{p}$ точно в первой степени. Относительная норма $\mathfrak{p}^f$ идеала $\mathfrak{P}$ есть произведение всех $\mathfrak{P}^{(i)}$, поэтому среди последних имеется по f совпадающих и, значит, существует точно $\frac{m}{f}$ различных между собой, где m — степень K относительно k. Пусть, скажем, $\mathfrak{P}^{(1)}$, $\mathfrak{P}^{(2)}$, ..., $\mathfrak{P}^{(f)}$ — совпадающие с $\mathfrak{P}$ его сопряженные.

В силу теоремы 112, для доказательства теоремы 115 достаточно указать число A из K, относительная дифферента которого не делилась бы на $\mathfrak{P}$. Возьмем в качестве A первообразный корень $\bmod \mathfrak{P}$, делящийся на $\frac{\mathfrak{p}}{\mathfrak{P}}$. Согласно сказанному выше $\mathfrak{P}^{(f+1)}$, ..., $\mathfrak{P}^{(m)}$ отличны от $\mathfrak{P}$, и, следовательно, $\frac{\mathfrak{p}}{\mathfrak{P}^{(i)}}$ делится на $\mathfrak{P}$ для $i = f+1, \ldots, m$. Тем самым и

$$A^{(i)} \equiv 0 \pmod{\mathfrak{P}} \quad \text{для} \quad i = f+1, \ldots, m.$$

Пусть теперь

$$\Phi(x) = \prod_{r=1}^{m} (x - A^{(r)})$$

и, значит, есть полином в k. В силу (44),

$$\Phi(x)^{n(\mathfrak{p})} \equiv \Phi(x^{n(\mathfrak{p})}) \pmod{\mathfrak{p}},$$

так что сравнение $\Phi(x) \equiv 0 \pmod{\mathfrak{P}}$ во всяком случае имеет корни 0, A, $A^{n(\mathfrak{p})}$, ..., $A^{n(\mathfrak{p})^{f-1}}$. Так как A — первообразное число $\bmod \mathfrak{P}$, то эти $f+1$ чисел наверное различны $\bmod \mathfrak{P}$. Поэтому, в силу равенства $\Phi(x) = \prod_{r=1}^{m} (x - A^{(r)})$, по меньшей мере $f+1$ среди чисел $A^{(1)}$, ..., $A^{(m)}$ должны быть различны $\bmod \mathfrak{P}$. А так как последние $m-f$ из этих чисел сравнимы с нулем $\bmod \mathfrak{P}$, то $A^{(1)}$, ..., $A^{(f)}$ различны $\bmod \mathfrak{P}$ и, следовательно, относительная дифферента

$$\delta_k(A^{(1)}) = (A^{(1)} - A^{(2)}) \ldots (A^{(1)} - A^{(m)})$$

не делится на $\mathfrak{P}$, чем теорема и доказана.

§ 39. Законы разложения в относительных полях $K(\sqrt[l]{\mu})$

В качестве наиболее важного примера на применение полученных результатов исследуем законы разложения простых идеалов некоторого основного поля k в относительном поле K, получающемся путем

присоединения к полю k корня l-й степени из какого-нибудь числа этого же поля k. При этом мы сделаем следующие

Предположения: l — положительное рациональное простое число (допускается также $l=2$); поле k содержит корень l-й степени из 1 $\zeta=e^{\frac{2\pi i}{l}}$.

Лемма. *Числа* $1-\zeta^a$ $(\alpha \not\equiv 0 \pmod l)$ *все взаимно ассоциированы. Имеет место равенство идеалов*

$$(l)=(1-\zeta)^{l-1}. \tag{80}$$

В самом деле, пусть a, a_1 — целые рациональные числа, не делящиеся на l. Определим положительное целое рациональное число b так, чтобы удовлетворялось сравнение

$$ab \equiv a_1 \pmod l,$$

и, значит, имело место равенство

$$\zeta^{a_1}=\zeta^{ab}.$$

Тогда

$$\frac{1-\zeta^{a_1}}{1-\zeta^a}=\frac{1-\zeta^{ab}}{1-\zeta^a}=1+\zeta^a+\zeta^{2a}+\ldots+\zeta^{(b-1)a},$$

т. е. $\frac{1-\zeta^{a_1}}{1-\zeta^a}$ есть целое число; точно так же убеждаемся в том, что и обратное отношение $\frac{1-\zeta^a}{1-\zeta^{a_1}}$ есть целое число; следовательно, эти отношения суть единицы.

Далее,

$$1+x+\ldots+x^{l-1}=\frac{x^l-1}{x-1}=(x-\zeta)(x-\zeta^2)\ldots(x-\zeta^{l-1}),$$

откуда при $x=1$ получаем

$$l=(1-\zeta)(1-\zeta^2)\ldots(1-\zeta^{l-1}).$$

В силу первой части леммы отсюда вытекает равенство идеалов (80).

Из доказанной леммы мы можем, в частности, сделать тот вывод, что поле $K(\zeta)$ имеет точно степень $l-1$. В самом деле, согласно § 30, степень поля $K(\zeta)$ не превосходит $\varphi(l)=l-1$, а с другой стороны, в силу (80), в этом поле простое число l есть $(l-1)$-я степень идеала, значит, по теореме 81, степень поля не может быть меньше $l-1$ и, таким образом, она точно равна $l-1$; кроме того, в силу той же теоремы 81, $1-\zeta$ есть простой идеал в $K(\zeta)$.

Теорема 116. *Если* μ *— число из* k, *не являющееся* l*-й степенью никакого числа из* k, *то поле* $K(\sqrt[l]{\mu};k)$ *имеет степень* l *относительно* k *и совпадает со всеми своими относительно сопряженными полями (т. е. является относительным полем Галуа).*

Действительно, число $M = \sqrt[l]{\mu}$ (где взято какое-нибудь фиксированное значение корня) удовлетворяет уравнению $x^l - \mu = 0$, все корни которого даются формулой

$$\zeta^a M \quad (a = 0, 1, \ldots, l-1).$$

Среди этих чисел должны во всяком случае содержаться все числа, относительно сопряженные с M. Пусть это будет m ($m \leqslant l$) чисел $\zeta^{a_1}M, \ldots, \zeta^{a_m}M$. Их произведение как относительная норма числа M должно быть числом из k; поэтому M^m содержится в k. Но также и $M^l = \mu$ содержится в k. Если поэтому $m < l$, так что m взаимно просто с l (ибо l — простое число), то M, будучи представимым в виде произведений степеней M^l и M^m, само есть число из k, что противоречит предположению. Таким образом $m = l$, и теорема доказана.

Числа $M_1 = \sqrt[l]{\mu_1}$ и $M_2 = \sqrt[l]{\mu_2}$ порождают одно и то же относительное поле, если имеет место равенство

$$\mu_1^a \mu_2^b = \alpha^l,$$

где α — число из k, а a и b — целые рациональные числа, не делящиеся на l. Каждое число из K может быть единственным образом представлено в форме

$$A = \alpha_0 + \alpha_1 M + \ldots + \alpha_{l-1} M^{l-1},$$

где $\alpha_0, \alpha_1, \ldots, \alpha_{l-1}$ — числа из k. Числа, относительно сопряженные с A, мы получим, заменяя здесь M последовательно через ζM, $\zeta^2 M, \ldots, \zeta^{l-1}M$. Пусть теперь вообще sA означает то из относительно сопряженных с A чисел, которое получается путем замены M через ζM:

$$sA = \alpha_0 + \alpha_1(\zeta M) + \alpha_2(\zeta M)^2 + \ldots + \alpha_{l-1}(\zeta M)^{l-1},$$
$$sM = \zeta M,$$

и пусть, для каждого целого рационального $n \geqslant 1$,

$$s^1 A = sA, \quad s^n A = s(s^{n-1}A), \quad \text{следовательно,} \quad s^n M = \zeta^n M,$$

так что

$$s^l A = s^{2l} A = \ldots = s^{ml} A = A$$

для всякого натурального m. Эти l „подстановок“ $s, s^2, \ldots, s^l$ образуют, очевидно, циклическую группу порядка l, в которой s^l играет роль единичного элемента. Отрицательные степени s определяются тогда как в § 35:

$$s^0 A = A, \quad s^{-1}A = s^{l-1}A, \quad s^{-n}A = s^{n(l-1)}A \quad (n > 0).$$

Из теоремы 55 вытекает, что каждое рациональное соотношение между числами $A_1, A_2, \ldots$ из K с коэфициентами из k остается справедливым, если одновременно заменить все $A_1, A_2, \ldots$ через $sA_1, sA_2, \ldots$, следовательно, вообще через $s^m A_1, s^m A_2, \ldots$

Основываясь на этом обстоятельстве циклическую группу $(s, s^2, \ldots, s^{l-1}, s^l)$ называют группой Галуа поля K относительно поля k, а поле K называют *относительно циклическим полем относительно* k (или циклическим полем расширения k).

Так как относительная степень l есть, по предположению, простое число, то по теореме 54 число A из K либо отлично от всех чисел sA, s^2A, ..., s^{l-1}A, либо совпадает со всеми ними.

Символ подстановки s^m мы будем применять также к идеалам, обозначая через $s^m\mathfrak{A}$ тот из сопряженных с $\mathfrak{A}$ идеалов, который получится, если все числа A из $\mathfrak{A}$ заменить через s^mA.

Теорема 117. *При переходе от k к K простой идеал $\mathfrak{p}$ поля k может лишь остаться и в K простым идеалом, либо стать в K l-й степенью простого идеала, либо стать в K произведением l различных простых идеалов.*

Действительно, пусть $\mathfrak{P}$ — простой идеал из K, делящий $\mathfrak{p}$. Тогда, в силу теоремы 108, относительная норма $\mathfrak{P}$ равна

$$\mathfrak{P} \cdot s\mathfrak{P} \ldots s^{l-1}\mathfrak{P} = \mathfrak{p}^{f_1},$$

где f_1 — относительная степень $\mathfrak{P}$. Следовательно, в $\mathfrak{p}$ входят лишь простые идеалы $s^m\mathfrak{P}$. Теперь, либо $\mathfrak{P}$ совпадает с каким-нибудь $s^m\mathfrak{P}$ ($m \not\equiv 0 \pmod{l}$) и, значит, со всеми $s^m\mathfrak{P}$, так что

$$\mathfrak{p} = \mathfrak{P}^a,$$

для некоторого натурального a; беря относительные нормы обеих частей, мы получаем $\mathfrak{p}^l = \mathfrak{p}^{f_1 a}$, $l = f_1 a$, откуда или $a = 1$ и, значит, $\mathfrak{p}$ остается простым идеалом и в K, или $a = l$ и $\mathfrak{p}$ есть l-я степень простого идеала $\mathfrak{P}$. Либо же $\mathfrak{P}$ отличен от всех своих относительно сопряженных идеалов; тогда имеет место разложение

$$\mathfrak{p} = \mathfrak{P}^{a_0}(s\mathfrak{P})^{a_1} \ldots (s^{l-1}\mathfrak{P})^{a_{l-1}}$$

с некоторыми показателями $a, a_1, \ldots, a_{l-1}$. Производя подстановки $s, s^2, \ldots, s^{l-1}$, мы получаем

$$a = a_1 = \ldots = a_{l-1}$$

и

$$\mathfrak{p} = (\mathfrak{P} \cdot s\mathfrak{P} \ldots s^{l-1}\mathfrak{P})^a = \mathfrak{p}^{f_1 a},$$

$$1 = f_1 a, \quad a = f_1 = 1.$$

В этом случае $\mathfrak{p}$ есть произведение l различных сопряженных идеалов $\mathfrak{P}, s\mathfrak{P}, \ldots, s^{l-1}\mathfrak{P}$, имеющих каждый относительную степень 1.

Теорема 118. *Пусть простой идеал $\mathfrak{p}$ входит множителем в число μ точно a раз. Если при этом a не делится на l, то $\mathfrak{p}$ является l-й степенью простого идеала в K: $\mathfrak{p} = \mathfrak{P}^l$. Если же $a = 0$ и $\mathfrak{p}$ не входит в l, то $\mathfrak{p}$ разлагается в K в произведение l различных простых идеалов, когда сравнение*

$$\mu \equiv \xi^l \pmod{\mathfrak{p}}$$

имеет целое решение ξ в k, и остается простым идеалом в K в противном случае.

Доказательство. I. Если a не делится на l, то мы можем считать $a=1$. В самом деле, взяв целое число β из k, делящееся на $\mathfrak{p}$, но не делящееся на $\mathfrak{p}^2$, мы можем, в силу условия $(a, l)=1$, так подобрать целые рациональные числа x, y, чтобы $\mu^*=\mu^x\beta^{ly}$ делилось на $\mathfrak{p}$, но не на $\mathfrak{p}^2$; при этом $\sqrt[l]{\mu^*}$, в силу замечания, сделанного на стр. 152, будет порождать то же относительное поле, что и $\sqrt[l]{\mu}$. А для этого μ^* показатель a равен 1, так что мы можем предполагать, что это имеет место уже для μ. Теперь, возводя идеал

$$\mathfrak{P}=(\mathfrak{p}, \sqrt[l]{\mu})$$

в l-ю степень, получаем $\mathfrak{P}^l=(\mathfrak{p}^l, \mu)=\mathfrak{p}$. В силу теоремы 108, $\mathfrak{P}$ есть тогда простой идеал в K.

II. Пусть теперь a делится на l. Тогда мы заменим μ таким $\mu^*=\mu\beta^{-a}=\mu(\beta^{-\frac{a}{l}})^l$, которое порождает то же поле $K=K(\sqrt[l]{\mu^*}; k)$ и для которого показатель a равен нулю.

II 1. $\mathfrak{p}$ не делит ни l, ни μ, и существует целое ξ из k, для которого

$$\mu\equiv\xi^l \pmod{\mathfrak{p}}.$$

В силу этого $\mathfrak{p}$ делит произведение

$$\mu-\xi^l=(\mathrm{M}-\xi)(s\mathrm{M}-\xi)\ldots(s^{l-1}\mathrm{M}-\xi). \tag{81}$$

Но $\mathfrak{p}$ не делит ни один из множителей этого произведения, так как, будучи идеалом в k, $\mathfrak{p}$ должен был бы делить тогда все (относительно сопряженные) множители, следовательно, также разность двух из них, т. е.

$$\mathfrak{p}\,|\,(\zeta^a\mathrm{M}-\zeta^b\mathrm{M}),\quad \mathfrak{p}\,|\,(\zeta^a-\zeta^b)\,\mathrm{M};$$

так как, однако, $\mathfrak{p}$ взаимно прост с M, то он должен был бы делить $\zeta^a-\zeta^b$ и, значит, в силу леммы, делить также l, вопреки нашему предположению. Таким образом $\mathfrak{p}$ не является простым идеалом в K. Из наших рассмотрений явствует, кроме того, что

$$\mathfrak{P}=(\mathfrak{p}, M-\xi)$$

есть отличный от 1 делитель $\mathfrak{p}$, отличный от всех своих относительно сопряженных; очевидно $\mathfrak{p}=\mathfrak{P}\cdot s\mathfrak{P}\ldots s^{l-1}\mathfrak{P}$.

II 2. $\mathfrak{p}$ не делит ни l, ни μ, и разлагается на l различных множителей в K:

$$\mathfrak{p}=\mathfrak{P}\cdot s\mathfrak{P}\ldots s^{l-1}\mathfrak{P}.$$

Как показывает это равенство, $\mathfrak{P}$ имеет относительную степень 1; поэтому, в силу теоремы 110, каждое число из K сравнимо по модулю $\mathfrak{P}$ с некоторым числом из k, следовательно, в k существует такое ξ, что

$$\mathrm{M}\equiv\xi \pmod{\mathfrak{P}}.$$

Поэтому относительная норма числа $\mathrm{M}-\xi$, т. е. $\mu-\xi^l$, делится на относительную норму идеала $\mathfrak{P}$, т. е.

$$\mu \equiv \xi^l \pmod{\mathfrak{p}}.$$

Тем самым теорема 117 доказана.

Таким образом аналогично тому как разложение простого числа p в квадратичном поле $K(\sqrt{d})$ связано с квадратичными вычетами в $k(1)$, разложение $\mathfrak{p}$ при переходе к $K\sqrt[l]{\mu}; k)$ связано, как мы видим, с l-ми степенными вычетами в поле k.

Вопрос о разложении множителей числа l разрешается следующей теоремой:

Теорема 119. *Пусть* $\mathfrak{l}$ *— простой множитель* $1-\zeta$, *входящий в* $1-\zeta$ *точно в* a*-й степени:* $1-\zeta=\mathfrak{l}^a\mathfrak{l}_1$, $(\mathfrak{l},\mathfrak{l}_1)=1$; *пусть* $\mathfrak{l}$ *не входит в* μ. *Точка* $\mathfrak{l}$ *распадается в поле* $K(\sqrt[l]{\mu}; k)$ *на* l *различных множителей, если сравнение*

$$\mu \equiv \xi^l \pmod{\mathfrak{l}^{al+1}} \tag{82}$$

имеет решение ξ *в* k. *Если же разрешимо сравнение*

$$\mu \equiv \xi^l \pmod{\mathfrak{l}^{al}}, \tag{83}$$

а сравнение (82) *неразрешимо, то* $\mathfrak{l}$ *остается и в* K *простым идеалом. Наконец, если также сравнение* (83) *неразрешимо, то* $\mathfrak{l}$ *является* l*-й степенью простого идеала в* K.

1. Покажем, что разрешимость сравнения (82) равносильна факту распадения $\mathfrak{l}$ на различные множители в K. Пусть $\mathfrak{l}=\mathfrak{L}\cdot s\mathfrak{L}\ldots s^{l-1}\mathfrak{L}$, где все множители отличны друг от друга. Отсюда, как и в доказательстве теоремы 110, вытекает, что каждое целое число из K сравнимо по любой степени $\mathfrak{L}$ с некоторым целым числом из k. Таким образом, в частности, для каждого натурального b существует такое ξ из k, что

$$\mathrm{M}-\xi \equiv 0 \quad (\mathfrak{L}^b);$$

тогда относительная норма числа $\mathrm{M}-\xi$ делится на $N_k(\mathfrak{L})^b=\mathfrak{l}^b$ значит, сравнение $\mu\equiv\xi\mathfrak{l} \pmod{\mathfrak{l}^b}$ разрешимо для любого натурального b.

Пусть теперь, обратно, $\mu\equiv\xi^l \pmod{\mathfrak{l}^{al+1}}$. Пусть ρ — нецелое число из k, представимое в виде отношения $\rho=\frac{\mathfrak{r}}{\mathfrak{l}^a}$, где числитель $\mathfrak{r}$ — целый идеал, взаимно простой с $\mathfrak{l}$. Тогда прежде всего число $\mathrm{A}=\rho(\mathrm{M}-\xi)$ является целым. В самом деле, оно является корнем полинома

$$f(x)=(x+\rho\xi)^l-\rho^l\mu=$$
$$=x^l+\binom{l}{1}\rho\xi x^{l-1}+\ldots+\binom{l}{l-1}\rho^{l-1}\xi^{l-1}x+\rho^l(\xi^l-\mu);$$

но биномиальные коэфициенты делятся на l и, значит, в силу (80) и предположения относительно $\mathfrak{l}$, на $\mathfrak{l}^{a(l-1)}$, следовательно, все $\binom{l}{m}\rho^m$

$(m=1, \ldots, l-1)$ — целые; свободный же член является целым в силу (82). Положим $\mathfrak{L}=(\mathfrak{l}, A)$. Этот идеал отличен от 1, так как $N_k(A)=\rho^l(\xi^l-\mu)$ делится на $\mathfrak{l}$. Далее, все сопряженные идеала $\mathfrak{L}$ взаимно просты, так как в $(\mathfrak{L}, s^m\mathfrak{L})$ содержится число $A-s^mA=\rho M(1-\zeta^m)$, взаимно простое с $\mathfrak{l}$. Таким образом $\mathfrak{l}$ содержит в K делитель, взаимно простой со всеми своими сопряженными и, значит, в силу теоремы 117, распадается на l различных простых множителей.

II. Если разрешимо сравнение $\mu\equiv\xi^l \pmod{\mathfrak{l}^{al}}$, то, так же как выше, убеждаемся в том, что $A=\rho(M-\xi)$ — целое число из K, относительная диферента которого $\delta_k(A)=\rho^{l-1}M^{l-1}\prod_{m=1}^{l-1}(1-\zeta^m)$ взаимно проста с $\mathfrak{l}$. Поэтому, в силу теоремы 114, $\mathfrak{l}$ не может быть l-й степенью простого идеала в K; если вместе с тем сравнение (82) неразрешимо, то, в силу доказанного в I, $\mathfrak{l}$ не может распадаться на l различных множителей, значит, согласно теореме 117, $\mathfrak{l}$ остается в этом случае простым идеалом и в K.

III. Пусть сравнение $\mu\equiv\xi^l \pmod{\mathfrak{l}^{al}}$ **неразрешимо и** u — высший показатель, для которого разрешимо сравнение $\mu\equiv\xi^l \pmod{\mathfrak{l}^u}$. Здесь во всяком случае $u\geqslant 1$, так как, в силу теоремы Ферма, $\mu\equiv\mu^{N(\mathfrak{l})}=\mu^{l^f} \pmod{\mathfrak{l}}$ или $\mu\equiv(\mu^{l^f-1})^l \pmod{\mathfrak{l}}$. Покажем, что u не делится на l. Для этого, принимая во внимание максимальность показателя u, достаточно доказать, что из разрешимости сравнения

$$\mu\equiv\xi^l \pmod{\mathfrak{l}^{bl}},\quad 0<b\leqslant a-1,$$

вытекает разрешимость этого сравнения и по модулю $\mathfrak{l}^{bl+1}$. Пусть λ — целое число в k, делящееся на $\mathfrak{l}^b$, но не делящееся на $\mathfrak{l}^{b+1}$; тогда, при $b\leqslant a-1$, для каждого целого ω имеет место сравнение

$$(\xi+\lambda\omega)^l\equiv\xi^l+\lambda^l\omega^l \pmod{\mathfrak{l}^{bl+1}},$$

и так как ω^l может представлять любой класс по модулю $\mathfrak{l}$, то мы можем подобрать ω таким образом, чтобы удовлетворялось сравнение

$$\mu-(\xi+\lambda\omega)^l\equiv 0 \pmod{\mathfrak{l}^{bl+1}}.$$

Таким образом, поскольку $u<al$, u не делится на l. Пусть $u=bl+v$ $(0<v\leqslant l-1,\ b<a)$ и ρ — нецелое число из k, представимое в виде отношения $\rho=\frac{\mathfrak{r}}{\mathfrak{l}^b}$, где числитель $\mathfrak{r}$ — целый идеал, взаимно простой с $\mathfrak{l}$. Так же, как выше, убеждаемся в том, что $A=\rho(M-\xi)$ есть целое число, не делящееся на $\mathfrak{l}$, если $\mu\equiv\xi^l \pmod{\mathfrak{l}^u}$, причем, однако, $N_k(A)$ делится на $\mathfrak{l}^v$. Следовательно, $\mathfrak{L}=(\mathfrak{l}, A)$ есть идеал в K, отличный от $\mathfrak{l}$ и (1), поэтому $\mathfrak{l}$ не является простым в K; и так как случай I здесь не имеет места, то, в силу теоремы 117, $\mathfrak{l}$ может быть лишь l-й степенью простого идеала в K.

Из теорем 118 и 119 вытекает

Теорема 120. *Относительный дискриминант поля* $K(\sqrt[l]{\mu}; k)$ *относительно* k *тогда и только тогда равен* 1, *когда* μ *есть* l*-я сте-*

пень идеала из k и одновременно, в предположении, что μ выбрано взаимно простым с l, сравнение $\mu \equiv \xi^l \pmod{(1-\zeta)^l}$ разрешимо в k.

В самом деле, в силу теорем 114, 115 и 117 и определения относительного дискриминанта (см. стр. 149), относительный дискриминант поля $K(\sqrt[l]{\mu}; k)$ тогда и только тогда будет равен 1, когда каждый простой идеал поля k при переходе к K либо остается простым, либо распадается на различные простые множители. Поскольку в теоремах 118 и 119 рассмотрены все возможные случаи разложения простых идеалов $\mathfrak{p}$ из k в поле K, остается отбросить те из этих случаев, которые приводят к разложению вида $\mathfrak{p} = \mathfrak{P}^l$. Из теоремы 118 прежде всего явствует, что нужно отбросить случай, когда хотя бы один простой множитель входит в μ в степени, не кратной l. Таким образом μ должно быть l-й степенью целого идеала из k. В этом случае, как показывает теорема 118, все простые $\mathfrak{p}$, не входящие в l, при переходе к K либо остаются простыми, либо распадаются на различные простые множители, так что остается рассмотреть лишь простые множители $\mathfrak{l}$ числа l. В силу (80), это будут простые множители числа $1-\zeta$. Теорема 119 показывает, что здесь приходится отбросить лишь случай, когда хотя бы для одного такого $\mathfrak{l}$ неразрешимо сравнение (83) (причем предполагается, что μ не делится на идеалы $\mathfrak{l}$, т. е. взаимно просто с l). А это приводит ко второму утверждению доказываемой теоремы.

Как уже было указано на стр. 132, дискриминант поля никогда не может быть равен ± 1. Фундаментальное значение для всей арифметики имеет то обстоятельство, что относительные дискриминанты (относительно полей, отличных от $k(1)$) вполне могут быть равны 1. Открытие этого факта принадлежит Кронекеру. Гильберт понял значение таких полей для общей арифметики и построил на этом теорию законов взаимности высших степеней. Как оказалось, имеет место теорема [1]), что поле $K(\sqrt[l]{\mu}; k)$ с относительным дискриминантом 1 существует тогда и только тогда, когда число классов идеалов [2]) в k делится на l. Относительное поле K, обладающее этим свойством, называется *гильбертовым полем классов k.*

---

[1]) По поводу этих вопросов см. §§ 54—58 в гильбертовом отчете о теории алгебраических чисел, а также основоположную работу Гильберта „Über die Theorie der relativ Abelschen Zahlkörper“ (Acta mathematica, t. 26 (1902), и Göttinger Nachrichten, 1898). Наметки Гильберта были затем подробно развиты в большом количестве работ и частично доведены до завершающих результатов Фуртвенглером (две важнейшие из его работ: „Allgemeiner Existenzbeweis fur den Klassenkörper eines beliebigen algebraischen Zahlkörpers“, Math. Ann., Bd. 63 (1906), и „Die Reziprozitätsgesetze fur Potenzreste mit Primzahlexponenten in algebraischen Zahlkörpern“ I, II, III, Math. Ann., Bd. 67, 72, 74 (1909—1913)).

[2]) В случае $l = 2$ здесь имеется в виду более узкое понятие класса (см. последние параграфы этой книги).

ГЛАВА VI

ВВЕДЕНИЕ ТРАНСЦЕНДЕНТНЫХ МЕТОДОВ В ИССЛЕДОВАНИЕ АРИФМЕТИКИ ЧИСЛОВЫХ ПОЛЕЙ

§ 40. Плотность идеалов в классе

В 1840 г. Дирихле в своей проложившей новые пути работе „Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres“ (Crelles Journal, Bd. 19; Werke, Bd. I, стр. 411 и сл.) показал, как можно применить могущественные методы анализа непрерывных переменных к решению чисто арифметических проблем. Эти методы стали приобретать все более и более возрастающее значение для арифметики числовых полей. Еще и поныне проблема числа классов и проблема распределения простых идеалов доступны лишь этим трансцендентным методам, совершенно не поддаваясь чисто арифметическому исследованию.

В этой главе будет итти речь об обеих названных проблемах и их решении методами Дирихле.

Основной факт, открытый Дирихле [1]), состоит в том, что можно говорить о „плотности“ идеалов в некотором классе идеалов поля K и что эта плотность для всех классов идеалов в K одинакова. Точно этот результат формулируется в виде следующей теоремы:

Теорема 121. *Пусть A — произвольный класс идеалов поля K и $Z(t;\ A)$ — число целых идеалов класса A, нормы которых не превосходят t. Тогда существует предел*

$$\lim_{t\to\infty}\frac{Z(t;\ A)}{t}=\varkappa,$$

причем $\varkappa$ — не зависящее от A определяемое лишь самим полем число

$$\varkappa=\frac{2^{r_1+r_2}\pi^{r_2}R}{w\,|\sqrt{d}\,|}$$

(обозначения — те же, что и в §§ 34, 35).

Доказательство. Пусть $\mathfrak{a}$ — целый идеал из обратного к A класса A^{-1}, так что при умножении каждого идеала из A на $\mathfrak{a}$ полу-

[1]) Дирихле получил свои результаты лишь для квадратичных полей и притом в применении не к идеалам, а к квадратичным формам (см. § 53). На общие алгебраические числовые поля идеи Дирихле перенес Дедекинд.

чается главный идеал. Таким образом для каждого целого идеала $\mathfrak{b}$ из A существует один и только один делящийся на $\mathfrak{a}$ главный идеал (ω) такой, что

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

Следовательно, $Z(t; A)$ оказывается равным числу делящихся на $\mathfrak{a}$ целых попарно неассоциированных чисел ω поля K, нормы которых по абсолютной величине не превосходят $tN(\mathfrak{a})$.

Постараемся теперь найти способ выделения из каждой системы ассоциированных чисел по одному представителю. Пусть $\varepsilon_1, \ldots, \varepsilon_r$, как в § 35, — система r основных единиц. Тогда для каждого отличного от нуля числа ω поля существует однозначно определенная система вещественных чисел $c_1, \ldots, c_r$, такая, что для r первых сопряженных с ω имеют место равенства

$$\ln\left|\frac{\omega^{(p)}}{\sqrt[n]{N(\omega)}}\right| = c_1 \ln|\varepsilon_1^{(p)}| + \ldots + c_r \ln|\varepsilon_r^{(p)}| \quad (p = 1, \ldots, r). \tag{84}$$

Числа c мы будем называть показателями числа ω. Полагая, как и в §§ 34—35, $e_p = 1$, если поле $K^{(p)}$ вещественно, и $e_p = 2$ — в противном случае, мы видим, что вследствие соотношений

$$\sum_{p=1}^{r+1} e_p \ln\left|\frac{\omega^{(p)}}{\sqrt[n]{N(\omega)}}\right| = 0 \quad \text{и} \quad \sum_{p=1}^{r+1} e_p \ln|\varepsilon_k^{(p)}| = 0$$

равенство (84) имеет место также для $p = r+1$, а значит, и для всех вообще сопряженных. Так как теперь, в силу теоремы 100, каждая единица представима в виде

$$\zeta \varepsilon_1^{m_1} \varepsilon_2^{m_2} \ldots \varepsilon_r^{m_r},$$

где ζ — один из w корней из 1, содержащихся в поле K, а m_i — целые рациональные числа, то система ассоциированных ω имеет показатели

$$c_1 + m_1, \; c_2 + m_2, \; \ldots, \; c_r + m_r.$$

Тем самым для каждого ω существует ассоциированное число, показатели которого удовлетворяют условиям

$$0 \leqslant c_0 < 1 \quad (i = 1, \ldots, r);$$

при этом среди ассоциированных с ω существует точно w различных чисел такого рода, а именно, w чисел, отличающихся лишь множителями ζ. Отсюда следует что $wZ(t; A)$ равно количеству делящихся на $\mathfrak{a}$ целых чисел ω поля K, удовлетворяющих условиям

$$|N(\omega)| = |\omega^{(1)}\omega^{(2)} \ldots \omega^{(n)}| \leqslant N(\mathfrak{a})\, t, \tag{85}$$

$$\ln\left|\frac{\omega^{(p)}}{\sqrt[n]{N(\omega)}}\right| = \sum_{q=1}^{r} c_q \ln|\varepsilon_q^{(p)}|; \quad 0 \leqslant c_q < 1 \quad (p = 1, \ldots, n). \tag{86}$$

Но для того чтобы ω делилось на $\mathfrak{a}$, необходимо и достаточно, чтобы для некоторых целых рациональных $x_1, \ldots, x_n$ удовлетворялись равенства

$$\omega^{(p)} = \sum_{k=1}^{n} x_k \alpha_k^{(p)} \quad (p = 1, \ldots, n), \tag{87}$$

где $\alpha_1, \ldots, \alpha_n$ — какой-нибудь определенный базис идеала $\mathfrak{a}$. Тем самым $wZ(t; A)$ равно количеству систем целых рациональных $x_1, \ldots, x_n$, где не все x_i равны нулю, удовлетворяющих условиям (85)—(87).

Если теперь для x_i выбраны какие-либо произвольные вещественные значения, то соответствующими $\omega^{(p)}$, если все они отличны от нуля, однозначно определяются, в силу равенств (86), некоторые вещественные c_q. Поэтому, если рассматривать $x_1, \ldots, x_n$ как прямоугольные декартовы координаты точек n-мерного пространства и отбросить сначала точки, лежащие хотя бы на одном многообразии меньшего числа измерений $\omega^{(p)} = 0$, неравенствами (85), (86) выделится некоторая ограниченная область B_t, ибо

$$|\omega^{(p)}| = \sqrt[n]{N(\omega)}\, e^{\sum_{q=1}^{r} c_q \ln |\varepsilon_q^{(p)}|} \leqslant \sqrt[n]{tN(\mathfrak{a})}\, e^{rM} \quad (p = 1, \ldots, n),$$

где M — наибольшее из чисел $\left|\ln |\varepsilon_q^{(p)}|\right|$. Дополним теперь B_t до замкнутой, точно так же ограниченной области B_t^*, присоединяя к B_t те конечные части линейных многообразий $\omega^{(p)} = 0$, в которых удовлетворяются условия

$$|\omega^{(p)}| \leqslant \sqrt[n]{tN(\mathfrak{a})}\, e^{rM} \quad (p = 1, \ldots, n).$$

Число целых точек $x_1, \ldots, x_n$ (т. е. точек с целыми рациональными координатами), содержащихся в этой замкнутой области B_t^*, будет равно числу $wZ(t; A)$, увеличенному на 1 (поскольку засчитывается и нулевая точка). Но *число целых точек этой области ассимптотически равно ее объему.* В самом деле, с помощью подстановки $x_k = y_k \sqrt[n]{t}$ область B_t^* в пространстве x переходит в область B_1^* в пространстве y; целым точкам x соответствуют те точки y, координаты которых имеют вид

$$\frac{\text{целое рациональное число}}{\sqrt[n]{t}},$$

т. е. пространство y оказывается разбитым на кубики с длиной ребер $\frac{1}{\sqrt[n]{t}}$, и по определению объема мы имеем

$$\lim_{t\to\infty} \frac{wZ(t; A)}{t} = \int_{(B_1^*)} \ldots \int dy_1 \ldots dy_n = J,$$

где интегрирование распространяется на определенную выше область B_1^*. Полагая теперь

$$\omega^{(p)} = \sum_{k=1}^{n} y_k \alpha_k^{(p)} \quad (p = 1, \ldots, n),$$

мы видим, что эта область определяется следующими неравенствами

$$0 < |\omega^{(1)} \ldots \omega^{(n)}| \leqslant N(\mathfrak{a}),$$

$$\ln \left| \frac{\omega^{(p)}}{\sqrt[n]{N(\omega)}} \right| = \sum_{q=1}^{r} c_q \ln |\varepsilon_q^{(p)}|, \text{ где } 0 \leqslant c_q < 1 \quad (p, q = 1, \ldots, r),$$

или

$$|\omega^{(p)}| \leqslant e^{rM} \sqrt[n]{N(\mathfrak{a})} \text{ и хотя бы для одного } p \ \omega^{(p)} = 0.$$

Так как последним условием выделяются лишь многообразия низшего числа измерений, то соответствующая часть области ничего не вносит в значение рассматриваемого n-кратного интеграла, и мы можем поэтому совсем не принимать указанного условия в расчет.

Для вычисления интеграла J введем вместо y в качестве переменных интеграции вещественные и мнимые части величин $\omega^{(p)}$. Положим

$$z_p = \omega^{(p)} \text{ для } p = 1, \ldots, r_1,$$

$$z_p + i z_{p+r_2} = \omega^{(p)} \text{ для } p = r_1 + 1, \ldots, r_1 + r_2,$$

так что (как при доказательстве теоремы 95)

$$\left| \frac{\partial (z_1, \ldots, z_n)}{\partial (y_1, \ldots, y_n)} \right| = 2^{-r_2} N(\mathfrak{a}) |\sqrt{d}|.$$

Выражая тогда z_p и z_{p+r_2} в тригонометрическом виде:

$$z_p = \rho_p \cos \varphi_{p-r_1} \quad (\rho_p > 0, \ 0 \leqslant \varphi_{p-r_1} < 2\pi, \ p = r_1 + 1, \ldots, r_1 + r_2),$$

$$z_{p+r_2} = \rho_p \sin \varphi_{p-r_1},$$

и полагая для симметрии

$$z_p = \rho_p \quad (p = 1, \ldots, r_1),$$

получаем

$$\frac{\partial (z_1, \ldots, z_n)}{\partial (\rho_1, \ldots, \rho_{r+1}, \varphi_1, \ldots, \varphi_{r_2})} = \rho_{r_1+1} \ldots \rho_{r_1+r_2},$$

и область B_1 в новых переменных определяется условиями

$$0 < \prod_{p=1}^{r+1} |\rho_p|^{e_p} \leqslant N(\mathfrak{a}),$$

$$\ln |\rho_p| = \frac{1}{n} \ln \prod_{k=1}^{r+1} |\rho_k|^{e_k} + \sum_{q=1}^{r} c_q \ln |\varepsilon_q^{(p)}|, \quad 0 \leqslant c_q < 1,$$

$$\rho_p > 0 \text{ и } 0 \leqslant \varphi_{p-r_1} < 2\pi \text{ для } p = r_1 + 1, \ldots, r_1 + r_2.$$

Интегрирования по φ выполняются непосредственно, а при интегрировании по ρ мы можем рассматривать лишь положительные значения переменных $\rho_1, \ldots, \rho_{r_1}$, приписав перед интегралом множитель 2^{r_1}. Мы получаем, таким образом,

$$J = \frac{2^{r_1+r_2}\pi^{r_2}}{N(\mathfrak{a})\,|\sqrt{d}\,|} \int \ldots \int 2^{r_2}\rho_{r_1+1}\ldots\rho_{r_1+r_2}\,d\rho_1\ldots d\rho_{r+1} =$$

$$= \frac{2^{r_1+r_2}\pi^{r_2}}{N(\mathfrak{a})\,|\sqrt{d}\,|} \int \ldots \int dv_1\ldots dv_{r+1},$$

где $v_k = \rho_k^{e_k}$. При этом область изменения переменных v определяется следующими условиями:

$$0 < v_1 v_2 \ldots v_{r+1} \leqslant N(\mathfrak{a}), \quad v_p > 0,$$

$$\ln v_p = \frac{e_p}{n} \ln (v_1 \ldots v_{r+1}) + e_p \sum_{q=1}^{r} c_q \ln |\varepsilon_q^{(p)}|, \quad 0 \leqslant c_q < 1.$$

Наконец, вводим вместо v в качестве новых переменных $c_1, \ldots, c_r$ и

$$u = v_1 v_2 \ldots v_{r+1},$$

так что

$$\ln v_p = \frac{e_p}{n} \ln u + e_p \sum_{q=1}^{r} c_q \ln |\varepsilon_q^{(p)}|,$$

$$\frac{\partial(v_1, \ldots, v_{r+1})}{\partial(u, c_1, \ldots, c_r)} = \frac{v_1 v_2 \ldots v_{r+1}}{u} \begin{vmatrix} e_1 \ln|\varepsilon_1^{(1)}| & \ldots & e_1 \ln|\varepsilon_r^{(1)}| \\ \ldots & \ldots & \ldots \\ e_r \ln|\varepsilon_1^{(r)}| & \ldots & e_r \ln|\varepsilon_r^{(r)}| \end{vmatrix} = \pm R.$$

Тогда получаем

$$J = \frac{2^{r_1+r_2}\pi^{r_2}}{N(\mathfrak{a})\,|\sqrt{d}\,|} R \int_0^{N(a)} du \int_{0 \leqslant c_q < 1} \ldots \int dc_1 \ldots dc_r = \frac{2^{r_1+r_2}\pi^{r_2} R}{|\sqrt{d}\,|},$$

что и завершает доказательство теоремы 121.

§ 41. Плотность идеалов и число классов

Выписывая доказанное в предыдущем параграфе предельное соотношение для всех классов идеалов поля K и суммируя, мы приходим к соотношению Дирихле-Дедекинда между плотностью целых идеалов поля и числом его классов, выражаемому следующей теоремой:

Теорема 122. *Пусть $Z(t)$ означает число всех целых идеалов поля, нормы которых не превосходят t. Имеет место соотношение*

$$\lim_{t\to\infty}\frac{Z(t)}{t}=h\varkappa, \tag{88}$$

где h — число классов поля.

Но число $Z(t)$, в определении которого понятие класса идеалов не участвует, можно вычислить и другим путем, а именно, основываясь на законах разложения в данном поле рациональных простых чисел. Тем самым устанавливается связь между числом классов и законами разложения, и в некоторых случаях, исходя из этого, можно вывести замечательно простое выражение для числа классов, к которому до сих пор не удалось притти никаким другим путем.

Обозначим через $F(m)$ число целых идеалов поля, нормы которых равны положительному числу m. Тогда, очевидно,

$$Z(t)=\sum_{m=1}^{t}F(m),$$

причем запись $\sum_{m=1}^{t}$ означает, что m пробегает все целые рациональные числа, удовлетворяющие условию $1\leqslant m\leqslant t$. Далее,

$$F(ab)=F(a)F(b), \quad \text{если} \quad (a,\ b)=1. \tag{89}$$

В самом деле, из каждой пары целых идеалов $\mathfrak{a}$, $\mathfrak{b}$ с $N(\mathfrak{a})=a$, $N(\mathfrak{b})=b$ получается идеал $\mathfrak{c}=\mathfrak{ab}$ с $N(\mathfrak{c})=ab$. Обратно, пусть $\mathfrak{c}$ — целый идеал с нормой ab. Положим

$$(\mathfrak{c},\ a)=\mathfrak{a}_1, \quad (\mathfrak{c},\ b)=\mathfrak{b}_1. \tag{90}$$

Перемножая эти идеалы, мы получим

$$\mathfrak{a}_1\mathfrak{b}_1=(\mathfrak{c}^2,\ \mathfrak{c}a,\ \mathfrak{c}b,\ ab)=\mathfrak{c}\left(\mathfrak{c},\ a,\ b,\ \frac{ab}{\mathfrak{c}}\right)=\mathfrak{c}.$$

С другой стороны, переходя в (90) к сопряженным, мы получаем, что $N(\mathfrak{a}_1)$ есть делитель числа a^n и, значит, взаимно прост с b, и точно так же $N(\mathfrak{b}_1)$ взаимно прост с a; так как в то же время $N(\mathfrak{a}_1)N(\mathfrak{b}_1)=ab$, то $N(\mathfrak{a}_1)=a$, $N(\mathfrak{b}_1)=b$, и, значит, $\mathfrak{c}$ разложено на два множителя, нормы которых равны соответственно a и b. Это и доказывает справедливость соотношения (89).

Таким образом применением этой формулы вычисление $F(m)$ сводится к вычислению $F(p^k)$, где p — простые числа.

Техника определения $F(p^k)$ и, значит, $F(m)$ значительно облегчается введением новой функции, с помощью которой предельный процесс (88) преобразуется в более удобный для вычисления предельный процесс. Этой функцией является дзета-функция Дирихле-Дедекинда.

§ 42. Дзета-функция Дедекинда

Рядом Дирихле называют ряд вида

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

где $a_1, a_2, \ldots$ — заданная числовая последовательность, s — переменная, которая будет во всем дальнейшем считаться вещественной, а под n^s понимается положительное значение степени. Числа a_n называются коэфициентами ряда. Ряд Дирихле, в случае сходимости, представляет некоторую функцию от s.

Лемма a). *Ряд* $\sum_{n=1}^{\infty} \frac{1}{n^s}$ *при* $s > 1$ *сходится и представляет непрерывную функцию, так называемую риманову дзета-функцию* $\zeta(s)$; *далее,*

$$\lim_{s \to 1} (s-1)\zeta(s) = 1.$$

Действительно, очевидно

$$\int_n^{n+1} \frac{dx}{x^s} < \frac{1}{n^s} < \int_{n-1}^{n} \frac{dx}{x^s} \quad (n > 1).$$

Это показывает, что ряд $\sum_{n=1}^{\infty} \frac{1}{n^s}$ сходится одновременно с интегралом $\int_1^{\infty} \frac{dx}{x^s}$, т. е. для всех $s > 1$, и только для них. Как ряд с непрерывными положительными членами, он представляет, в силу известной теоремы Дини, непрерывную функцию; эту функцию обозначают $\zeta(s)$. При этом

$$\int_1^{\infty} \frac{dx}{x^s} < \zeta(s) < \int_1^{\infty} \frac{dx}{x^s} + 1$$

или

$$1 < (s-1)\zeta(s) < s,$$

откуда вытекает и утверждаемое в лемме предельное соотношение.

Лемма b). *Положим* $S(m) = a_1 + \ldots + a_m$, *следовательно,* $a_n = S(n) - S(n-1)$. *Если тогда существует такое число* σ (> 0), *что*

$$\left| \frac{S(m)}{m^{\sigma}} \right| < A \quad (m = 1, 2, \ldots), \tag{91}$$

где A — *постоянная, не зависящая от* m, *то при* $s > \sigma$ *ряд* $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ *сходится и представляет непрерывную функцию от* s.

Действительно, для положительных целых m, h

$$\sum_{n=m}^{m+h}\frac{a_n}{n^s}=\sum_{n=m}^{m+h}\frac{S(n)-S(n-1)}{n^s}=$$

$$=\frac{S(m+h)}{(m+h)^s}-\frac{S(m-1)}{m^s}+\sum_{n=m}^{m+h-1}S(n)\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right).$$

Так как

$$\frac{1}{n^s}-\frac{1}{(n+1)^s}=s\int_n^{n+1}\frac{dx}{x^{s+1}},$$

то при $s>\sigma$, в силу (91), получаем

$$\left|\sum_{n=m}^{m+h}\frac{a_n}{n^s}\right|<\frac{2A}{m^{s-\sigma}}+As\int_m^{\infty}\frac{dx}{x^{s-\sigma+1}}=\frac{2A}{m^{s-\sigma}}+\frac{As}{s-\sigma}\frac{1}{m^{s-\sigma}}.$$

Отсюда явствует, что рассматриваемый ряд сходится для всех $s>\sigma$, и притом равномерно для всех $s\geqslant\sigma+\delta$ при любом фиксированном положительном δ и, значит, представляет в области $s>\sigma$ непрерывную функцию от s.

Лемма c) *Если, в обозначениях предыдущей леммы,*

$$\lim_{m\to\infty}\frac{S(m)}{m}=c,$$

то при приближении к $s=1$ *справа* $(s>1)$

$$\lim_{s\to 1}(s-1)\sum_{n=1}^{\infty}\frac{a_n}{n^s}=c.$$

В самом деле, в силу леммы b), ряд сходится при $s>1$. Положим

$$S(n)=cn+\varepsilon_n n,$$

так что, в силу предположения, $\lim\limits_{n\to\infty}\varepsilon_n=0$, и обозначим сумму рассматриваемого ряда через $\varphi(s)$. Тем же путем, что и выше, получаем для $s>1$

$$|\varphi(s)-c\zeta(s)|=s\left|\sum_{n=1}^{\infty}n\varepsilon_n\int_n^{n+1}\frac{dx}{x^{s+1}}\right|<s\sum_{n=1}^{\infty}|\varepsilon_n|\int_n^{n+1}\frac{dx}{x^s}.$$

Но для каждого положительного δ существует такое целое число N что $|\varepsilon_n|<\delta$ для всех $n\geqslant N$. Выберем, кроме того, такое число C

чтобы для всех n имело место неравенство $|\varepsilon_n| < C$. Тогда мы будем иметь

$$|(s-1)\varphi(s) - c(s-1)\zeta(s)| <$$
$$< Cs(s-1)\sum_{n=1}^{N-1}\int_n^{n+1}\frac{dx}{x} + \delta s(s-1)\sum_{N}^{\infty}\int_n^{n+1}\frac{dx}{x^s} <$$
$$< Cs(s-1)\ln N + \delta s(s-1)\int_N^{\infty}\frac{dx}{x^s}.$$

Так как последнее выражение при $s \to 1$ сходится к δ, то, в силу произвольности δ,

$$\lim_{s\to 1}\{(s-1)\varphi(s) - c(s-1)\zeta(s)\} = 0,$$

что, в силу леммы a), и доказывает лемму c).

Теперь каждому алгебраическому числовому полю k мы отнесем функцию непрерывного переменного s — так называемую дзета-функцию поля k

$$\zeta_k(s) = \sum_{\mathfrak{a}}\frac{1}{N(\mathfrak{a})^s}, \tag{92}$$

где $\mathfrak{a}$ пробегает все целые отличные от нуля идеалы поля k. Эти функции были первоначально введены Дирихле для квадратичных полей, а затем Дедекинд распространил их определение на произвольные поля k. С помощью функции $F(m)$ из предыдущего параграфа мы можем записать ряд (92) также в виде

$$\zeta_k(s) = \sum_{n=1}^{\infty}\frac{F(n)}{n^s};$$

тогда из предельной теоремы 122 и лемм b) и c) получается следующая теорема:

Теорема 123. *Ряд* (92) *сходится при* $s > 1$. *Функция* $\zeta_k(s)$ *для этих значений* s *непрерывна. Имеет место предельное соотношение*

$$\lim_{s\to 1}(s-1)\zeta_k(s) = hx.$$

Выражая $\zeta_k(s)$ существенно другим путем, а именно, через посредство простых идеалов поля k, мы получаем возможность вычислить из найденного предельного соотношения число классов h.

Теорема 124. *При* $s > 1$ *имеет место равенство*

$$\zeta_k(s) = \prod_{\mathfrak{p}}\frac{1}{1-\frac{1}{N(\mathfrak{p})^s}}, \tag{93}$$

где $\mathfrak{p}$ *пробегает все различные простые идеалы поля* k.

Прежде всего произведение в (93) сходится при $s > 1$, ибо ряд $\sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s}$, как составная часть ряда для $\zeta_k(s)$, сходится. Для отдельных множителей этого произведения мы получаем сходящиеся ряды из положительных членов

$$\frac{1}{1-N(\mathfrak{p})^{-s}} = 1 + \frac{1}{N(\mathfrak{p})^s} + \frac{1}{N(\mathfrak{p}^2)^s} + \cdots \tag{94}$$

Перемножая формально эти выражения для всех $\mathfrak{p}$, мы получим ряд с членами

$$\frac{1}{N(\mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\ldots\mathfrak{p}_r^{a_r})^s},$$

где под знак нормы входит каждое произведение степеней простых идеалов точно один раз. Но по основной теореме теории идеалов мы получим в этой форме каждый целый идеал поля k точно один раз, т. е. формальное перемножение всех выражений (94) дает ряд для $\zeta_k(s)$. А так как при $s > 1$ ряды для отдельных множителей, равно как произведение и ряд для $\zeta_k(s)$, абсолютно сходятся, то из формального совпадения рядов вытекает и равенство сумм рядов, чем формула (93) и доказана.

Теорема 125. *Определение числа классов h сводится (по Дедекинду) с помощью соотношения*

$$h\varkappa = \lim_{s\to 1}(s-1)\prod_{\mathfrak{p}}\frac{1}{1-\frac{1}{N(\mathfrak{p})^s}} \tag{95}$$

к определению простых идеалов поля.

Эта фундаментальная формула послужит исходным пунктом для дальнейших рассмотрений. В тех полях, где известно разложение рациональных простых чисел p на простые идеалы, из нее можно будет вывести удобное для употребления выражение для числа классов (см. § 51, где проведено вычисление для квадратичного поля). Обратно, из теорем 123 и 124, используя лишь тот факт, что $h\varkappa$ во всяком случае отлично от нуля, мы сможем сделать некоторые заключения о простых идеалах поля. Об этом будет итти речь в следующем параграфе.

§ 43. Распределение простых идеалов первой степени, в частности, рациональных простых чисел в арифметических прогрессиях

Так как $h\varkappa$ отлично от нуля, то теорема 123 показывает, что дедекиндова дзета-функция $\zeta_k(s)$ при $s \to 1$ есть бесконечно большая величина первого порядка, так что

$$\ln \zeta_k(s) = \ln \frac{1}{s-1} + g(s), \tag{96}$$

где $g(s)$ при $s \to 1$ остается ограниченной функцией. Но тогда из представления (93) следует

ТЕОРЕМА 126. *Если* $\mathfrak{p}_1$ *пробегает лишь различные простые идеалы первой степени в* k, *то при* $s > 1$

$$\sum_{\mathfrak{p}_1} \frac{1}{N(\mathfrak{p}_1)^s} = \ln \frac{1}{s-1} + g_1(s), \tag{97}$$

где $g_1(s)$ *при* $s \to 1$ *остается ограниченной. Таким образом в* k *существует бесконечное множество простых идеалов первой степени.*

Доказательство. Пусть $\mathfrak{p}_f$ пробегает различные простые идеалы степени f ($f = 1, \ldots, n$; разумеется, $\mathfrak{p}_f$ могут вовсе не существовать для некоторых f). Так как в заданное рациональное простое число p входят множителями не больше n различных простых идеалов поля k, то во всяком случае

$$1 \leqslant \prod_{\mathfrak{p}_f} \frac{1}{1 - \frac{1}{N(\mathfrak{p}_f)^s}} \leqslant \prod_{p} \frac{1}{\left(1 - \frac{1}{p^{fs}}\right)^n} = \zeta(fs)^n \quad (s > 1).$$

Это показывает, что часть произведения для $\zeta_k(s)$, распространенная на все $\mathfrak{p}_f$ с $f \geqslant 2$, остается при $s \to 1$ заключенной между двумя фиксированными положительными границами. Поэтому бесконечное возрастание $\zeta_k(s)$ обусловливается единственно лишь простыми идеалами $\mathfrak{p}_1$. При этом, логарифмируя, мы получаем

$$\ln \zeta_k(s) = -\sum_{\mathfrak{p}_1} \ln\left(1 - \frac{1}{N(\mathfrak{p}_1)^s}\right) + f(s), \tag{98}$$

где $f(s)$ также остается ограниченной. Но так как $N(\mathfrak{p}_1) \geqslant 2$, то при $s \geqslant 1$

$$-\ln\left(1 - \frac{1}{N(\mathfrak{p}_1)^s}\right) = \frac{1}{N(\mathfrak{p}_1)^s} + \varphi(\mathfrak{p}_1, s),$$

причем

$$0 \leqslant \varphi(\mathfrak{p}_1, s) = \frac{1}{2}\frac{1}{N(\mathfrak{p}_1)^{2s}} + \frac{1}{3}\frac{1}{N(\mathfrak{p}_1)^{3s}} + \ldots <$$
$$< \frac{1}{N(\mathfrak{p}_1)^{2s}}\left(1 + \frac{1}{2^s} + \frac{1}{4^s} + \ldots\right) < \frac{2}{N(\mathfrak{p}_1)^{2s}};$$

суммируя по $\mathfrak{p}_1$, получаем отсюда

$$0 \leqslant \sum_{\mathfrak{p}_1} \varphi(\mathfrak{p}_1, s) \leqslant 2\sum_{\mathfrak{p}_1} \frac{1}{N(\mathfrak{p}_1)^{2s}} \leqslant 2n \sum_{p} \frac{1}{p^{2s}} \leqslant 2n \sum_{p} \frac{1}{p^2},$$

т. е. сумма $\sum_{\mathfrak{p}_1} \varphi(\mathfrak{p}_1, s)$ при $s \geqslant 1$ ограничена. В соединении с (98) мы получаем отсюда, что разность

$$\ln \zeta_k(s) - \sum_{\mathfrak{p}_1} \frac{1}{N(\mathfrak{p}_1)^s}$$

остается ограниченной при $s \to 1$, а тогда, в силу (96), и получается утверждение (97). Таким образом при приближении s к 1 сумма, распространенная на простые идеалы $\mathfrak{p}_1$, становится бесконечно большой и, следовательно, она необходимо должна содержать бесконечное количество членов.

Эта общая теорема, справедливая для всякого алгебраического числового поля, позволяет теперь доказать очень важные факты из арифметики рациональных чисел, относящиеся к распределению простых чисел.

Именно, возьмем в качестве поля k поле корней m-й степени из 1. В силу теоремы 92, в этом поле нормами простых идеалов первой степени служат как раз все, за конечным числом исключений, рациональные простые числа p, удовлетворяющие сравнению $p \equiv 1 \pmod m$. Тем самым из теоремы 126 вытекает:

Теорема 127. *Существует бесконечное множество положительных рациональных простых чисел, удовлетворяющих сравнению* $p \equiv 1 \pmod m$.

Пусть n_0 — степень поля корней m-й степени из 1 (которая, как показано в § 30, не превосходит $\varphi(m)$). Тогда каждое p, удовлетворяющее условию теоремы 127, распадается в k точно на n_0 различных простых идеалов, так что равенство (97) принимает здесь вид

$$n_0 \sum_{p \equiv 1 (m)} \frac{1}{p^s} = \ln \frac{1}{s-1} + g_1(s). \tag{99}$$

Дирихле показал, как отсюда, с помощью относительно простых формальных соображений, можно вывести заключение о наличии простых чисел в остальных классах вычетов $\bmod m$. Для этой цели введем в рассмотрение характеры по модулю m, определенные в § 15.

Теорема 128. *Пусть* $\chi(n)$ — *характер числа* n *по модулю* m. *Тогда при* $s > 1$ *ряд Дирихле*

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

абсолютно сходится, причем имеет место разложение

$$L(s, \chi) = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}}, \tag{100}$$

где p *пробегает все положительные рациональные простые числа. Если* χ — *не главный характер, то бесконечный ряд для* $L(s, \chi)$ *сходится уже при* $s > 0$.

Абсолютная сходимость ряда и произведения при $s > 1$ вытекает из того, что коэфициенты $\chi(n)$ по абсолютной величине не превосхо-

дят 1, поскольку $\chi(n)$ есть либо корень из 1, либо, в случае $(n, m) > 1$, нуль. В силу равенства

$$\chi(ab) = \chi(a)\chi(b),$$

верного для всех пар положительных целых a, b, мы получаем для каждого множителя бесконечного произведения (100) разложение

$$\frac{1}{1 - \frac{\chi(p)}{p^s}} = 1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \ldots;$$

перемножая все эти ряды, мы в силу абсолютной сходимости, так же как и выше при доказательстве теоремы 124, приходим к формуле (100).

Если, наконец, χ не есть главный характер $\chi_1 \bmod m$, то, по основному свойству характеров, $\sum_n \chi(n) = 0$, когда n пробегает какую-нибудь полную систему вычетов $\bmod m$. Поэтому для всякого x, $x = ym + r$, где y, r целые и $0 \leqslant r < m$, имеем

$$\left|\sum_{n=1}^{x} \chi(n)\right| = \left|\sum_{n=1}^{ym} \chi(n) + \sum_{n=0}^{r} \chi(n)\right| = \left|\sum_{n=0}^{r} \chi(n)\right| \leqslant m,$$

так что сумма $\sum_{n=1}^{x} \chi(n)$ остается ограниченной при бесконечном возрастании x, и потому, в силу леммы b) предыдущего параграфа, ряд Дирихле для $L(s, \chi)$ сходится при $s > 0$. Отсюда, в частности, следует, что функции $L(s, \chi)$ остаются непрерывными в точке $s = 1$, если χ — не главный характер.

Теорема 129. *Для каждого характера* $\chi \bmod m$ *при* $s > 1$

$$\ln L(s, \chi) = \sum_p \frac{f(p)}{p^s} + g(s, \chi),$$

где $g(s, \chi)$ *при* $s \to 1$ *остается ограниченной.*

Определим функцию ln при $s > 0$ сходящимся рядом

$$\ln \frac{1}{1 - \frac{\chi(p)}{p^s}} = \frac{\chi(p)}{p^s} + \frac{1}{2}\frac{\chi(p^2)}{p^{2s}} + \frac{1}{3}\frac{\chi(p^3)}{p^{3s}} + \ldots = \frac{\chi(p)}{p^s} + \frac{f(s, p)}{p^{2s}},$$

где, очевидно,

$$|f(s, p)| \leqslant 1 \quad \text{при} \quad p \geqslant 2, \; s \geqslant 1.$$

Тогда и сумма этих выражений, распространенная по всем положительным простым числам p, будет сходиться при $s > 1$ и представлять поэтому одну из ветвей функции $\ln L(s, \chi)$; для нее и имеет место теорема 129, ибо

$$|g(s, \chi)| = \left|\sum_p \frac{f(s, p)}{p^{2s}}\right| \leqslant \sum_p \frac{1}{p^{2s}}.$$

Для главного характера $\chi = \chi_1$

$$\ln L(s, \chi_1) = \ln \frac{1}{s-1} + H(s), \tag{101}$$

где $H(s)$ остается конечной при $s \geqslant 1$.

В самом деле, беря в (97) в качестве k поле $k(1)$, мы получаем, что разность

$$\sum_p \frac{1}{p^s} - \ln \frac{1}{s-1}$$

при $s \to 1$ остается конечной; с другой стороны, $\chi_1(p)$ отлично от 1 (и именно равно нулю) лишь для конечного множества простых чисел p — тех, которые входят множителями в m. Тем самым равенство (101) и доказано.

Нашей задачей является теперь перейти к суммам, распространенным лишь на простые числа некоторого класса вычетов $\bmod m$. Пусть a — произвольное целое рациональное число, взаимно простое с m, и b — такое целое рациональное число, что

$$ab \equiv 1 \pmod m.$$

Тогда при $s > 1$ имеем

$$\sum_\chi \chi(b) \ln L(s, \chi) = \sum_\chi \chi(b) \sum_p \frac{\chi(p)}{p^s} + \sum_\chi \chi(b)\, g(s, \chi),$$

где $\sum_\chi$ означает суммирование по всем характерам $\bmod m$. Последняя сумма, которую мы обозначим через $f(s)$, во всяком случае остается ограниченной при $s \to 1$. В двойной же сумме имеем

$$\sum_\chi \chi(b)\chi(p) = \sum_l \chi(bp) = \begin{cases} 0, & \text{если } bp \not\equiv 1 \pmod m, \\ \varphi(m), & \text{если } bp \equiv 1 \pmod m \end{cases}$$

и, следовательно, получаем

$$\sum_l \chi(b) \ln L(s, \chi) = \varphi(m) \sum_{p \equiv a \pmod m} \frac{1}{p^s} + f(s), \tag{102}$$

где в правой части суммирование производится по всем положительным простым числам p, сравнимым с $a \bmod m$.

Пусть теперь s стремится к критическому значению 1. Тогда член в левой части (102), образованный с помощью главного характера $\chi = \chi_1$, будет, в силу (101), бесконечно возрастать; если поэтому другие слагаемые в левой части остаются конечными, то также вся сумма в левой части будет безгранично возрастать, и, следовательно, сумма, стоящая в правой части, должна будет содержать бесконечно много членов, т. е. существует бесконечное множество простых чисел d, сравнимых с $a \bmod m$.

Таким образом остающийся еще существенный пункт в ходе идей Дирихле состоит в доказательстве справедливости следующего утверждения:

Если χ не есть главный характер, то при $s \to 1$ величины $\ln L(s, \chi)$ остаются конечными.

Но так как, в силу последней части теоремы 128, эти $L(s, \chi)$ являются непрерывными функциями для всех $s > 0$, то сформулированное утверждение равносильно следующей теореме:

ТЕОРЕМА 130. *Если χ не есть главный характер, то*

$$L(1, \chi) = \lim_{s \to 1} L(s, \chi) \neq 0.$$

Необращение L-рядов в нуль является, однако, непосредственным следствием того, что $\zeta_k(s)$ при $s \to 1$ есть бесконечно большая величина первого порядка. Действительно, из (102) при $a = b = 1$ получаем

$$\sum_{\chi} \ln L(s, \chi) = \varphi(m) \sum_{p \equiv 1 (m)} \frac{1}{p^s} + G(s),$$

что в соединении с доказанным выше соотношением (99) приводит к равенству

$$\sum_{\chi} \ln L(s, \chi) = \frac{\varphi(m)}{n_0} \ln \frac{1}{s-1} + G_1(s), \tag{103}$$

где $G_1(s)$, как и $G(s)$, остается конечной при $s \to 1$. Член суммы в левой части, соответствующий главному характеру χ_1, выражается в виде (101), так что для остальных членов получаем

$$\sum_{\chi \neq \chi_1} \ln L(s, \chi) = \left(\frac{\varphi(m)}{n_0} - 1\right) \ln \frac{1}{s-1} + G_2(s),$$

$$\prod_{\chi \neq \chi_1} L(s, \chi) = \left(\frac{1}{s-1}\right)^{\frac{\varphi(m)}{n_0} - 1} e^{G_2(s)}.$$

Как уже было упомянуто, $\varphi(m) \geqslant n_0$. Теперь, если бы $\varphi(m)$ было больше n_0, то правая часть при приближении s к 1 бесконечно возрастала бы, тогда как произведение в левой части наверное остается конечным, поскольку это уже доказано для отдельных его сомножителей. Таким образом мы прежде всего получаем

$$\varphi(m) = n_0.$$

Но тогда правая часть приводится к $e^{G_2(s)}$ и наверное не может стремиться к нулю, так как $G_2(s)$ остается конечной. То же, значит, справедливо и для произведения в левой части, и так как каждый его сомножитель стремится к конечному пределу, то теорема 130 доказана.

Тем самым, в силу сказанного выше, доказана знаменитая теорема Дирихле:

ТЕОРЕМА 131. *Если $(a, m) = 1$, то существует бесконечное множество положительных простых чисел p, удовлетворяющих сравнению $p \equiv a \pmod m$. Иными словами, арифметическая прогрессия $mx + a$, $x = 1, 2, \ldots$, содержит бесконечное множество простых чисел.*

В качестве побочного результата мы получили при доказательстве этой теоремы равенство

$$\varphi(m) = n_0,$$

т. е. из законов разложения вытекает также точная степень поля корней m-й степени из 1. Тем самым доказано, что установленное в § 30 алгебраическое уравнение для $\zeta = e^{\frac{2\pi i}{m}}$ неприводимо в поле рациональных чисел.

Просматривая еще раз всю цепь заключений, приведшую нас к доказательству теоремы 131, мы видим, что наиболее трудным пунктом являлось доказательство того, что $L(1, \chi) \neq 0$; это доказательство основывалось на том факте, что функция $\zeta_k(s)$ при $s \to 1$ является бесконечно большой первого порядка, а это в свою очередь базировалось на теоремах § 40 о плотности идеалов, для доказательства которых потребовалась вся теория единиц. Нелишне будет отметить, что доказательство теоремы 131 можно провести и без помощи этих теоретико-числовых средств, основываясь зато на более точном изучении функционально-теоретических свойств функций $L(s, \chi)$. Мы приведем здесь по этому вопросу лишь некоторые ориентирующие указания.

Прежде всего с помощью леммы b) § 42 можно доказать (путем почленного дифференцирования), что функция $L(s, \chi)$, где χ — не главный характер, дифференцируема при $s = 1$, и потому, если бы было $L(1, \chi) = 0$, она имела бы в $s = 1$ нуль по крайней мере первого порядка, ибо тогда существовал бы предел

$$\lim_{s \to 1} \frac{L(s, \chi)}{s - 1} = \lim_{s \to 1} \frac{L(s, \chi) - L(1, \chi)}{s - 1} = \frac{dL(s, \chi)}{ds}\Big|_{s=1}.$$

С другой стороны, произведение всех $\varphi(m)$ рядов $L(s, \chi)$ является при $s > 1$ сходящимся рядом с положительными членами. В самом деле, если в группе классов вычетов $\bmod m$ p есть элемент порядка f, то по теореме 32 $\varphi(m)$ чисел $\chi(p)$ пробегают все корни f-й степени из 1, каждый повторенный одинаковое число раз. Следовательно,

$$\prod_{\chi} \left(1 - \frac{\chi(p)}{p^s}\right) = \left(1 - \frac{1}{p^{fs}}\right)^e \quad \left(e = \frac{\varphi(m)}{f}\right),$$

а это показывает, что $\prod_{\chi} L(s, \chi)$ есть ряд с положительными коэффициентами, причем сумма его больше 1 для всех $s > 1$. Так как теперь соответствующая главному характеру функция $L(s, \chi_1)$ совпадает, с точностью до несущественных множителей, с $\zeta(s)$, то при $s \to 1$ она является бесконечно большой величиной первого порядка, и так как все остальные $L(s, \chi)$ либо имеют в $s = 1$ нуль по меньшей мере первого порядка, либо во всяком случае стремятся к конечному пределу, то обращаться в нуль может самое большее один из множителей $L(1, \chi)$, причем характер, для которого это имеет место, должен быть вещественным (принимающим, следовательно, лишь значения ± 1, 0, т. е. представляющим собой квадратичный характер $\bmod m$). В самом деле, если бы χ был невещественным характером, то ком-

плексно сопряженная функция $\overline{\chi}$ была бы отличным от него характером, для которого $L(1, \overline{\chi})$ также было бы равно нулю, что противоречит только что доказанному. Таким образом остается показать, что $L(1, \chi) \neq 0$ для всех квадратичных характеров χ.

Мертенсу [1]) удалось доказать это утверждение путем непосредственной оценки членов ряда $L(1, \chi)$. Это дало независимое от теории полей доказательство теоремы Дирихле.

Сам Дирихле воспользовался квадратичным законом взаимности, с помощью которого можно доказать, что ряды $L(s, \chi)$, соответствующие вещественным характерам χ, входят множителями в дзета-функции некоторых квадратичных числовых полей и в силу этого не могут обращаться в нуль при $s = 1$. Таким образом Дирихле опирался в своем доказательстве не на арифметику полей деления круга, как это сделано в настоящей книге, а лишь на арифметику квадратичных полей.

Последнюю группу составляют чисто теоретико-функциональные доказательства, наиболее доступные обобщению. В них функции $L(s, \chi)$ исследуются как аналитические функции комплексного переменного s. Оказывается, что $L(s, \chi)$ представляют собой регулярные аналитические функции для всех конечных значений s, кроме функции $L(s, \chi_1)$, имеющей лишь при $s = 1$ полюс первого порядка. Если бы теперь один из L-рядов обращался в нуль при $s = 1$, то произведение всех L-рядов представляло бы функцию, регулярную во всей плоскости s. Но это противоречит тому, что, будучи рядом Дирихле с положительными коэфициентами, это произведение, в силу одной общей теоремы теории функций, должно иметь по крайней мере одну конечную особую точку [2]).

Идея, лежащая в основе метода Дирихле введения групповых характеров, допускает значительные обобщения: вместо разбиения рациональных чисел в $k(1)$ на классы вычетов $\bmod m$ мы можем рассматривать какие-либо разбиения чисел любого поля k на классы, образующие абелевы группы [3]). Наконец, мы можем применить теорему 126 и к другим полям, отличным от $k(e^{\frac{2\pi i}{m}})$, равно как и к относительным полям. В каждом случае, зная законы разложения, господствующие в данном поле, мы сможем доказать существование бесконечного множества простых чисел или простых идеалов этого поля, обладающих известного рода свойствами. В следующей главе (§ 48) мы проделаем это в применении к квадратичному полю.

---

[1]) Mertens, Über die Nichtverschwinden Dirichletscher Reihen mit reellen Gliedern, Sitzungsber. d. Akad. d. Wiss. in Wien, math.-naturw. Klasse, Bd. 104 (1895).

[2]) См., например, E. Landau, Handbuch der Lehre von der Verteilung der Primzahlen (Leipzig 1909), Bd. I, § 121; см также Hecke, Über die L-Funktionen und den Dirichletschen Primzahlsatz fur einen beliebigen Zahlkörper, Nachr. v. d. K. Ges. d. Wissens h. zu Göttingen, 1917.

[3]) Эта общая постановка вопроса принадлежит Веберу: см. H. Weber, Über Zahlengruppen in algebraischen Körpern, I, II, III, Math. Ann., Bd. 48, 49, 50 (1897—1898).

ГЛАВА VII

КВАДРАТИЧНОЕ ЧИСЛОВОЕ ПОЛЕ

§ 44. Сводка полученных результатов. Система классов идеалов

В этой главе будет подвергнуто дальнейшему изучению квадратичное числовое поле, рассматривавшееся уже в качестве примера в § 29. Напомним прежде всего полученные там результаты.

Пусть D — положительное либо отрицательное целое рациональное число, отличное от 1 и не делящееся ни на один рациональный квадрат, кроме 1. Числами $\sqrt{D}$ порождаются все квадратичные числовые поля. Дискриминант поля, порожденного числом $\sqrt{D}$, есть

$$d = D, \quad \text{если } D \equiv 1 \pmod 4,$$
$$d = 4D, \quad \text{если } D \equiv 2 \text{ или } 3 \pmod 4.$$

Во всех случаях числа 1, $\frac{d+\sqrt{d}}{2}$ образуют базис. Каждое целое число поля представимо в виде $\alpha = \frac{x+y\sqrt{d}}{2}$ с целыми рациональными x, y. Нечетное положительное простое число p распадается на два различных или одинаковых простых множителя или остается простым, смотря по тому, имеет ли символ квадратичного вычета $\left(\frac{d}{p}\right)$ значение 1, 0 или -1.

Определим теперь *символ квадратичного вычета со знаменателем* 2, однако, лишь для тех числителей d, которые служат дискриминантами квадратичных полей:

Если d четное, то положим $\left(\frac{d}{2}\right) = 0$.

Если d нечетное, то положим $\left(\frac{d}{2}\right) = +1$, если d квадратичный вычет mod 8, и $\left(\frac{d}{2}\right) = -1$, если d квадратичный невычет mod 8.

Тогда закон разложения числа 2 в поле $k(\sqrt{d})$ будет формулироваться таким же образом, как выше для нечетного p.

В вещественных квадратичных полях, по теореме 100, имеется одна основная единица. Так как единственные вещественные корни из 1 суть ± 1, то совокупность всех единиц поля совпадает с совокуп-

ностью чисел $\pm\varepsilon^n$ ($n=0, \pm1, \pm2, \ldots$), где ε — основная единица; последняя однозначно определяется при дополнительном условии $\varepsilon>1$. Очевидно, мы получим все единицы $\eta=\frac{x+y\sqrt{d}}{2}$, решая в целых рациональных x, y уравнение $N(\eta)=\pm1$, т. е.

$$x^2-dy^2=\pm4. \tag{104}$$

Это — так называемое *уравнение Пелля*.

В мнимых квадратичных полях каждая единица η является корнем из 1. При $d<0$ уравнение (104) (где, конечно, нужно взять верхний знак), кроме тривиальных решений $y=0$, $x=\pm2$, т. е. $\eta=\pm1$, имеет решения лишь при $d\geqslant-4$, а именно, при $d=-4$ пару решений $x=0$, $y=\pm1$, и при $d=-3$ еще пару решений $x=\pm1$, $y=\pm1$. Таким образом число w корней из 1 в $K(\sqrt{-3})$ — поле корней третьей степени из 1 — равно 6, в $k(\sqrt{-1})$ равно 4 и во всех остальных квадратичных полях равно 2.

Нашей целью будет теперь найти, исходя из общей теории, метод, позволяющий для любых двух данных идеалов $\mathfrak{a}$, $\mathfrak{b}$ рассматриваемого квадратичного поля решить, эквивалентны они или нет, и этим путем задать полную систему неэквивалентных идеалов, т. е. вместе с тем вычислить число классов.

Так как $N(\mathfrak{b})=\mathfrak{b}\mathfrak{b}'$ есть рациональный главный идеал, то соотношение эквивалентности $\mathfrak{a}\sim\mathfrak{b}$ равносильно соотношению $\mathfrak{a}\mathfrak{b}'\sim1$; таким образом мы должны определить, является ли данный идеал главным идеалом. Если теперь целый идеал $\mathfrak{a}$ задан, скажем, как наибольший общий делитель (α, β) двух главных идеалов α, β, то $\mathfrak{a}$ есть содержание формы $\alpha u+\beta v$, следовательно, $\mathfrak{a}\mathfrak{a}'=N(\mathfrak{a})$ есть содержание формы

$$(\alpha u+\beta v)(\alpha' u+\beta' v)=\alpha\alpha' u^2+(\alpha'\beta+\alpha\beta')uw+\beta\beta' v^2,$$

т. е. $N(\mathfrak{a})$ есть наибольший общий делитель рациональных чисел $\alpha\alpha'$, $\alpha'\beta+\alpha\beta'$, $\beta\beta'$. Пусть это будет положительное рациональное число n; мы приходим, следовательно, к вопросу, является ли $\pm n$ нормой целого числа рассматриваемого поля и, далее, если $\pm n$ — норма целого ω, $N(\omega)=\pm n$, то верно ли равенство $\omega=(\alpha, \beta)$. Но последнее равенство в свою очередь будет иметь место тогда и только тогда, когда $\frac{\alpha}{\omega}$ и $\frac{\beta}{\omega}$ — целые числа, ибо в этом случае, по построению числа ω, идеал $\left(\frac{\alpha}{\omega}, \frac{\beta}{\omega}\right)$ есть целый идеал с нормой 1 и, значит, сам равен (1).

Таким образом остается единственная трудность: нахождение всех главных идеалов (ω), нормы которых имеют заданное значение. Это приводит к задаче определения всех целых рациональных решений уравнения

$$x^2-dy^2=\pm4n. \tag{105}$$

Для мнимых квадратичных полей все такие решения x, y определяются путем конечного числа проверок, ибо вследствие отрицатель-

ности числа d целые рациональные x, y, которые вообще могут удовлетворять уравнению (105), подчиняются условиям

$$|x| \leqslant 2\sqrt{n}, \quad |\sqrt{d}|\,|y| \leqslant 2\sqrt{n},$$

так что нужно лишь проверить вычислением, для скольких целых рациональных y из интервала $0 \leqslant y \leqslant 2\left|\sqrt{\frac{n}{d}}\right|$ выражение $\sqrt{4n+dy^2}$ представляет рациональное число.

Для нахождения решений уравнения (105) при $d>0$, т. е. для вещественных квадратичных полей, достаточно знания одной отличной от ± 1 единицы (не обязательно основной). Действительно, если

$$\eta = \frac{u+v\sqrt{d}}{2} \quad (v>0)$$

— единица поля $k(\sqrt{d})$, бо́льшая чем 1, то мы всегда сможем найти среди ассоциированных с заданным ω чисел $\alpha = \omega\eta^n$ ($n = 0, \pm 1, \pm 2, \ldots$) такое, для которого удовлетворялось бы условие

$$1 \leqslant \left|\frac{\alpha}{\alpha'}\right| < \eta^2;$$

в самом деле, $\alpha' = \omega'\eta'^n = \pm\omega'\eta^{-n}$, так что $\left|\frac{\alpha}{\alpha'}\right| = \left|\frac{\omega}{\omega'}\right|\eta^{2n}$; беря тогда $n = -k$, где k — такое целое рациональное число, что $\eta^{2k} \leqslant \left|\frac{\omega}{\omega'}\right| < \eta^{2k+2}$, мы, очевидно, удовлетворим требуемому условию. Таким образом достаточно разыскать те решения уравнения (105), которые, если положить $\alpha = \omega = \frac{x+y\sqrt{d}}{2}$, удовлетворяют еще указанному только что условию; это условие можно записать также в форме

$$|\omega'| \leqslant |\omega| < |\omega'|\eta^2 \quad \text{или} \quad |\omega|\eta^{-2} < |\omega'| \leqslant |\omega|$$

или, в силу равенства $|\omega\omega'| = n$, также и так:

$$\left.\begin{aligned} \sqrt{n} \leqslant |\omega| < \eta\sqrt{n}, \\ \eta^{-1}\sqrt{n} < |\omega'| \leqslant \sqrt{n}. \end{aligned}\right\} \tag{106}$$

Если, кроме того, $\omega>0$, то в случае верхнего знака в (105) имеем также $\omega'>0$, и из (106) путем сложения мы получаем

$$(\eta^{-1}+1)\sqrt{n} < x < (\eta+1)\sqrt{n}; \tag{107}$$

в случае же нижнего знака получаем

$$(\eta^{-1}+1)\sqrt{n} < y\sqrt{d} < (\eta+1)\sqrt{n}. \tag{108}$$

Таким образом в обоих случаях требуется лишь для конечного числа значений x, y определить, удовлетворяется ли для них уравнение (105). Существуют ли среди найденных таким образом чисел $\omega = \frac{x+y\sqrt{d}}{2}$ ассоциированные, устанавливается тогда простым делением.

Нахождение требуемой единицы η может быть выполнено различными способами. Один из способов непосредственно доставляется доказательством теоремы Дирихле о единицах (лемма b), § 35). Этот способ в существенном сводится к разложению $\sqrt{d}$ в непрерывную дробь. Результат § 52 о числе классов даст нам другое выражение для единицы в $k(\sqrt{d})$, составленное с помощью корней d-й степени из 1.

Таким образом мы во всяком случае можем путем выполнения конечного числа рациональных операций решить, эквивалентны ли два заданных идеала квадратичного поля.

Для нахождения отсюда числа классов, вспомним, что по теореме 96 в каждом классе существует целый идеал, норма которого не превосходит $|\sqrt{d}|$. Поэтому мы сначала определяем все целые идеалы, нормы которых удовлетворяют этому условию; на основании законов разложения (§ 29) это выполняется для всех простых идеалов, а затем путем умножения мы получаем все вообще требуемые идеалы. Затем мы определяем, сколько среди получившегося конечного числа идеалов имеется неэквивалентных; найденное число и будет числом классов.

Проиллюстрируем изложенные соображения на нескольких числовых примерах.

1. $k(\sqrt{-1})$, $k(\sqrt{-3})$, $k(\sqrt{-2})$ имеют число классов $h=1$. В самом деле, ближайшим к $|\sqrt{d}|$ меньшим целым числом является соответственно 1, 1, 2. Таким образом в первых двух полях в каждом классе существует целый идеал с нормой $\leqslant 1$, и это будет необходимо идеал (1), т. е. главный идеал. В $k(\sqrt{-2})$ мы должны, кроме того, исследовать еще идеалы с нормой 2. Здесь 2 будет квадратом простого идеала $\mathfrak{p}$, который, очевидно, равен $(\sqrt{-2})$, т. е. тоже есть главный идеал.

2. В $k(\sqrt{7})$ $d=28$, так что нужно исследовать лишь идеалы с нормами 2, 3, 4, 5. Но в рассматриваемом поле простые числа 2, 3, 5 распадаются на простые идеалы следующим образом:

$$2=\mathfrak{p}_2^2,\quad 3=\mathfrak{p}_3\mathfrak{p}_3',\quad 5 \text{ само есть простой идеал.}$$

Поэтому идеалов с нормой 4 имеется лишь один, а именно, $\mathfrak{p}_2^2=2$, т. е. главный идеал. Таким образом, кроме главного класса, имеются еще лишь классы, представляемые идеалами $\mathfrak{p}_2$, $\mathfrak{p}_3$, $\mathfrak{p}_3'$. Путем подбора получаем

$$2=3^2-7\cdot 1^2,\ \text{т. е.}\ \mathfrak{p}_2=(3+\sqrt{7})\sim 1.$$

При этом, так как $\mathfrak{p}_2=\mathfrak{p}_2'$, то числа $3+\sqrt{7}$ и $3-\sqrt{7}$ должны быть ассоциированными, т. е. отношение

$$\eta=\frac{3+\sqrt{7}}{3-\sqrt{7}}=\frac{(3+\sqrt{7})^2}{2}=8+3\sqrt{7}$$

есть единица. Посмотрим, не является ли $\mathfrak{p}_3$ главным идеалом. Из $\mathfrak{p}_3=(a+b\sqrt{7})$ вытекало бы

$$\pm 3 = a^2 - 7b^2, \quad \text{т. е.} \quad \pm 3 \equiv a^2 \pmod 7.$$

Здесь верхний знак не может иметь места, так как 3 есть невычет mod 7. Таким образом, в силу (108), достаточно испробовать для b значения, ограниченные неравенствами

$$(9-3\sqrt{7})\sqrt{3} < b\sqrt{28} < (9+3\sqrt{7})\sqrt{3}$$

или, тем более,

$$0 < b < \left(\sqrt{\frac{81}{28}}+\frac{3}{2}\right)\sqrt{3} < 3+\sqrt{\frac{27}{4}}, \quad 0 < b \leqslant 5.$$

Но уже $b=1$ дает

$$a = \sqrt{-3+7\cdot 1^2} = 2,$$

так что $\mathfrak{p}_3=(2+\sqrt{7})$, т. е. $\mathfrak{p}_3$ — главный идеал. Таким образом и здесь $h=1$.

3. В $k(\sqrt{-5})$ число классов отлично от 1, ибо, как было обнаружено в § 23, идеал $\mathfrak{p}_3=(3, 4+\sqrt{-5})$ не является главным. Так как здесь $d=-20$, то нужно исследовать идеалы с нормами 2, 3, 4. Имеем $2=\mathfrak{p}_2^2$; здесь $\mathfrak{p}_2$ не является главным идеалом, так как 2 непредставимо в форме a^2+5b^2. Единственным идеалом с нормой 4 является главный идеал $\mathfrak{p}_2^2=4$. Так как, наконец, $\mathfrak{p}_3\mathfrak{p}_3'=3$ и $\mathfrak{p}_3^2=(2-\sqrt{-5})\sim 1$, то $\mathfrak{p}_3'\sim\mathfrak{p}_3$, так что, кроме главного класса, мы имеем еще классы, представляемые идеалами $\mathfrak{p}_2$, $\mathfrak{p}_3$. Если бы теперь $\mathfrak{p}_2$ не было эквивалентно $\mathfrak{p}_3$, то мы имели бы точно три различных класса и, в силу группового свойства, $\mathfrak{p}_2^3$ был бы главным идеалом; но так как $\mathfrak{p}_2^2\sim 1$, то отсюда следовало бы, что уже $\mathfrak{p}_2\sim 1$, что неверно. Таким образом $\mathfrak{p}_2\sim\mathfrak{p}_3$ и значит $h=2$.

4. В $k(\sqrt{-23})$ $d=-23$; нужно рассмотреть идеалы с нормами 2, 3, 4. Имеем

$$\left(\frac{-23}{2}\right)=+1, \quad 2=\mathfrak{p}_2\mathfrak{p}_2',$$

$$\left(\frac{-23}{3}\right)=+1, \quad 3=\mathfrak{p}_3\mathfrak{p}_3'.$$

Таким образом идеалы с нормами 2, 3, 4 суть

$$\mathfrak{p}_2,\ \mathfrak{p}_2',\ \mathfrak{p}_3,\ \mathfrak{p}_3',\ \mathfrak{p}_2^2,\ \mathfrak{p}_2'^2,\ \mathfrak{p}_2\mathfrak{p}_2'; \tag{109}$$

как нетрудно видеть, лишь последний из них является главным идеалом. Далее, для справедливости соотношения $\mathfrak{p}_2\sim\mathfrak{p}_3$ необходимо, чтобы выполнялось соотношение $\mathfrak{p}_2\mathfrak{p}_3'\sim 1$; так как $N(\mathfrak{p}_2\mathfrak{p}_3')=6$, то мы должны посмотреть, является ли 6 нормой какого-нибудь числа;

непосредственной проверкой убеждаемся в том, что это действительно так, причем

$$6 = \frac{x^2 + 23y^2}{4} \quad \text{лишь при } x = \pm 1,\ y = \pm 1.$$

Таким образом существует точно два, и притом сопряженных, главных идеала с нормой 6; это показывает, что либо $\mathfrak{p}_2\mathfrak{p}_3$, либо $\mathfrak{p}_2\mathfrak{p}_3'$ является главным идеалом. Так как выбор нумерации сопряженных в нашем распоряжении, то мы можем считать, что $\mathfrak{p}_2\mathfrak{p}_3' \sim 1$. Таким образом среди идеалов (109) неэквивалентны самое большее идеалы

$$1,\ \mathfrak{p}_2,\ \mathfrak{p}_2',\ \mathfrak{p}_2^2,\ \mathfrak{p}_2'^2.$$

Идеал $\mathfrak{p}_2$ неэквивалентен ни $\mathfrak{p}_2'$, ни $\mathfrak{p}_2^2$. Однако

$$\mathfrak{p}_2 \sim \mathfrak{p}_2'^2,\ \mathfrak{p}_2' \sim \mathfrak{p}_2^2,\ \text{т. е. } \mathfrak{p}_2^3 \sim 1;$$

в самом деле, $N(\mathfrak{p}_2^3) = 8$ и 8 есть норма целого числа $\frac{3 + \sqrt{-23}}{2}$, очевидно не делящегося ни на одно рациональное число, кроме ± 1; но единственными идеалами с нормой 8, не имеющими рациональных делителей, являются $\mathfrak{p}_2^3$ и $\mathfrak{p}_2'^3$, следовательно, один из них, а значит, также другой, является главным идеалом.

Таким образом $h = 3$, и представителями трех классов служат

$$\mathfrak{p}_2,\ \mathfrak{p}_2^2,\ \mathfrak{p}_2^3 \sim 1.$$

§ 45. Понятие эквивалентности в узком смысле. Структура группы классов

Для исследования квадратичных полей оказывается полезным ввести несколько модифицированное понятие эквивалентности.

Определение. Мы называем два идеала $\mathfrak{a}$, $\mathfrak{b}$ ($\neq 0$) квадратичного поля k *эквивалентными в узком смысле*, если в k существует такое число λ, что

$$\mathfrak{a} = \lambda\mathfrak{b} \quad \text{и} \quad N(\lambda) > 0.$$

Мы пишем

$$\mathfrak{a} \approx \mathfrak{b}$$

и причисляем $\mathfrak{a}$ и $\mathfrak{b}$ к одному и тому же *классу идеалов в узком смысле*.

Эти классы могут быть обычным путем объединены в абелеву группу. Пусть $\mathfrak{M}$ — группа всех идеалов, отличных от 0, $\mathfrak{H}_0$ — группа всех главных идеалов (μ) с $N(\mu) > 0$, $\mathfrak{H}$ — группа всех главных идеалов ($\neq 0$), причем в качестве композиции служит умножение идеалов. Тогда классы идеалов в узком смысле суть смежные классы при разложении $\mathfrak{M}$ по $\mathfrak{H}_0$; факторгруппа $\mathfrak{M}/\mathfrak{H}_0$ есть группа классов идеалов в узком смысле, ее единичным элементом служит система

идеалов группы $\mathfrak{H}_0$. Группа классов в предшествующем смысле есть факторгруппа $\mathfrak{M}/\mathfrak{H}$.

Из $\mathfrak{a} \approx \mathfrak{b}$ вытекает $\mathfrak{a} \sim \mathfrak{b}$; таким образом новое разбиение на классы есть подразбиение старого. Если, обратно, $\mathfrak{a} \sim \mathfrak{b}$, то, очевидно, либо $\mathfrak{a} \approx \mathfrak{b}$, либо $\mathfrak{a} \approx \mathfrak{b}\sqrt{d}$; таким образом класс в широком смысле распадается самое большее на два класса в узком смысле, и, значит, число классов в узком смысле h_0 конечно и не превосходит $2h$.

Так как равенство $\mathfrak{a} = \mu\mathfrak{b}$ определяет число μ лишь с точностью до единичного множителя, то оба понятия эквивалентности только тогда совпадают, когда в каждой полной системе ассоциированных чисел содержатся числа с положительными нормами, т. е., следовательно, $h_0 = h$, если k — мнимое поле, либо если k вещественное и основная единица в k имеет норму -1.

В остающемся еще случае, когда k вещественное и каждая единица в k имеет норму $+1$, идеалы $\mathfrak{a}$ и $\mathfrak{a}\sqrt{d}$, очевидно, неэквивалентны в узком смысле, т. е. тогда $h_0 = 2h$.

Основной задачей должно было бы быть исследование структуры определенной только что группы классов в узком смысле. Однако эту задачу до сих пор оказалось возможным выполнить лишь в очень небольшой части; полученные результаты выражаются следующей теоремой:

Теорема 132. *Принадлежащее числу* 2 *базисное число* $e_0(2)$ *группы классов в узком смысле равно* $t-1$, *где* t — *число различных простых множителей дискриминанта* d *поля* k.

Для доказательства мы должны, в силу теоремы 28, показать, что в k существует точно 2^{t-1} классов (в узком смысле), квадрат которых есть главный класс (в узком смысле). Заметим прежде всего, что, в силу установленных выше законов разложения, квадрат каждого из t различных простых идеалов $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$, содержащихся в d, есть рациональный главный идеал, т. е. ≈ 1. Покажем, что каждый идеал $\mathfrak{a}$, для которого $\mathfrak{a}^2 \approx 1$, необходимо эквивалентен некоторому произведению степеней этих идеалов $\mathfrak{q}$. Из $\mathfrak{a}^2 \approx 1$ и $\mathfrak{a}\mathfrak{a}' \approx 1$ вытекает

$$\frac{\mathfrak{a}}{\mathfrak{a}'} \approx 1, \quad \frac{\mathfrak{a}}{\mathfrak{a}'} = \omega,$$

где ω — число с положительной нормой, которое, в случае его вещественности, мы можем предполагать положительным. Так как оно является отношением двух сопряженных идеалов, то $N(\omega) = 1$. Но тогда ω есть также отношение двух сопряженных чисел, именно

$$\omega = \frac{1+\omega}{1+\omega'}.$$

Так как теперь идеал $\frac{\mathfrak{a}}{1+\omega}$ совпадает со своим сопряженным $\frac{\mathfrak{a}'}{1+\omega'}$, то, в силу установленных законов разложения,

$$\frac{\mathfrak{a}}{1+\omega} = r\mathfrak{q}_1^{a_1} \ldots \mathfrak{q}_t^{a_t},$$

где r — рациональное число и показатели a_i равны 0 или 1. Но это и означает, как утверждалось, что

$$\mathfrak{a} \approx \mathfrak{q}_1^{a_1} \dots \mathfrak{q}_t^{a_t},$$

ибо $N(1+\omega) = \omega(1+\omega')^2 > 0$.

Целый **идеал в** $k(\sqrt{d})$, совпадающий со своим сопряженным и не содержащий рациональных множителей (кроме ± 1), называется *двусторонним идеалом*. Класс идеалов, совпадающий со своим сопряженным, называется *двусторонним классом*. Из приведенных рассуждений видно, что в каждом двустороннем классе содержится двусторонний идеал.

Для завершения доказательства теоремы остается еще показать, что среди t двусторонних классов $Q_1, \dots, Q_t$, определяемых соответственно идеалами $\mathfrak{q}_1, \dots, \mathfrak{q}_t$, имеется ровно $t-1$ независимых (в теоретико-групповом смысле). Но если имеет место нетривиальное соотношение

$$Q_1^{a_1} \dots Q_t^{a_t} = 1, \tag{110}$$

где, следовательно, не все a_i четны, то существует число α такое, что

$$\alpha = \mathfrak{q}_1^{a_1} \dots \mathfrak{q}_t^{a_t}, \quad N(\alpha) > 0. \tag{111}$$

Тогда $(\alpha) = (\alpha')$, $\alpha = \eta\alpha'$, где η — единица с $N(\eta) = +1$. Рассмотрим следующие три случая:

a) $d < 0$. Мы можем считать, что $d < -4$, так как при $d = -3$ и $d = -4$ имеем $h = 1$ и $t = 1$, и, в силу этого, теорема 132 верна. Но при $d < -4$ в поле k содержатся лишь единицы ± 1, значит,

$$\alpha = \pm\alpha', \quad \alpha = r(\sqrt{d})^n \qquad (n = 0 \text{ или } 1), \tag{112}$$

где r — рациональное число. При $n = 0$ все показатели a в (111) четны, при $n = 1$ по крайней мере одно a нечетно, так как d не есть квадрат рационального числа.

b) $d > 0$, и норма основной единицы ε равна -1. Здесь $\eta > 0$, ибо $N(\alpha) = \eta\alpha'^2 > 0$; поэтому $\eta = \varepsilon^{2n}$ с целым рациональным n. Так как

$$\varepsilon^2 = -\frac{\varepsilon}{\varepsilon'} = \frac{\varepsilon\sqrt{d}}{-\varepsilon'\sqrt{d}},$$

то получаем

$$\frac{\alpha}{(\varepsilon\sqrt{d})^n} = \frac{\alpha'}{(-\varepsilon'\sqrt{d})^n}, \quad \alpha = r(\varepsilon\sqrt{d})^n \tag{113}$$

с рациональным r. И здесь при четном n все a четны, а при нечетном по крайней мере одно a нечетно.

c) $d > 0$, и норма основной единицы ε ($\varepsilon > 0$) равна $+1$. Имеем

$$\eta = \varepsilon^n, \quad \varepsilon = \frac{1+\varepsilon}{1+\varepsilon'}, \quad \eta = \frac{(1+\varepsilon)^n}{(1+\varepsilon')^n}, \quad \alpha = r(1+\varepsilon)^n. \tag{114}$$

Идеал $(1+\varepsilon)$ совпадает со своим сопряженным, однако, не является рациональным главным идеалом. Действительно, из равенства

$$1+\varepsilon = r_1 \varepsilon^k$$

с рациональным r_1 следовало бы

$$\varepsilon = \frac{1+\varepsilon}{1+\varepsilon'} = \varepsilon^{2k}, \quad \varepsilon^{2k-1} = 1,$$

что невозможно. Отсюда вытекает, что $(1+\varepsilon)$ имеет разложение

$$(1+\varepsilon) = \text{рациональный идеал} \times \mathfrak{q}_1^{b_1} \dots \mathfrak{q}_t^{b_t},$$

где по крайней мере один показатель b_i нечетен.

Таким образом во всех случаях мы получаем, что если α обладает разложением (111), где не все показатели a_i четны, то оно должно представляться в одной из трех форм (112), (113), (114) с нечетным n. Это показывает, что в соотношении (110) показатели a_i однозначно определены по модулю 2 и, значит, существует не более одного нетривиального соотношения между t классами $Q_1, \dots, Q_t$. Но, обратно, одно такое соотношение действительно существует, как показывает разложение главного идеала (в узком смысле) $\sqrt{d}$, соответственно $\varepsilon\sqrt{d}$, соответственно $1+\varepsilon$ в случаях a), b), c), где по крайней мере один из показателей a_i нечетен.

Таким образом среди классов Q имеется точно $t-1$ независимых, что и завершает доказательство теоремы 132.

Сформулируем еще особо два важных следствия из теоремы 132:

Теорема 133. *Если дискриминант d поля $k(\sqrt{d})$ делится только на одно простое число $(t=1)$, то h_0, а потому также h, нечетно и, следовательно, в случае $d>0$ норма основной единицы равна -1.*

Теорема 134. *Если d есть произведение двух положительных простых чисел q_1, q_2, сравнимых с 3 по модулю 4, то в поле $k(\sqrt{q_1 q_2})$ либо q_1, либо q_2 есть норма главного идеала в узком смысле.*

Прежде всего в поле, о котором идет речь в теореме 134, норма каждой единицы равна $+1$. В самом деле, из $N(\alpha)=-1$ и $\alpha = \frac{x+y\sqrt{q_1 q_2}}{2}$ следовало бы

$$-4 \equiv x^2 \pmod{q_1 q_2},$$

и, значит, -1 было бы квадратичным вычетом $\bmod q_1$; однако, в силу формулы (31) § 16

$$\left(\frac{-1}{q_1}\right) = (-1)^{\frac{q_1-1}{2}} = -1.$$

Далее, в силу последней части доказательства теоремы 132, в поле $k(\sqrt{q_1q_2})$ имеет место соотношение

$$q_1^{a_1}q_2^{a_2} \approx 1, \tag{115}$$

где хотя бы одно из a_1, a_2 нечетно. Если бы теперь a_1 и a_2 были оба нечетны, то мы имели бы $q_1q_2 = (\sqrt{q_1q_2}) \approx 1$, и, значит, существовала бы такая единица η, что $N(\eta\sqrt{q_1q_2}) > 0$, т. е. $N(\eta) = -1$; но, как было только что показано, это невозможно. Таким образом в (115) один из показателей можно взять равным единице, а другой нулю, что и доказывает теорему 134.

Так как в рассматривавшемся поле h_0 должно быть равно $2h$, то нечетность h совместима с теоремой 132. Что h здесь действительно нечетно, можно без труда убедиться путем, аналогичным доказательству теоремы 132.

§ 46. Квадратичный закон взаимности. Новая формулировка законов разложения в квадратичных полях

Теорема 135. *Пусть p и q — нечетные положительные простые числа. Тогда имеют место соотношения:*

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

II. $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$,

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

Первая формула непосредственно вытекает из определения символа Лежандра (см. (31) § 16). Несколько сложнее, но зато по аналогии с последующими доказательствами формул II и III, мы можем вывести формулу I, основываясь на теории полей, а именно, следующим образом: Если $\left(\frac{-1}{p}\right) = +1$, то p разложимо в поле $k(\sqrt{-1})$, и так как $h_0 = 1$, то p есть норма некоторого главного идеала x, значит, $p = a^2 + b^2$. Так как каждый квадрат $\equiv 0$ или $1 \pmod 4$, то отсюда следует, что $p \equiv 1 \pmod 4$. Обратно, если $p \equiv 1 \pmod 4$, то, в силу последней части теоремы 133, в поле $k(\sqrt{p})$ число -1 является нормой целого числа $\varepsilon = \frac{a + b\sqrt{p}}{2}$, значит, $-4 \equiv a^2 \pmod p$, т. е. -1 есть квадратичный вычет $\bmod p$. Это и доказывает формулу I.

При доказательстве формулы II мы будем различать три случая:

1. $p \equiv q \equiv 1 \pmod 4$. Мы покажем, что $\left(\frac{p}{q}\right)$ и $\left(\frac{q}{p}\right)$ одновременно равны $+1$, значит, одновременно также равны -1, следовательно,

равны между собой, что и требуется утверждением теоремы в рассматриваемом случае.

Если $\left(\frac{q}{p}\right)=+1$, то простое число p разлагается в поле $k(\sqrt{q})$ на два различных множителя $\mathfrak{p}$, $\mathfrak{p}'$. Имеем

$$\mathfrak{p}^{h_0}=\alpha=\frac{x+y\sqrt{q}}{2},$$

где норма числа α положительна; отсюда

$$p^{h_0}=\frac{x^2-qy^2}{4},\quad 4p^{h_0}\equiv x^2 \pmod q.$$

Следовательно, p^{h_0} есть квадратичный вычет mod q, и так как h_0 по теореме 133 нечетно, то p само есть вычет mod q, т. е. $\left(\frac{p}{q}\right)=+1$. Так как наши предположения относительно p и q одинаковы, то точно так же из $\left(\frac{p}{q}\right)=+1$ вытекает $\left(\frac{q}{p}\right)=+1$, и формула II в рассматриваемом случае доказана.

2. $q\equiv 1 \pmod 4$, $p\equiv 3 \pmod 4$. Из $\left(\frac{q}{p}\right)=+1$, как и выше, вытекает, что и $\left(\frac{p}{q}\right)=+1$; в силу I имеем также $\left(\frac{-p}{q}\right)=\left(\frac{-1}{q}\right)\left(\frac{p}{q}\right)=+1$.

Если, обратно, $\left(\frac{-p}{q}\right)=+1$, то замечаем, что $-p\equiv 1 \pmod 4$, и, так же как выше, рассматривая поле $k(\sqrt{-p})$, заключаем, что также $\left(\frac{q}{p}\right)=+1$. Таким образом

$$\left(\frac{-p}{q}\right)=\left(\frac{q}{p}\right),\quad \text{т. е.}\quad \left(\frac{p}{q}\right)=\left(\frac{q}{p}\right),$$

в согласии с II.

3. $p\equiv q\equiv 3 \pmod 4$. Так же как и выше, можно доказать, что из $\left(\frac{-p}{q}\right)=+1$ вытекает $\left(\frac{-q}{p}\right)=-1$. Однако обратное утверждение так не получится. Поэтому мы пойдем другим путем. Рассмотрим поле $k(\sqrt{pq})$. В силу теоремы 134, в этом поле одно из чисел p, q является нормой некоторого целого числа $\frac{x+y\sqrt{pq}}{2}$. Пусть, скажем,

$$4p=x^2-pqy^2.$$

Тогда x, очевидно, должно делиться на p, $x=pu$, следовательно,

$$4=pu^2-qy^2.$$

Из этого равенства заключаем, что

$$\left(\frac{p}{q}\right)=+1\quad\text{и}\quad\left(\frac{-q}{p}\right)=+1,\quad\text{т. е.}\quad\left(\frac{q}{p}\right)=-1.$$

Точно так же при

$$4q = x^2 - pqy^2$$

мы получили бы

$$\left(\frac{p}{q}\right) = -1 \quad \text{и} \quad \left(\frac{q}{p}\right) = +1.$$

Таким образом в рассматриваемом случае $\left(\frac{p}{q}\right)$ и $\left(\frac{q}{p}\right)$ всегда различны, что и завершает доказательство формулы II.

Нам осталось доказать формулу III. Пусть $\left(\frac{2}{p}\right) = +1$. Тогда p разложимо в поле $k(\sqrt{2})$, и так как здесь $h = h_0 = 1$, то p является нормой целого числа:

$$p = x^2 - 2y^2.$$

Отсюда следует, что

$$p \equiv x^2 \pmod 8, \text{ если } y \text{ четно},$$

$$p \equiv x^2 - 2 \pmod 8, \text{ если } y \text{ нечетно},$$

значит, ввиду нечетности x, $p \equiv \pm 1 \pmod 8$.

Пусть, обратно, $p \equiv \pm 1 \pmod 8$. Рассмотрим тогда поле $k(\sqrt{\pm p})$, в котором по теореме 133 h_0 нечетно.

В этом поле, согласно законам разложения, установленным в начале этой главы, число 2 разлагается на различные множители, $2 = \mathfrak{p}\mathfrak{p}'$: тогда $2^{h_0} = \frac{x^2 \mp py^2}{4}$, т. е. $\left(\frac{2^{h_0+2}}{p}\right) = +1$; вследствие нечетности h_0 отсюда вытекает, что и $\left(\frac{2}{p}\right) = +1$.

Таким образом мы доказали, что $\left(\frac{2}{p}\right) = +1$ тогда и только тогда, когда $p \equiv \pm 1 \pmod 8$. Но это равносильно формуле III.

Мы **обобщим** теперь доказанные формулы на тот случай, когда p и q являются **составными** положительными нечетными числами. Уже в § 16 лежандров символ, в котором по его первоначальному определению „знаменателем“ служит простое число, мы определили и для составных знаменателей. Оказывается, что и для этих „якобиевых символов“ имеет место тот же закон взаимности.

Пусть a, b — произвольные целые нечетные числа. Так как

$$(a-1)(b-1) \equiv 0 \pmod 4,$$

то

$$ab - 1 \equiv a - 1 + b - 1 \pmod 4,$$

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2. \tag{116}$$

Точно так же из

$$(a^2-1)(b^2-1) \equiv 0 \pmod{16}$$

вытекает

$$\frac{a^2b^2-1}{8} \equiv \frac{a^2-1}{8} + \frac{b^2-1}{8} \pmod 2. \tag{117}$$

Повторным применением этих формул получаем для r целых нечетных чисел $p_1, \ldots, p_r$

$$\frac{p_1 p_2 \ldots p_r - 1}{2} \equiv \sum_{i=1}^{r} \frac{p_i - 1}{2} \pmod 2,$$

$$\frac{(p_1 p_2 \ldots p_r)^2 - 1}{8} \equiv \sum_{i=1}^{r} \frac{p_i^2 - 1}{8} \pmod 2.$$

Пусть теперь P, Q — положительные нечетные числа, и

$$P = p_1 p_2 \ldots p_r, \quad Q = q_1 q_2 \ldots q_s$$

— их разложения на простые множители. Тогда, в силу данного в § 16 определения якобиева символа и формул I, II, III, (116) и (117), получаем

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\ldots\left(\frac{-1}{p_r}\right) = (-1)^{\sum_{i=1}^{r} \frac{p_i - 1}{2}} = (-1)^{\frac{P-1}{2}}, \quad (118)$$

$$\left(\frac{2}{P}\right) = (-1)^{\sum_{i=1}^{r} \frac{p_i^2 - 1}{8}} = (-1)^{\frac{P^2-1}{8}} \quad (119)$$

и

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \prod_{\substack{i=1,\ldots,r \\ k=1,\ldots,s}} \left(\frac{p_i}{q_k}\right) = (-1)^{\left(\sum_{i=1}^{r} \frac{p_i - 1}{2}\right)\left(\sum_{k=1}^{s} \frac{q_k - 1}{2}\right)} \prod_{\substack{i=1,\ldots,r \\ k=1,\ldots,s}} \left(\frac{q_k}{p_i}\right),$$

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right)(-1)^{\frac{P-1}{2}\frac{Q-1}{2}} \quad (120)$$

Распространим теперь определение якобиева символа на отрицательные знаменатели, полагая

$$\left(\frac{a}{n}\right) = \left(\frac{a}{-n}\right). \quad (121)$$

При формулировке закона взаимности для отрицательных чисел мы будем пользоваться символом „sgn a“ (читается „сигнум a“), определяемым для вещественных a следующим образом:

$$\operatorname{sgn} a = \begin{cases} +1, & \text{если } a > 0, \\ -1, & \text{если } a < 0, \end{cases}$$

$$|a| = a \operatorname{sgn} a.$$

В силу (116), имеем

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{|P|-1}{2}} = (-1)^{\frac{P-1}{2} + \frac{\operatorname{sgn} P - 1}{2}}$$

Следовательно, для нечетных P, Q

$$\left(\frac{P}{Q}\right)=\left(\frac{\operatorname{sgn} P}{Q}\right)\left(\frac{|P|}{Q}\right)=(-1)^{\frac{\operatorname{sgn} P-1}{2}\cdot\frac{Q-1}{2}+\frac{\operatorname{sgn} P-1}{2}\cdot\frac{\operatorname{sgn} Q-1}{2}}\left(\frac{|P|}{Q}\right),$$

и, в силу (120),

$$\left(\frac{|P|}{Q}\right)=\left(\frac{|P|}{|Q|}\right)=\left(\frac{|Q|}{|P|}\right)(-1)^{\frac{|P|-1}{2}\cdot\frac{|Q|-1}{2}}=$$

$$=\left(\frac{Q}{P}\right)(-1)^{\frac{\operatorname{sgn} Q-1}{2}\cdot\frac{|P|-1}{2}+\frac{P|-1}{2}\cdot\frac{|Q|-1}{2}}.$$

Из этих формул вытекает

Теорема 136. (Общий квадратичный закон взаимности). *Пусть P, Q — нечетные целые рациональные числа. Имеют место равенства*

$$\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}+\frac{\operatorname{sgn} P-1}{2}},$$

$$\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}},$$

$$\left(\frac{P}{Q}\right)=\left(\frac{Q}{P}\right)(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}+\frac{\operatorname{sgn} P-1}{2}\cdot\frac{\operatorname{sgn} Q-1}{2}}.$$

Наконец, обобщим определение символа вычетов на четные знаменатели, однако, накладывая при этом ограничения на числитель. По теореме 45 группа классов вычетов mod 2^k, $k\geqslant 3$, обладая двумя базисными классами, не является циклической. Каждое нечетное число сравнимо с некоторым $(-1)^a 5^b \pmod{2^k}$ $(k\geqslant 3)$, где показатель a однозначно определен mod 2, а показатель b однозначно определен mod 2^{k-2}. Числа с $a\equiv 0 \pmod 2$ образуют циклическую подгруппу группы $\mathfrak{N}(2^k)$; это суть числа, сравнимые с 1 mod 4. Среди классов этой подгруппы классы, являющиеся квадратами, выделяются тогда посредством задания одного характера. В соответствии с этим мы введем следующее

Определение. Для целого рационального $a\equiv 0$ или $1 \pmod 4$

$$\left(\frac{a}{2}\right)=\left(\frac{a}{-2}\right)=\begin{cases}0, & \text{если } a\equiv 0 \pmod 4,\\ +1, & \text{если } a\equiv 1 \pmod 8,\\ -1, & \text{если } a\equiv 5 \pmod 8.\end{cases} \tag{122}$$

В силу теоремы 136 $\left(\frac{a}{2}\right)=\left(\frac{2}{a}\right)$, если первый символ имеет смысл. Для двух таких чисел a, a' имеем, далее,

$$\left(\frac{a}{2}\right)=\left(\frac{a'}{2}\right), \text{ если } a\equiv a' \pmod 8,$$

$$\left(\frac{aa'}{2}\right)=\left(\frac{a}{2}\right)\left(\frac{a'}{2}\right).$$

Наконец, полагаем вообще при $a \equiv 0$ или $1 \pmod 4$ и произвольных знаменателях

$$\left(\frac{a}{2}\right)^c = \left(\frac{a}{2^c}\right), \quad \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right). \tag{123}$$

Определение (122) согласуется с принятым в § 44 соглашением, так как каждый дискриминант квадратичного поля $\equiv 0$ или $1 \pmod 4$.

Теорема 137. *Пусть d — дискриминант квадратичного поля и n, m — целые положительные числа. Тогда*

$$\left(\frac{d}{n}\right) = \left(\frac{d}{m}\right), \qquad \text{если } n \equiv m \pmod d, \tag{124}$$

$$\left(\frac{d}{n}\right) = \left(\frac{d}{m}\right)\operatorname{sgn} d, \quad \text{если } n \equiv -m \pmod d. \tag{125}$$

Таким образом $\left(\frac{d}{n}\right)$ при положительном n является характером $\bmod d$.

Для доказательства выделим наивысшие степени двойки, входящие в d, n, m. Пусть

$$d = 2^a d', \quad n = 2^b n', \quad m = 2^c m',$$

причем d', n', m' уже нечетны.

1-й случай: $a > 0$. Случай $b > 0$ здесь тривиален, ибо вследствие предположений теоремы тогда также $c > 0$ и оба символа как в (124), так и в (125) обращаются в нуль. Пусть поэтому $b = c = 0$. Тогда по теореме 136 получаем

$$\left(\frac{2^a d'}{n}\right) = \left(\frac{2}{d}\right)^a \left(\frac{d'}{n}\right) = (-1)^{a\frac{n^2-1}{8}} \left(\frac{n}{d'}\right)(-1)^{\frac{n-1}{2}\cdot\frac{d'-1}{2}} \tag{126}$$

и аналогичное соотношение для m. Так как d делится по меньшей мере на 4, то первый множитель в правой части формулы (126) совпадает с первым множителем в аналогичной формуле для m; то же верно и для обоих других множителей, если $n \equiv m \pmod d$; если же $n \equiv -m \pmod d$, то произведение этих множителей в формуле (126) отличается от соответствующего произведения в аналогичной формуле для m как раз множителем $\operatorname{sgn} d'$.

2-й случай: $a = 0$, следовательно, $d \equiv 1 \pmod 4$. Имеем

$$\left(\frac{d}{2^b n'}\right) = \left(\frac{d}{2}\right)^b \left(\frac{d}{n'}\right) = \left(\frac{2}{d}\right)^b \left(\frac{n'}{d}\right) = \left(\frac{n}{d}\right), \tag{127}$$

откуда непосредственно вытекает утверждение теоремы.

Эта теорема показывает, что выведенный в § 29 закон разложения для квадратичных полей, будучи формально совершенно разнотипным с законом разложения для полей деления круга, тем не менее по своему содержанию оказывается родственным с ним. Действительно, теорема 137 показывает, что *два положительных простых числа, принадлежащих одному и тому же классу вычетов* $\bmod d$, *разлагаются в* $k(\sqrt{d})$ *одинаковым образом.* Значит, *также* $k(\sqrt{d})$

является полем классов, соответствующим разбиению рациональных чисел на классы mod d. Именно, если мы будем причислять к одному „роду" те числа n, для которых $\left(\frac{d}{n}\right)$ имеет одно и то же отличное от 0 значение, то совокупность целых положительных чисел, взаимно простых с d, распадется на два различных рода. По теореме 137 все числа, принадлежащие одному и тому же классу вычетов mod d, будут принадлежать одному и тому же роду. Таким образом каждый род будет состоять из $\frac{1}{2}\varphi(d)$ классов вычетов mod d, взаимно простых с d. Пусть, скажем, $a_1, \ldots, a_m$ $\left(m = \frac{1}{2}\varphi(d)\right)$ — несравнимые mod d числа, принадлежащие тому же роду, что и 1 (среди них содержатся все квадратичные вычеты mod d); закон разложения может быть тогда формулирован следующим образом:

Пусть p — положительное число, взаимно простое с d, и f — наименьший положительный показатель, для которого p^f сравнимо с одним из чисел $a_1, \ldots, a_m$ по модулю d. Тогда p разлагается в $k(\sqrt{d})$ на $\frac{2}{f}$ различных простых идеалов; каждый из них имеет степень f.

Если, в частности, d — нечетное простое число, $d = (-1)^{\frac{q-1}{2}} q$, то, в силу формулы (126), $\left(\frac{d}{n}\right) = \left(\frac{n}{q}\right)$; кроме того, в силу формулы (31) (§ 16),

$$\left(\frac{n}{q}\right) \equiv n^{\frac{q-1}{2}} \pmod{q}.$$

Поэтому показатель f, о котором перед этим шла речь, является наименьшим положительным числом, для которого

$$p^{f\frac{q-1}{2}} \equiv 1 \pmod{q}.$$

§ 47. Группа норменных вычетов

Квадратичное поле $k(\sqrt{d})$ порождает в области рациональных чисел определенную группу классов вычетов по каждому модулю n. Именно, пусть n — целое рациональное число. Рассмотрим в группе $\mathfrak{R}(n)$ классов вычетов mod n, взаимно простых с n, те классы вычетов, которые могут быть представлены нормами целых чисел поля $k(\sqrt{d})$. Эти классы образуют, очевидно, подгруппу группы $\mathfrak{R}(n)$; она называется *группой норменных вычетов* mod n (для поля $k(\sqrt{d})$) и обозначается через $\mathfrak{N}(n)$. Целое рациональное a, взаимно простое с n, называется *норменным вычетом* mod n, если в поле k существует такое целое число α, что

$$a \equiv N(\alpha) \pmod{n};$$

в противном случае a называется *норменным невычетом* mod n. (Таким образом числа a, не взаимно простые с n, совершенно не принимаются во внимание.)

Оказывается, что, вообще говоря, группы $\mathfrak{N}(p)$ и $\mathfrak{N}(p)$ совпадают, они различны лишь если простое число p входит в дискриминант d.

Теорема 138. *Если нечетное простое число p не входит в дискриминант d, то каждое целое рациональное число, не делящееся на p, есть норменный вычет* mod p *для* $k(\sqrt{d})$.

При доказательстве этой теоремы мы будем различать два случая:

1. p разлагается в $k(\sqrt{d})$ на два различные множителя первой степени $\mathfrak{p}$ и $\mathfrak{p}'$. Тогда в $k(\sqrt{d})$ существует целое число π, делящееся на $\mathfrak{p}$ и не делящееся на $\mathfrak{p}'$, и для каждого целого α имеем

$$N(\pi'\alpha+\pi)\equiv\pi'^2\alpha \pmod{\mathfrak{p}}.$$

Отсюда явствует, что рациональные числа $N(\pi'\alpha+\pi)$ пробегают полную систему вычетов mod $\mathfrak{p}$ и, значит, также mod p, когда α пробегает полную систему вычетов mod $\mathfrak{p}$.

2. p остается неразложимым в $k(\sqrt{d})$ и, значит, является простым идеалом второй степени. Пусть ρ — первообразный корень mod p в $k(\sqrt{d})$. Тогда прежде всего

$$\rho^p\equiv\rho' \pmod{p}, \text{ следовательно, } N(\rho)\equiv\rho^{p-1} \pmod{p}. \quad (128).$$

В самом деле, если $f(x)=x^2+ax+b$ — квадратный трехчлен с целыми рациональными коэфициентами, имеющий корнями ρ, ρ', то функциональное сравнение

$$f(r)^p\equiv f(x^p) \pmod{p}$$

показывает, что

$$0\equiv f(\rho^p)\equiv(\rho^p-\rho)(\rho^p-\rho') \pmod{p},$$

откуда и следует (128), поскольку ρ^p не может быть сравнимо с ρ mod p. Из (128) получаем

$$N(\rho^a)\equiv\rho^{a(p-1)} \pmod{p},$$

причем для $a=1, 2, \ldots, p-1$ получаются числа различных классов вычетов, поскольку две степени числа ρ могут принадлежать одному и тому же классу лишь когда показатели этих степеней сравнимы по модулю $N(p)-1$, т. е. по модулю p^2-1. Таким образом нормы $N(\rho^a)$, $a=1, \ldots, p-1$, пробегают все рациональные классы вычетов mod p, взаимно простые с p.

Теорема 139. *Если нечетное простое число q входит множителем в дискриминант d поля $k(\sqrt{d})$, то норменные вычеты* mod q *составляют точно половину классов группы $\mathfrak{N}(q)$; это суть те классы из $\mathfrak{N}(q)$, которые могут быть представлены в виде квадрата некоторого класса.*

В самом деле, пусть $\mathfrak{q}$ — простой идеал из $k(\sqrt{d})$, делящий q. Так как $\mathfrak{q}$ имеет первую степень, то, в силу теоремы 85, каждое целое α из k сравнимо с некоторым рациональным числом r по модулю $\mathfrak{q}$. Но из $\alpha \equiv r \pmod{\mathfrak{q}}$, в силу $\mathfrak{q} = \mathfrak{q}'$, следует также $\alpha' \equiv r \pmod{\mathfrak{q}}$ и, значит,

$$N(\alpha) \equiv r^2 \pmod{\mathfrak{q}},$$

следовательно, также

$$N(\alpha) \equiv r^2 \pmod{q},$$

т. е., если $(r, q) = 1$,

$$\left(\frac{N(\alpha)}{q}\right) = +1.$$

Обратно, если выполнено условие $\left(\frac{a}{q}\right) = +1$, то существует целое рациональное x, удовлетворяющее сравнению $a \equiv x^2 \pmod{q}$ или $a \equiv N(x) \pmod{q}$, и, значит, a есть норменный вычет.

Лемма. *Пусть* $(m, n) = 1$ *и* α *— целое рациональное. Если в поле* $k(\sqrt{d})$ *существуют такие два целых числа* α, β, *что*

$$\alpha \equiv N(\alpha) \pmod{m} \quad \text{и} \quad \alpha \equiv N(\beta) \pmod{n},$$

то в $k(\sqrt{d})$ *существует также целое число* γ *такое, что*

$$\alpha \equiv N(\gamma) \pmod{mn}.$$

В самом деле, пусть b, c — положительные показатели, для которых

$$m^b \equiv 1 \pmod{n}, \quad n^c \equiv 1 \pmod{m}$$

(например, $b = \varphi(n)$, $c = \varphi(m)$). Тогда, как нетрудно убедиться, число

$$\gamma = n^c\alpha + m^b\beta$$

будет обладать требуемым свойством.

Что касается простого числа 2, то мы должны рассмотреть группу $\mathfrak{R}(2^a)$ при $a = 2$ и 3, ибо 2 может входить в дискриминант d квадратичного поля самое большее в третьей степени.

Теорема 140. *Если дискриминант* d *поля* $k(\sqrt{d})$ *нечетен, то каждое нечетное число является норменным вычетом* mod 8. *Если же* d *четно, то точно половина всех несравнимых* mod 8 *нечетных чисел будет представлять норменные вычеты* mod 8.

Доказательство мы осуществим путем непосредственного испробования классов вычетов mod 8 в $k(\sqrt{d})$. Пусть d нечетно. Полагая в $\alpha = x + y\sqrt{d}$ соответственно

$$x = 0,\ 1,\ 2,\ 1,$$

$$y = 1,\ 0,\ 1,\ 2,$$

получим

$$N(\alpha) \equiv 3,\ 1,\ 7,\ 5 \pmod 8 \quad \text{при } d \equiv 5 \pmod 8,$$
$$N(\alpha) \equiv 7,\ 1,\ 3,\ 5 \pmod 8 \quad \text{при } d \equiv 1 \pmod 8,$$

чем первая часть теоремы и доказана.

Таким же образом доказывается и вторая часть теоремы. В качестве норменных вычетов mod 8 при четных d выступают только следующие классы вычетов mod 8:

$$\left.\begin{aligned} N(\alpha) &\equiv 1 \text{ или } 5 \pmod 8, \text{ если } \frac{d}{4} \equiv 3 \pmod 4, \\ N(\alpha) &\equiv 1 \text{ или } -1 \pmod 8, \text{ если } \frac{d}{4} \equiv 2 \pmod 8, \\ N(\alpha) &\equiv 1 \text{ или } 3 \pmod 8, \text{ если } \frac{d}{4} \equiv 6 \pmod 8. \end{aligned}\right\} \tag{129}$$

Мы видим, кроме того, что при $\frac{d}{4} \equiv 3 \pmod 4$ все норменные вычеты mod 4 содержатся в классе вычетов mod 4, представляемом числом 1, так что также $\mathfrak{N}(4)$ *отлично от* $\mathfrak{N}(4)$.

Обнаруженное нами положение вещей можно несколько нагляднее выразить с помощью понятий общей теории групп, развитых в § 10. Нас будут интересовать норменные вычеты по делителям дискриминанта d. Пусть $q_1, q_2, \ldots, q_t$ будут t различных входящих в d положительных простых чисел, с тем исключением, что в случае четного d число q_t означает наивысшую входящую в d степень двойки. Тогда для каждого $i = 1, \ldots, t$ группа $\mathfrak{N}(q_i)$ норменных вычетов в $k(\sqrt{d})$ является подгруппой индекса 2 группы $\mathfrak{R}(q_i)$. Поэтому принадлежность какого-либо класса из $\mathfrak{R}(q_i)$ к этой подгруппе будет, в силу теоремы 33, характеризоваться тем, что для этого класса некоторый вполне определенный характер χ_i группы $\mathfrak{R}(q_i)$ принимает значение 1. Этот характер $\chi_i(n)$ легко определяется. Именно, прежде всего мы видим, что, в силу теоремы 139,

$$\chi_i(n) = \left(\frac{n}{q_i}\right), \text{ если } q_i \text{ нечетно.} \tag{130}$$

Далее, группа $\mathfrak{R}(8)$ имеет два базисных класса, каждый второго порядка, следовательно, она имеет три различных подгруппы индекса 2, и, как показывает таблица (129), каждая из них может представлять собой $\mathfrak{N}(8)$. Три отличных от 1 квадратичных характера mod 8 суть

$$(-1)^{\frac{n-1}{2}}, \quad (-1)^{\frac{n^2-1}{8}}, \quad (-1)^{\frac{n-1}{2}+\frac{n^2-1}{8}},$$

и получаем, таким образом, в случае четного d последний характер:

$$\left.\begin{aligned} \chi_t(n) &= (-1)^{\frac{n-1}{2}}, && \text{если } \frac{d}{4} \equiv 3 \pmod 4, \\ &= (-1)^{\frac{n^2-1}{8}}, && \text{если } \frac{d}{4} \equiv 2 \pmod 8, \\ &= (-1)^{\frac{n-1}{2}+\frac{n^2-1}{8}}, && \text{если } \frac{d}{4} \equiv 6 \pmod 8. \end{aligned}\right\} \tag{131}$$

Все эти случаи могут быть охвачены одной формулой:

$$\chi_t(n) = (-1)^{a\frac{n^2-1}{8}+\frac{d'-1}{2}\frac{n-1}{2}}, \text{ если } d = 2^a d',\ a > 0,\ d' \text{ нечетно.} \quad (132)$$

Принимая во внимание доказанную выше лемму, мы можем резюмировать полученные результаты в виде следующей теоремы:

Теорема 141. *Группа $\mathfrak{N}(d)$ норменных вычетов* $\bmod d$ *для квадратичного поля с дискриминантом d является подгруппой индекса 2^t группы $\mathfrak{N}(d)$, где t означает число различных простых делителей d. Для того чтобы число n было норменным вычетом* $\bmod d$, *необходимо и достаточно, чтобы t характеров χ_i ($i = 1, \ldots, t$), определяемых формулами* (130) *и* (132), *принимали для аргумента n значение* $+1$.

Для облегчения пользования литературой по этому вопросу заметим, что Гильберт определил понятие норменного вычета $\bmod p$ также для чисел n, не взаимно простых с p, причем его определение и в остальных случаях отлично по форме от данного выше.

Определение гильбертова символа норменных вычетов. Пусть n, m — целые рациональные числа, m — не квадрат, p — простое число (допускается также $p = 2$). Если тогда число n сравнимо по каждой степени p^e с нормой какого-нибудь целого числа из $k(\sqrt{m})$, то полагаем

$$\left(\frac{n, m}{p}\right) = +1$$

и называем n норменным вычетом поля $k(\sqrt{m})$ $\bmod p$. Во всех остальных случаях считаем $\left(\frac{n, m}{p}\right)$ равным -1 и называем n норменным невычетом $\bmod p$.

Если n не делится на p и p — один из простых делителей дискриминанта d поля $k(\sqrt{m})$, то

$$\left(\frac{n, d}{q_i}\right) = \chi_i(n) \qquad (q_i \text{ нечетно}),$$

$$\left(\frac{n, d}{2}\right) = \chi_t(n) \qquad (d \text{ четно}).$$

Если, напротив, p не делит nd, то $\left(\frac{n, d}{p}\right) = +1$.

§ 48. Группа норм идеалов и группа родов. Определение числа родов

Таким же образом, как нормы чисел, мы можем исследовать также нормы идеалов. Классы вычетов $\bmod d$, могущие быть представлены нормами целых взаимно простых с d идеалов поля $k(\sqrt{d})$, образуют, очевидно, подгруппу группы $\mathfrak{N}(d)$. Она называется *группой норм идеалов* $\bmod d$ и будет обозначаться через $\mathfrak{J}(d)$. $\mathfrak{N}(d)$ является подгруппой группы $\mathfrak{J}(d)$. В самом деле, если некоторый класс вычетов $\bmod d$ может быть представлен нормой $N(\alpha)$ числа α, то $N(\alpha + dx)$

для всех целых рациональных x будет принадлежать тому же классу; для достаточно большого x он будет, очевидно, положительным и, значит, будет являться нормой главного идеала $(\alpha + dx)$.

Так как структура группы $\mathfrak{N}(d)$ уже известна нам из теоремы 141, то для определения структуры группы $\mathfrak{J}(d)$ остается еще исследовать факторгруппу $\mathfrak{J}/\mathfrak{N}$. Так как порядок $\mathfrak{N}$ равен $\frac{\varphi(d)}{2^t}$, то порядок $\mathfrak{J}(d)$ есть кратное этого числа; с другой стороны, порядок $\mathfrak{J}(d)$ является делителем порядка $\varphi(d)$ группы $\mathfrak{N}(d)$; отсюда следует, что порядок факторгруппы $\mathfrak{J}/\mathfrak{N}$ равен 2^u, где целое число $u \leqslant t$. Первым нашим основным результатом будет установление равенства $u = t-1$, вторым — обнаружение связи этой факторгруппы $\mathfrak{J}/\mathfrak{N}$ с группой классов идеалов и теоремой 132.

Факторгруппа $\mathfrak{J}/\mathfrak{N}$ получится, если нормы идеалов, отличающиеся друг от друга $\bmod d$ лишь нормами чисел из k в качестве множителей, рассматривать как неразличные. Этим путем получается разбиение идеалов, выражаемое следующим определением:

Два целых идеала $\mathfrak{a}$, $\mathfrak{b}$ из k, взаимно простых с d, мы будем причислять к одному и тому же *роду*, если в k существует такое целое число α, что

$$|N(\mathfrak{a})| \equiv N(\alpha)\,|N(\mathfrak{b})| \pmod{d}.$$

Роды в k естественным образом объединяются в абелеву *группу родов*, где произведение родов G_1, G_2 определяется как род, которому принадлежит произведение $\mathfrak{a}_1\mathfrak{a}_2$ идеалов $\mathfrak{a}_1$, $\mathfrak{a}_2$ соответственно из G_1, G_2. Группа родов, очевидно, изоморфна факторгруппе $\mathfrak{J}/\mathfrak{N}$. Единичный элемент группы родов называется *главным родом*; он содержит идеал 1 и, следовательно, главные идеалы в узком смысле. Идеалы, эквивалентные в узком смысле, очевидно, принадлежат одному и тому же роду, если они взаимно просты с d. Поэтому каждый род состоит из некоторого числа классов идеалов в узком смысле. Так как классы, принадлежащие к главному роду, — пусть их число будет f, — очевидно, образуют подгруппу группы классов в узком смысле, то f есть делитель числа h_0, и каждый род содержит точно f классов. Обозначая через g число различных родов, имеем, таким образом,

$$h_0 = gf.$$

Квадрат каждого рода есть главный род, ибо для каждого идеала $\mathfrak{a}$, полагая $a = N(\mathfrak{a})$, имеем

$$N(\mathfrak{a}^2) = N(a).$$

Следовательно, порядок g группы родов должен быть степенью двойки, $g = 2^u$, что мы выше уже нашли для группы $\mathfrak{J}/\mathfrak{N}$. Но теперь мы можем утверждать уже нечто более определенное насчет величины u; число различных классов, представимых в виде квадратов, в силу теорем 29 и 132, равно $\frac{h_0}{2^{t-1}}$, поэтому

$$f \geqslant \frac{h_0}{2^{t-1}}, \quad g = \frac{h_0}{f} \leqslant 2^{t-1}, \quad u \leqslant t-1. \tag{133}$$

В целях доказательства равенства $u = t - 1$ мы будем строить теперь для группы родов групповые характеры. Эти последние сразу получаются из t функций $\chi_i(n)$ предыдущего параграфа. $\chi_i(n)$ имеют для каждого норменного вычета $n \bmod d$ значение 1. Положим теперь для каждого целого идеала $\mathfrak{a}$ из $k(\sqrt{d})$, взаимно простого с d,

$$\gamma_i(\mathfrak{a}) = \chi_i(N(\mathfrak{a})) \quad (i = 1, \ldots, t). \tag{134}$$

Тогда каждая из t функций $\gamma_i(\mathfrak{a})$ будет иметь для всех идеалов из одного и того же рода одинаковое значение. Так как, кроме того, $\gamma_i(\mathfrak{ab}) = \gamma_i(\mathfrak{a})\gamma_i(\mathfrak{b})$, то оказывается справедливой

Теорема 142. *t функций* (134) $\gamma_i(\mathfrak{a})$ *суть групповые характеры рода, представляемого идеалом* $\mathfrak{a}$.

Теперь, согласно § 10, группа характеров абелевой группы изоморфна этой абелевой группе. Но в группе родов имеется u и не более чем u независимых элементов, ибо эта группа имеет порядок 2^u и все ее элементы (кроме единичного) — второго порядка. Следовательно, имеется так же точно u независимых характеров. Поэтому между t характерами $\gamma_i(\mathfrak{a})$ должно существовать по крайней мере $t - u$ соотношений. Иными словами, так как $t - u \geqslant 1$, имеет место

Теорема 143. *Для всех взаимно простых с d идеалов $\mathfrak{a}$ поля $k(\sqrt{d})$ имеет место по крайней мере одно соотношение вида*

$$\prod_{i=1}^{t} \gamma_i^{c_i}(\mathfrak{a}) = 1,$$

где c_i — не зависящие от $\mathfrak{a}$ целые рациональные числа, не делящиеся одновременно на 2.

Таким образом при $t = 1$ должно иметь место равенство

$$\gamma_1(\mathfrak{a}) = \chi_1(N(\mathfrak{a})) = 1.$$

Но это в действительности есть как раз часть квадратичного закона взаимности, на который мы до сих пор в §§ 47 и 48 не опирались. Мы видим, что доказательство этого равенства по сути основывается на нечетности h_0 для полей с $t = 1$, как и наше доказательство в § 46.

Теперь мы, напротив, из квадратичного закона взаимности выведем равенство

$$\prod_{i=1}^{t} \gamma_i(\mathfrak{a}) = 1. \tag{135}$$

Для этого покажем, что для каждого целого положительного n, взаимно простого с d, выполняется соотношение

$$\prod_{i=1}^{t} \chi_i(n) = \left(\frac{d}{n}\right). \tag{136}$$

Именно, для нечетных d имеем

$$\prod_{i=1}^{t}\chi_i(n)=\prod_{i=1}^{t}\left(\frac{n}{q_i}\right)=\left(\frac{n}{q_1\dots q_t}\right)=\left(\frac{n}{d}\right),$$

что, в силу (127), равно обратному символу $\left(\frac{d}{n}\right)$. Если же $q_t=2^a$ $(a>0)$ и $d=2^a d'$, то имеем

$$\prod_{i=1}^{t-1}\chi_i(n)=\left(\frac{n}{d'}\right),\quad \chi_t(n)=(-1)^{a\frac{n^2-1}{8}+\frac{d'-1}{2}\frac{n-1}{2}},$$

что, в силу (126), снова дает (136).

Но отсюда немедленно вытекает соотношение (135) для простых идеалов первой степени, ибо для таких $\mathfrak{a}=\mathfrak{p}$, в силу законов разложения, $\left(\frac{d}{N(\mathfrak{p})}\right)=+1$. Если, далее, $\mathfrak{a}$ — простой идеал второй степени, то $N(\mathfrak{a})$ есть рациональный квадрат и потому $\chi_i(\mathfrak{a})=1$ для всех i. Так как соотношение (135), как мы видим, справедливо для каждого простого идеала, не входящего в d, то оно справедливо также для всех $\mathfrak{a}$, взаимно простых с d.

Тот факт, что число родов g точно равно 2^{t-1}, мы теперь удобнее всего докажем, показав, с помощью трансцендентных методов, что t характеров $\chi_i(\mathfrak{a})$ связаны только соотношением (135), поэтому существует $t-1$ независимых характеров $\chi_i(\mathfrak{a})$ группы родов, порядок которой, таким образом, по меньшей мере равен 2^{t-1}, а следовательно, в силу (133), точно равен 2^{t-1}.

То, что между характерами $\chi_i(\mathfrak{a})$ не может существовать никакого соотношения, отличного от (135), показывает

Теорема 144. *Пусть* $e_i=\pm 1$ $(i=1,\dots,t)$, *причем*

$$e_1e_2\dots e_t=1.$$

Существует бесконечное множество простых идеалов $\mathfrak{p}$ *первой степени поля* $k(\sqrt{d})$, *характеры которых удовлетворяют равенствам*

$$\chi_i(\mathfrak{p})=e_i\quad (i=1,\dots,t).$$

Положим $N(\mathfrak{p})=p$, тогда утверждение теоремы, очевидно, гласит следующее: существует бесконечное множество рациональных простых чисел p, удовлетворяющих условиям

$$\chi_i(p)=e_i\quad (i=1,\dots,t)\quad\text{и}\quad\left(\frac{d}{p}\right)=+1.$$

Последнее условие, в силу равенств (136) и $e_1e_2\dots e_t=+1$, является следствием первых t условий, которые только мы и должны поэтому принимать во внимание.

Так как каждое $\chi_i(n)$ является характером $\bmod q_i$, то равенство

$$\chi_i(n)=e_i$$

означает, что n должно принадлежать некоторым определенным классам вычетов $\bmod q_i$, а такие целые рациональные n всегда существуют. Одновременное же наличие t равенств $\chi_i(n) = e_i$ $(i = 1, \ldots, t)$ означает, что n должно относительно каждого из t модулей q_i принадлежать определенным классам вычетов; по теореме 15 это значит, что n принадлежит определенным классам $\bmod q_1 q_2 \ldots q_t$, т. е. $\bmod d$ (разумеется взаимно простым с d). Но в каждом взаимно простом с d классе вычетов $\bmod d$ существует, по теореме 131, бесконечное множество положительных рациональных простых чисел, и тем самым наше утверждение доказано.

Существование указанных простых чисел было доказано в § 43 с помощью теории поля корней d-й степени из 1. Важное значение имеет то обстоятельство, что, как мы это покажем в § 49, существование бесконечного множества простых чисел p, удовлетворяющих условиям $\chi_i(p) = e_i$, можно доказать также с помощью одной только теории квадратичных полей (но тоже трансцендентными методами).

Из теоремы 144, как было выше указано, вытекает, что $g = 2^{t-1}$, значит, $f = \frac{h_0}{2^{t-1}}$, иными словами, число классов, содержащихся в главном роде, равно числу классов идеалов, представимых в виде квадратов классов. Тем самым доказана

Теорема 145. (Фундаментальная теорема о родах.) *Число родов в квадратичном поле с дискриминантом d равно 2^{t-1}. Любые $t-1$ из функций*

$$\gamma_i(\mathfrak{a}) = \chi_i(N(\mathfrak{a})) \quad (i = 1, \ldots, t)$$

образуют полную систему независимых характеров группы родов. Для того чтобы класс идеалов был квадратом, необходимо и достаточно, чтобы он принадлежал главному роду.

Эта теорема была впервые найдена Гауссом, давшим для нее чисто арифметическое доказательство. Подобное доказательство изложено также в гильбертовом отчете.

Из последней части теоремы 145 заключаем еще, что для того чтобы идеал $\mathfrak{a}$, взаимно простой с d, был эквивалентен квадрату какого-либо идеала, необходимо и достаточно, чтобы $N(\mathfrak{a})$ был норменным вычетом $\bmod d$, т. е. чтобы было разрешимо в целых рациональных x сравнение

$$N(\mathfrak{a}) \equiv x^2 \pmod{d}.$$

Но тогда норма идеала $N(\mathfrak{a})$ будет также нормой целого или дробного числа поля $k(\sqrt{d})$, ибо из $\mathfrak{a} \approx \mathfrak{b}^2$ вытекает существование числа α поля $k(\sqrt{d})$, такого, что

$$\mathfrak{a} = \alpha\mathfrak{b}^2, \quad N(\alpha) > 0,$$

откуда

$$N(\mathfrak{a}) = N(\alpha)\,N(\mathfrak{b}^2) = N(\alpha)\,N(\mathfrak{b})^2 = N(\alpha b), \quad \text{где } b = N(\mathfrak{b}).$$

§ 49. Дзета-функция поля $k(\sqrt{d})$ и существование простых чисел с заданными квадратичными характерами

В целях выражения дзета-функции $\zeta_k(s)$ поля $k(\sqrt{d})$ через более простые функции рассмотрим в бесконечном произведении

$$\zeta_k(s)=\prod_{\mathfrak{p}}\frac{1}{1-N(\mathfrak{p})^{-s}}$$

часть, распространенную на простые идеалы $(\mathfrak{p})$, входящие в некоторое определенное рациональное простое число p. Из законов разложения следует, что эта часть

$$\prod_{\mathfrak{p}|p}(1-N(\mathfrak{p})^{-s})^{-1}=(1-p^{-s})^{-1}\left(1-\left(\frac{d}{p}\right)p^{-s}\right)^{-1}.$$

Тем самым $\zeta_k(s)$ при $s>1$ представляется в виде произведения

$$\zeta_k(s)=\prod_{p}\frac{1}{1-p^{-s}}\cdot\prod_{p}\frac{1}{1-\left(\frac{d}{p}\right)p^{-s}},$$

где p пробегает все положительные простые числа. Таким образом

$$\zeta_k(s)=\zeta(s)\,L(s),$$

где

$$L(s)=\prod_{p}\frac{1}{1-\left(\frac{d}{p}\right)p^{-s}}. \tag{137}$$

Подставляя это выражение функции $\zeta_k(s)$ в формулу для числа классов (95), получаем

$$h\varkappa=\lim_{s\to 1}L(s). \tag{138}$$

Отсюда заключаем, что при $s\to 1$ $L(s)$ стремится к конечному пределу, отличному от 0. Из этого факта мы выведем, подобно § 43, некоторые следствия относительно распределения символа $\left(\frac{d}{p}\right)$. Из (138) вытекает, что

$$\lim_{s\to 1}\ln L(s)\ \text{конечен}. \tag{139}$$

Так же как в § 43 для $L(s,\chi)$, находим

$$\ln L(s)=-\sum_{p}\ln\left(1-\left(\frac{d}{p}\right)p^{-s}\right)=\sum_{p}\sum_{m=1}^{\infty}\frac{1}{mp^{ms}}\left(\frac{d}{p}\right)^{m}=$$

$$=\sum_{p}\left(\frac{d}{p}\right)\frac{1}{p^{s}}+H(s),$$

где $H(s)$ — ряд Дирихле, сходящийся при $s > \frac{1}{2}$ и, следовательно, имеющий предел при $s \to 1$. Поэтому, в силу (139),

$$\lim_{s \to 1} \sum_{p} \left(\frac{d}{p}\right) \frac{1}{p^s} \quad \text{конечен.} \tag{140}$$

Это утверждение, очевидно, остается в силе, если опустить любое конечное число членов суммы и, следовательно, также если заменить d целым числом, отличающимся от d рациональным квадратным множителем. Тем самым мы получаем следующий результат:

Теорема 146. *Функция*

$$L(s; a) = \sum_{p > 2} \left(\frac{a}{p}\right) \frac{1}{p^s},$$

где a — любое положительное или отрицательное целое рациональное число, не являющееся квадратом, при $s \to 1$ стремится к конечному пределу.

Отсюда с помощью формальных соображений, сходных с примененными в § 43, получается

Теорема 147. *Пусть $a_1, a_2, \ldots, a_r$ — любые целые рациональные числа, подчиненные тому условию, что произведение их степеней*

$$a_1^{u_1} a_2^{u_2} \ldots a_r^{u_r}$$

лишь тогда является рациональным квадратом, когда все u четны. Далее, пусть $c_1, c_2, \ldots, c_r$ — произвольно заданные значения ± 1. Тогда существует бесконечное множество простых чисел p, удовлетворяющих условиям

$$\left(\frac{a_i}{p}\right) = c_i \qquad (i = 1, \ldots, r). \tag{141}$$

Для доказательства положим

$$L(s; 1) = \sum_{p > 2} \frac{1}{p^s}$$

(функция, по § 43 безгранично возрастающая при $s \to 1$) и образуем сумму из 2^r членов ($s > 1$)

$$\sum_{u_1, \ldots, u_r} c_1^{u_1} c_2^{u_2} \ldots c_r^{u_r} L(s;\ a_1^{u_1} a_2^{u_2} \ldots a_r^{u_r}) = \varphi(s), \tag{142}$$

где каждое u_i пробегает значения 0, 1. В силу определения функций L имеем

$$\varphi(s) = \sum_{p > 2} \left(1 + c_1\left(\frac{a_1}{p}\right)\right)\left(1 + c_2\left(\frac{a_2}{p}\right)\right) \ldots \left(1 + c_r\left(\frac{a_r}{p}\right)\right) \frac{1}{p^s}. \tag{143}$$

В этой сумме лишь те члены p^{-s} имеют отличный от нуля коэффициент (именно, равный 2^r), у которых p удовлетворяет условию (141) утверждения теоремы, если отвлечься от конечного числа p, входящих в a. Но

$$\lim_{s\to 1}\varphi(s)=\infty,$$

так как в сумме (142) $L(s;1)$ безгранично возрастает, тогда как все остальные $L(s;a)$, в силу нашего предположения и теоремы 146, остаются конечными. Отсюда следует, что в (143) должно содержаться бесконечное множество отличных от нуля членов, чем наша теорема и доказана.

В частности, при $r=1$ получаем:

В каждом квадратичном поле существует бесконечное множество простых идеалов как первой, так и второй степени.

Выбираем, в обозначениях предыдущего параграфа, $a_i=\pm q_i$ и $r=t$, так чтобы каждое a_i само было дискриминантом поля и произведение $a_1a_2\ldots a_t$ было равно d. Так как, в силу формулы (136), примененной к каждому отдельному полю $k(\sqrt{a_i})$,

$$\chi_i(p)=\left(\frac{a_i}{p}\right)\qquad (i=1,\ldots,t),$$

то, опираясь на теорему 147, мы получаем доказательство теоремы 144 предыдущего параграфа без помощи теоремы Дирихле о простых числах в арифметических прогрессиях, т. е. без помощи теории полей деления круга.

§ 50. Определение числа классов поля $k(\sqrt{d})$ без помощи дзета-функции

Мы перейдем теперь к определению числа h классов идеалов (в широком смысле) по методам главы VI. Сначала мы выполним это, следуя § 41, исходя из одной лишь плотности идеалов без применения $\zeta_k(s)$, а затем применим для той же цели формально более изящный метод теоремы 125, опирающийся на знание $\zeta_k(s)$.

Для первого способа требуется вычислить значение функции $F(n)$ — числа целых идеалов поля с нормой n. Согласно формуле (89), для взаимно простых a, b имеет место равенство $F(ab)=F(a)F(b)$.

Лемма. *Для каждой степени простого числа p^k*

$$F(p^k)=\sum_{i=0}^{k}\left(\frac{d}{p^i}\right)=1+\sum_{i=1}^{k}\left(\frac{d}{p}\right)^i. \tag{144}$$

Случай a): $\left(\frac{d}{p}\right)=-1$. Если $N(\mathfrak{a})=p^k$, то $\mathfrak{a}$ должно быть равно p^u с положительным целым рациональным u, поэтому $2u=k$, т. е.

$$F(p^k)=\begin{cases}1, & \text{если } k \text{ четно},\\ 0, & \text{если } k \text{ нечетно},\end{cases}$$

в согласии с утверждением (144).

Случай b): $\left(\frac{d}{p}\right)=0$. p есть квадрат простого идеала $\mathfrak{p}$ и из $N(\mathfrak{a})=p^k$ вытекает $\mathfrak{a}=\mathfrak{p}^u$, $u=k$, $F(p^k)=1$.

Случай c): $\left(\frac{d}{p}\right)=+1$. p есть произведение двух различных простых идеалов $\mathfrak{p}$, $\mathfrak{p}'$, и из $N(\mathfrak{a})=p^k$ следует $\mathfrak{a}=\mathfrak{p}^u\mathfrak{p}'^{u'}$ с $u+u'=k$. Поэтому $k+1$ пар чисел u, $k-u$ $(u=0, 1, \ldots, k)$ дают все различные идеалы $\mathfrak{a}$ требуемого вида, и

$$F(p^k)=k+1,$$

как и утверждается в лемме.

Теорема 148. *Для каждого натурального n*

$$F(n)=\sum_{m\mid n}\left(\frac{d}{m}\right),$$

где m пробегает все различные положительные делители числа n.

Действительно, пусть

$$n=p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}$$

— разложение n на различные простые множители. Тогда

$$F(n)=F(p_1^{k_1})F(p_2^{k_2})\ldots F(p_r^{k_r})=\prod_{i=1}^{r}\sum_{c_i=0}^{k_i}\left(\frac{d}{p_i^{c_i}}\right)=$$

$$=\sum_{\substack{c_1=0,\ldots,k_1\\ c_2=0,\ldots,k_2\\ \ldots\ldots}}\left(\frac{d}{p_1^{c_1}p_2^{c_2}\ldots p_r^{c_r}}\right)=\sum_{m\mid n}\left(\frac{d}{m}\right)$$

Мы положим во всем дальнейшем

$$\left(\frac{d}{n}\right)=\chi(n)\qquad(n>0),$$

указывая этим на то доказанное уже теоремой 137 обстоятельство, что $\left(\frac{d}{n}\right)$ для *положительных* n является характером mod d.

Внося теперь найденное для $F(n)$ выражение в формулу (88) § 41, мы получаем

$$h\varkappa=\lim_{x\to\infty}\frac{1}{x}\sum_{n\leqslant x}F(n)=\lim_{x\to\infty}\frac{1}{x}\sum_{n\leqslant x}\sum_{m\mid n}\chi(m).$$

Положим теперь $n = mm'$ (с целым m'), так что

$$\sum_{n \leqslant x} F(n) = \sum_{\substack{m,\, m' > 0 \\ mm' \leqslant x}} \chi(m),$$

где, следовательно, m, m' пробегают все натуральные числа, произведение которых не превосходит x. Таким образом при каждом фиксированном m число m' пробегает все целые значения из интервала

$$1 \leqslant m' \leqslant \frac{x}{m},$$

в количестве $\left[\frac{x}{m}\right]$, где $[u]$ означает наибольшее целое рациональное число, не превосходящее u. Тем самым получаем

$$\sum_{1 \leqslant n \leqslant x} F(n) = \sum_{1 \leqslant m \leqslant x} \chi(m) \left[\frac{x}{m}\right] =$$

$$= x \sum_{1 \leqslant m \leqslant x} \frac{\chi(m)}{m} + \sum_{1 \leqslant m \leqslant x} \chi(m) \left(\left[\frac{x}{m}\right] - \frac{x}{m}\right).$$

После деления на x первая сумма в правой части при $x \to \infty$ стремится к пределу

$$\sum_{m=1}^{\infty} \frac{\chi(m)}{m},$$

ибо этот ряд, по теореме 128, сходится при $s = 1$ как ряд $L(s, \chi)$. Следовательно,

$$h\varkappa = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} + \lim_{x \to \infty} \frac{1}{x} \sum_{1 \leqslant n \leqslant x} \chi(n) \left(\left[\frac{x}{n}\right] - \frac{x}{n}\right).$$

Но последний предел равен нулю, в силу следующей общей теоремы [1]):

Пусть последовательность коэфициентов $a_1, a_2, \ldots$ такова, что

$$\lim_{x \to \infty} \frac{1}{x} \sum_{n \leqslant x} a_n = 0 \quad \text{и} \quad \sum_{n \leqslant x} |a_n| \leqslant x \quad \text{для всех } x > 0.$$

Тогда

$$\lim_{x \to \infty} \frac{1}{x} \sum_{n \leqslant x} a_n \left(\left[\frac{x}{n}\right] - \frac{x}{n}\right) = 0.$$

Как мы видели при доказательстве теоремы 128, для последовательности $a_n = \chi(n)$ указанные условия действительно выполняются.

[1]) По поводу этой теоремы см. E. Landau, Über einige neuere Grenzwertsätze, Rendiconti del Circolo Matematico di Palermo, v. 34 (1912).

Тем самым имеем

$$h\varkappa = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}. \tag{145}$$

В следующем параграфе мы дадим более короткое доказательство этого равенства и подвергнем ряд в правой части дальнейшему исследованию.

§ 51. Определение числа классов с помощью дзета-функции

Мы уже представили в § 49 $\zeta_k(s)$ в виде $\zeta(s)L(s)$, где

$$L(s) = \prod_p \frac{1}{1-\chi(p)p^{-s}}, \tag{137}$$

и вывели отсюда, что

$$h\varkappa = \lim_{s\to 1} L(s). \tag{138}$$

Но так как $\chi(n)$ для натуральных n есть характер mod d, то определенная формулой (137) функция $L(s)$ совпадает с одной из функций $L(s,\chi)$ из § 43, и мы имеем

$$L(s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

откуда на основании теоремы 128 вытекает равенство

$$h\varkappa = L(1) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}, \tag{145}$$

выведенное уже нами в § 50 без помощи дзета-функции. Сравнивая два доказательства этой формулы, мы видим, что представление $\zeta_k(s)$ на основании законов разложения в виде $\zeta(s)L(s)$ по своему содержанию означает то же, что и вычисление $F(n)$ на основании теоремы 148.

Теперь для квадратичного поля с дискриминантом d

$$\varkappa = \frac{2\ln\varepsilon}{|\sqrt{d}|}, \quad \text{если } d>0,\ \varepsilon>1 \text{ — основная единица;}$$

$$\varkappa = \frac{2\pi}{w|\sqrt{d}|}, \quad \text{если } d<0 \ (w=2 \text{ при } d<-4).$$

Поэтому для положительных d из (145) вытекает замечательная

Теорема 149. *Выражение*

$$\varepsilon^{2h} = e^{\sqrt{d}\sum_{n=1}^{\infty}\left(\frac{d}{n}\right)\frac{1}{n}}$$

при $d>0$ представляет собой единицу бесконечного порядка поля $k(\sqrt{d})$. Эта единица является наибольшим из корней уравнения

$$x^2 - Ax + 1 = 0,$$

где

$$A = \varepsilon^{2h} + \varepsilon'^{2h} = \varepsilon^{2h} + \varepsilon^{-2h} = e^{\sqrt{d}\,L(1)} + e^{-\sqrt{d}\,L(1)}.$$

A (являющееся целым рациональным) может быть вычислено с помощью оценки остаточного члена сходящегося ряда $L(1)$, и тем самым мы имеем трансцендентный метод для нахождения единицы вещественного квадратичного поля.

Но сумма ряда $L(1)$ во всех случаях может быть представлена в легко обозримой форме; это дает, в частности, чрезвычайно простое выражение для h в мнимых квадратичных полях.

Так как $\chi(n)$ при $n>0$ является периодической функцией целого аргумента n с периодом $|d|$, то естественно возникает мысль представить $\chi(n)$ в виде конечного ряда Фурье. Для этой цели мы должны так определить $|d|$ величин c_n $(n=0, 1, \ldots, |d|-1)$, чтобы удовлетворялись уравнения

$$\chi(a) = \sum_{n=0}^{|d|-1} c_n \zeta^{an} \qquad \left(\zeta = e^{\frac{2\pi i}{|d|}}\right) \tag{146}$$

для

$$a = 0, 1, \ldots, |d|-1.$$

Эти $|d|$ линейных уравнений относительно c_n однозначно разрешимы, так как определитель коэфициентов ζ^{an} отличен от нуля. Для вычисления целесообразно определить $\chi(n)$ и c_n для любых, значит, также отрицательных целых рациональных n, полагая

$$\chi(n) = \chi(m) \quad \text{и} \quad c_n = c_m, \quad \text{если} \quad n \equiv m \pmod{d},$$

вследствие чего уравнения (146) будут удовлетворяться для всех целых рациональных a.

($\chi(n)$ при отрицательных n уже не будет иметь значения $\left(\frac{d}{n}\right)$, так как, согласно данному ранее определению, $\left(\frac{d}{n}\right) = \left(\frac{d}{-n}\right)$.)

По теореме 137

$$\chi(n) = \chi(-n)\operatorname{sgn} d; \tag{147}$$

отсюда получается аналогичное свойство и для c_n. Именно,

$$\chi(-a) = \sum_n c_n \zeta^{-an},$$

где n может пробегать любую полную систему вычетов mod d; так как то же справедливо тогда и для $-n$, то получаем отсюда

$$\chi(-a) = \sum_n c_{-n} \zeta^{an},$$

или, в силу (147),

$$\chi(a) = \sum_n c_{-n} \operatorname{sgn} d \cdot \zeta^{an}.$$

Так как c_n однозначно определяются из уравнений (146), то получаем

$$c_{-n} = c_n \operatorname{sgn} d. \tag{147a}$$

Вычисление коэфициентов c_n мы отложим до следующего параграфа. Но уже теперь мы можем представить $L(1)$ в существенно новой форме. Имеем

$$L(1) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \frac{1}{n} \sum_{q=0}^{|d|-1} c_q \zeta^{qn}.$$

Так как при $\zeta^q \neq 1$, $|\zeta| = 1$, как известно,

$$-\ln(1-\zeta^q) = \sum_{n=1}^{\infty} \frac{\zeta^{qn}}{n},$$

в частности, этот ряд сходится при $q \not\equiv 0 \pmod{d}$, то c_0 должно быть равно нулю, ибо $\sum_{n=1}^{\infty} \frac{1}{n}$ расходится, тогда как весь ряд для $L(1)$ сходится. Мы можем, таким образом, написать

$$L(1) = \sum_{q=1}^{|d|-1} c_q \sum_{n=1}^{\infty} \frac{\zeta^{qn}}{n}.$$

Объединяя здесь члены с q и $|d|-q$ и принимая во внимание (147a), мы получаем

$$L(1) = \frac{1}{2} \sum_{q=1}^{|d|-1} c_q \sum_{n=1}^{\infty} \frac{\zeta^{qn} + \operatorname{sgn} d \cdot \zeta^{-qn}}{n},$$

что при $d > 0$ и $d < 0$ дает два существенно различных выражения:

1. $d < 0$.

$$L(1) = i \sum_{q=1}^{|d|-1} c_q \sum_{n=1}^{\infty} \frac{\sin \frac{2\pi qn}{|d|}}{n}$$

Но, как известно,

$$\sum_{n=1}^{\infty} \frac{\sin 2\pi nx}{n} = \pi\left(\frac{1}{2} - x\right) \quad \text{для} \quad 0 < x < 1$$

Поэтому

$$L(1) = \frac{\pi i}{2} \sum_q c_q - \pi i \sum_{q=1}^{|d|-1} c_q \frac{q}{|d|}.$$

Здесь первая сумма равна нулю, в чем убеждаемся, положив в (146) $a=0$. Таким образом

$$L(1)=-\frac{\pi i}{|d|}\sum_{n=1}^{|d|-1} nc_n,$$

$$h=\frac{-w i}{2|\sqrt{d}|}\sum_{n=1}^{|d|-1} nc_n. \tag{148}$$

2. $d>0$.

$$L(1)=\frac{1}{2}\sum_{q=1}^{d-1} c_q \sum_{n=1}^{\infty}\frac{\zeta^{qn}+\zeta^{-qn}}{n}=-\sum_{q=1}^{d-1} c_q \Re \ln(1-\zeta^q)\ ^{1})=$$

$$=-\sum_{q=1}^{d-1} c_q \ln|1-\zeta^q|=-\sum_{q=1}^{d-1} c_q \ln\left|e^{\frac{\pi i q}{d}}-e^{-\frac{\pi i q}{d}}\right|,$$

где в последних двух формулах берутся вещественные значения логарифма. Имеем

$$h=\frac{-|\sqrt{d}|}{2\ln\varepsilon}\sum_{n=1}^{d-1} c_n \ln\sin\frac{\pi n}{d}. \tag{149}$$

В обоих полученных для h формулах остается еще вычислить коэфициенты c_n из линейных уравнений (146); этим мы и займемся в следующем параграфе.

§ 52. Суммы Гаусса и окончательные формулы для числа классов

Умножая обе части уравнения (146) на ζ^{-am} и суммируя по $a \bmod d$, получаем

$$\sum_{a=0}^{|d|-1}\chi(a)\zeta^{-am}=\sum_{n=0}^{|d|-1} c_n \sum_{a=0}^{|d|-1}\zeta^{a(n-m)}=c_m|d|,$$

$$c_n=\frac{1}{|d|}\sum_{a=0}^{|d|-1}\chi(a)\zeta^{-an}=\frac{\chi(-1)}{|d|}\sum_{a}\chi(-a)\zeta^{-an}=\frac{1}{d}\sum_{a=0}^{|d|-1}\chi(a)\zeta^{an}.$$

Суммы последнего вида называют *суммами Гаусса*. Гаусс впервые исследовал их и вычислил их значения, причем главную трудность представляло определение их знака. В настоящем параграфе мы установим лишь простейшие свойства сумм Гаусса, откладывая более подробное исследование до следующей главы, где мы будем заниматься аналогом сумм Гаусса для произвольных алгебраических числовых полей.

---

[1]) $\Re u$ означает вещественную часть u.

В этом параграфе мы полагаем, для произвольного дискриминанта d квадратичного поля и целого рационального n,

$$G(n, d) = \sum_{a \bmod d} \chi(a) e^{\frac{2\pi i a n}{|d|}}, \tag{150}$$

где

$$\chi(-a) = \chi(a) \operatorname{sgn} d$$

и для положительных a

$$\chi(a) = \left(\frac{d}{a}\right).$$

Из (150) вытекает, что

$$G(n_1, d) = G(n_2, d), \quad \text{если} \quad n_1 \equiv n_2 \pmod{d}.$$

Покажем, что суммы $G(n, d)$ могут быть выражены через $G(n, q)$, где q — дискриминанты, делящиеся лишь на одно простое число. Для этой цели, пусть, в обозначениях § 47, при $t > 1$

$$d = (\pm q_1)(\pm q_2)\ldots(\pm q_t),$$

где знаки выбраны так, что каждое $\pm q$ само является дискриминантом. Определим далее характеры

$$\left.\begin{aligned} \chi_r(n) &= \left(\frac{\pm q_r}{n}\right) \\ \chi_r(-n) &= \chi_r(n) \operatorname{sgn}(\pm q_r) \end{aligned}\right\} \quad (r = 1, \ldots, t, \quad n > 0), \tag{151}$$

так что с помощью $\chi_r(n)$ можно будет образовать суммы $G(n, \pm q_r)$. Наконец, выберем специальную систему вычетов $a \bmod d$, именно,

$$a = a_1 \frac{|d|}{q_1} + \ldots + a_t \frac{|d|}{q_t},$$

где каждое a_r должно пробегать полную систему вычетов $\bmod q_r$. Имеем

$$\chi(n) = \chi_1(n)\chi_2(n)\ldots\chi_t(n),$$

$$\chi_r(a) = \chi_r(a_r)\chi_r\left(\frac{|d|}{q_r}\right),$$

$$G(n, d) = \sum_{a_1, \ldots, a_t} \chi_1(a_1)\ldots\chi_t(a_t) e^{2\pi i n\left(\frac{a_1}{q_1}+\ldots+\frac{a_t}{q_t}\right)} C,$$

где

$$C = \prod_{r=1}^{t} \chi_r\left(\frac{|d|}{q_r}\right). \tag{152}$$

Таким образом

$$G(n, d) = C \prod_{r=1}^{t} G(n, \pm q_r), \quad C = \pm 1. \tag{153}$$

Из этого равенства заключаем, что

$$G(n, d) = 0, \quad \text{если} \quad (n, d) \neq 1. \tag{154}$$

В самом деле, если n и d имеют общим множителем нечетное простое число q_r, то для этого q_r по теореме 31

$$G(n, \pm q_r) = G(0, \pm q_r) = \sum_{a \bmod q_r} \chi_r(a) = 0,$$

ибо χ_r есть характер $\bmod q_r$. Если же n и d имеют общим множителем 2, то в произведение (153) входит последним множителем $G(n, -4)$ или $G(n, \pm 8)$, и непосредственным подсчетом убеждаемся в том, что при четном n эти функции равны нулю.

Далее, имеем

$$G(cn, d) = \chi(c)\, G(n, d), \quad \text{если} \quad (c, d) = 1. \tag{155}$$

В самом деле,

$$\chi(c)\, G(cn, d) = \sum_{a \bmod d} \chi(ac)\, e^{\frac{2\pi i n ac}{|d|}} = G(n, d),$$

ибо одновременно с a также ac пробегает полную систему вычетов $\bmod d$. В силу $\chi^2(c) = 1$ отсюда и вытекает утверждение.

Теорема 150. *Для каждого целого рационального* n

$$G(n, d) = \chi(n)\, G(1, d),$$

$$c_n = \chi(n)\, \frac{G(1, d)}{d}$$

Действительно, если n и d не взаимно просты, то обе части первого равенства по (154) равны нулю. Если же $(n, d) = 1$, то для доказательства достаточно выбрать в (155) c так, чтобы было $cn \equiv 1 \pmod d$, следовательно, $\chi(c) = \chi(n)$.

Таким образом для завершения вычисления c_n остается еще вычислить сумму $G(1, d)$, не зависящую уже от n.

Теорема 151. $G^2(1, d) = d$.

В силу равенства (153) достаточно доказать это утверждение для дискриминантов d, делящихся только на одно простое число. Для $d = -4$ или ± 8 доказываем теорему непосредственным подсчетом. Если же $|d|$ равно нечетному простому числу, то имеем

$$G^2(1, \pm q) = \sum_{a, b} \chi(a)\chi(b)\zeta^{a+b} = \sum_{a=1}^{q-1} \chi(a) \sum_{b=1}^{q-1} \chi(ab)\zeta^{a+ab} =$$

$$= \sum_{b=1}^{q-1} \chi(b) \sum_{a=1}^{q-1} \zeta^{(b+1)a}.$$

Но

$$1 + \zeta^n + \zeta^{2n} + \ldots + \zeta^{(q-1)n} = \begin{cases} 0, & \text{если } (n, q) = 1, \\ q, & \text{если } n \equiv 0 \pmod q. \end{cases}$$

Следовательно,

$$G^2(1, \pm q) = -\sum_{b \not\equiv -1 \pmod q} \chi(b) + (q-1)\chi(-1) =$$

$$= q\chi(-1) - \sum_{b \bmod d} \chi(b) = \pm q.$$

Таким образом дело сводится к следующей проблеме: какому из обоих значений $\sqrt{d}$ равно определенное трансцендентным путем, а именно, с помощью показательной функции, число $G(1, d)$? Это — знаменитая проблема определения знака сумм Гаусса, решение которой будет изложено в следующей главе.

Теорема 152. *Число классов h квадратичного поля с дискриминантом d имеет значение*

1. $h = -\frac{\rho}{|d|}\sum_{n=1}^{|d|-1} n\left(\frac{d}{n}\right)$, $\rho = \frac{-iG(1, d)}{|\sqrt{d}|} = \pm 1$ при $d < -4$.

2. $h = \frac{\rho}{2\ln\varepsilon}\ln\frac{\prod_a \sin\frac{\pi a}{d}}{\prod_b \sin\frac{\pi b}{d}}$, $\rho = \frac{G(1, d)}{|\sqrt{d}|} = \pm 1$ при $d > 0$.

Во втором выражении a, b пробегают те из чисел 1, 2, ..., $d-1$, *для которых соответственно*

$$\left(\frac{d}{a}\right) = -1, \quad \left(\frac{d}{b}\right) = +1.$$

В качестве окончательного результата мы получим, что всегда $\rho = +1$ (см. § 58). Формула для числа классов мнимого квадратичного поля чрезвычайно проста и по своему строению представляется вполне укладывающейся в рамки элементарной арифметики. И однако до сих пор не удалось доказать эту формулу чисто арифметическим путем, без помощи трансцендентных средств, примененных Дирихле. До сих пор не удалось даже показать каким-либо другим путем, что выражение для h всегда положительно. При современном состоянии науки мы можем воспринимать эту формулу лишь как не вполне еще понятный числовой факт.

Так же обстоит дело и со второй формулой. Из нее, в частности, следует, что отношение $\frac{\prod_a}{\prod_b}$ является единицей поля $k(\sqrt{d})$. Последнее можно также довольно просто доказать с помощью теории поля корней $2d$-й степени из 1, которому, очевидно, принадлежит рассматриваемое число. Однако то обстоятельство, что эта единица > 1 и притом связана с числом классов указанным образом, до сих пор не удалось доказать чисто арифметическим путем.

§ 53. Связь между идеалами поля $k(\sqrt{d})$ и бинарными квадратичными формами

В заключение этой главы остановимся еще на связи современной теории квадратичных полей с классической основанной Гауссом теорией бинарных квадратичных форм.

Под *бинарной квадратичной формой* переменных x, y понимают выражение

$$F(x, y) = Ax^2 + Bxy + Cy^2,$$

где коэфициенты формы A, B, C суть независимые от x и y величины, не равные одновременно нулю.

Такая форма, очевидно, всегда может быть представлена в виде произведения двух однородных линейных функций от x, y:

$$F(x, y) = (\alpha x + \beta y)(\alpha' x + \beta' y). \tag{156}$$

Четыре величины α, β, α', β', естественно, не определяются однозначно коэфициентами A, B, C. Если $A \neq 0$, то, например, имеем

$$F(x, y) = \left(\sqrt{A}x + \frac{B + \sqrt{B^2 - 4AC}}{2\sqrt{A}}\, y\right)\left(\sqrt{A}x + \frac{B - \sqrt{B^2 - 4AC}}{2\sqrt{A}}\, y\right).$$

Сравнение коэфициентов показывает, что

$$D = B^2 - 4AC = (\alpha\beta' - \alpha'\beta)^2 = \begin{vmatrix} \alpha & \beta \\ \alpha' & \beta' \end{vmatrix}^2. \tag{157}$$

Это выражение называется *дискриминантом* (или также детерминантом) формы.

Если мы подвергнем переменные x, y однородному линейному преобразованию

$$x = ax_1' + by_1', \quad y = cx_1' + dy_1', \tag{158}$$

то $F(x, y)$, очевидно, преобразуется в квадратичную форму относительно x', y'. Исходя из представления $F(x, y)$ в виде (156), будем иметь

$$F(ax_1 + by_1,\ cx_1 + dy_1) =$$
$$= ((\alpha a + \beta c)x_1 + (\alpha b + \beta d)y_1)((\alpha' a + \beta' c)x_1 + (\alpha' b + \beta' d)y_1) =$$
$$= A_1 x_1^2 + B_1 x_1 y_1 + C_1 y_1^2 = F_1(x_1, y_1).$$

Связь между A, B, C и A_1, B_1, C_1 в отдельности нас не будет интересовать. Что же касается дискриминантов, то имеем

$$D_1 = B_1^2 - 4A_1C_1 = \begin{vmatrix} \alpha a + \beta c & \alpha b + \beta d \\ \alpha' a + \beta' c & \alpha' b + \beta' d \end{vmatrix}^2 = \begin{vmatrix} \alpha & \beta \\ \alpha' & \beta' \end{vmatrix}^2 \begin{vmatrix} a & b \\ c & d \end{vmatrix}^2,$$

$$D_1 = D(ad - bc)^2. \tag{159}$$

Если определитель преобразования $ad - bc$ отличен от нуля, то при должном преобразовании переменных x_1, y_1 форма $F_1(x_1, y_1)$ пере-

ходит обратно в первоначальную форму $F(x, y)$. Именно, из (158) получаем

$$x_1 = \frac{dx - by}{ad - bc}, \quad y_1 = \frac{-cx + ay}{ad - bc}. \tag{160}$$

Это преобразование называется *обратным* к преобразованию (158). Его определителем является $\frac{1}{ad - bc}$.

Мы будем рассматривать исключительно такие преобразования, в которых коэфициенты a, b, c, d суть целые рациональные числа с определителем $+1, -1$ — так называемые *унимодулярные целочисленные преобразования*. Как показывают приведенные выше формулы, преобразование, обратное такому преобразованию, будет обладать тем же свойством.

Определение. Если при унимодулярном целочисленном преобразовании форма $F(x, y)$ переходит в форму $F_1(x_1, y_1)$, то F называется *эквивалентной* F_1; символически это записывается так:

$$F \sim F_1.$$

В силу сказанного выше тогда также $F_1 \sim F$, так как F_1 переходит в F с помощью обратного преобразования. Таким образом соотношение эквивалентности симметрично относительно F и F_1. Кроме того, всегда $F \sim F$.

Лемма а). *Если для квадратичных форм F, F_1, F_2 имеют место соотношения*

$$F \sim F_1 \quad и \quad F_1 \sim F_2,$$

то также

$$F \sim F_2.$$

В самом деле, пусть существуют два унимодулярных преобразования с целочисленными коэфициентами a, b, c, ∂ и a_1, b_1, c_1, ∂_1 такие, что

$$F(ax + by, \ cx + \partial y) = F_1(x, y)$$

и

$$F_1(a_1x + b_1y, \ c_1x + \partial_1 y) = F_2(x, y).$$

Тогда, полагая в первом равенстве

$$x = a_1x_1 + b_1y_1, \quad y = c_1x_1 + \partial_1 y_1$$

и опуская затем у переменных x_1, y_1, обозначение которых находится в нашем распоряжении, индекс 1, мы получаем, в комбинации со вторым равенством,

$$F((aa_1 + bc_1)x + (ab_1 + b\partial_1)y, \ (ca_1 + \partial c_1)x + (cb_1 + \partial\partial_1)y) = F_2(x, y).$$

Аргументы в F получаются из x, y с помощью целочисленного однородного линейного преобразования, и определитель коэфициентов этого преобразования есть

$$\begin{vmatrix} \alpha a_1 + bc_1 & ab_1 + b\delta_1 \\ ca_1 + \delta c_1 & cb_1 + \delta\delta_1 \end{vmatrix} = (\alpha\delta - bc)(a_1\delta_1 - b_1c_1) = 1.$$

Следовательно, $F \sim F_2$, и соотношение эквивалентности транзитивно.

Под *классом эквивалентных форм* понимают совокупность всех форм, эквивалентных некоторой заданной форме, скажем, F; F называется тогда представителем класса. Все формы одного класса имеют, в силу равенства (159), один и тот же дискриминант.

В дальнейшем мы будем рассматривать лишь вещественные формы, т. е. формы с вещественными коэфициентами. Если F — вещественная форма, то то же справедливо и для всех форм, эквивалентных F.

Теорема 153. *Пусть D — дискриминант формы F. Если $D > 0$, то $F(x, y)$ может принимать как положительные, так и отрицательные значения. Если $D < 0$, то либо для всех вещественных x, y $F(x, y) \geqslant 0$, либо для всех вещественных x, y $F(x, y) \leqslant 0$, причем $F(x, y)$ обращается в нуль лишь при $x = y = 0$.*

Для доказательства рассмотрим разложение

$$AF(x, y) = \left(Ax + \frac{B}{2}y\right)^2 - \frac{D}{4}y^2.$$

Если $D = B^2 - 4AC < 0$, то A должно быть отлично от нуля, и из написанного равенства следует, что

$$AF(x, y) \geqslant 0,$$

причем равенство имеет место лишь, если $y = 0$ и $Ax + \frac{B}{2}y = 0$, т. е. $x = y = 0$. Тем самым $F(x, y)$ всегда имеет знак коэфициента A, если $D < 0$ и $x^2 + y^2 \neq 0$.

Пусть теперь $D > 0$. Если $A \neq 0$, то

$$AF(1, 0) = A^2 > 0,$$
$$AF(B, -2A) = -DA^2 < 0,$$

т. е. F может принимать значения обоих знаков, причем, очевидно, может обращаться в нуль и для вещественных x, y, не обращающихся одновременно в нуль.

Если же $D > 0$ и $A = 0$, то справедливость утверждения теоремы явствует из равенства

$$F(x, y) = y(Bx + Cy).$$

Форма F называется *неопределенной*, если $D > 0$, напротив, *определенной*, если $D < 0$, причем в последнем случае, — *положительно определенной* или *отрицательно определенной*, смотря по тому, будет ли $F(x, y) \geqslant 0$ или $F(x, y) \leqslant 0$.

Начиная отсюда, мы будем рассматривать исключительно целочисленные формы, т. е. формы с целыми рациональными коэфициентами. Их дискриминанты D, очевидно, $\equiv 0$ или $1 \pmod 4$.

Пусть теперь d — дискриминант квадратичного поля $k(\sqrt{d})$. Мы изложим метод *сопоставления каждому классу идеалов поля* $k(\sqrt{d})$ *(в узком смысле) класса эквивалентных форм с дискриминантом* d.

Пусть $\mathfrak{a}$ — произвольный целый идеал заданного класса из $k(\sqrt{d})$. Мы понимаем под α_1, α_2 базис идеала $\mathfrak{a}$, для которого величина

$$\alpha_1\alpha_2' - \alpha_2\alpha_1' = \pm N(\mathfrak{a})\sqrt{d} \text{ положительная или положительно мнимая.} \quad (161)$$

Поставим идеалу $\mathfrak{a}$ в соответствие форму

$$F(x, y) = \frac{(\alpha_1 x + \alpha_2 y)(\alpha_1' x + \alpha_2' y)}{N(\mathfrak{a})}.$$

Эта форма имеет, очевидно, целые рациональные коэфициенты, так как наибольший общий делитель ее коэфициентов по теореме 87 равен произведению $\mathfrak{a}\mathfrak{a}' = N(\mathfrak{a})$. Дискриминант же ее, в силу (157), равен

$$D = \frac{(\alpha_1\alpha_2' - \alpha_2\alpha_1')^2}{N(\mathfrak{a})^2} = d.$$

Если форма $F(x, y)$ порождается описанным образом идеалом $\mathfrak{a}$, то мы будем говорить, что F *принадлежит* $\mathfrak{a}$, и писать $F(x, y) \to \mathfrak{a}$.

При $d < 0$ мы, очевидно, получим лишь положительно определенные формы, так как первый коэфициент

$$A = \frac{\alpha_1\alpha_1'}{N(\mathfrak{a})} = \frac{|N(\alpha_1)|}{N(\mathfrak{a})} > 0.$$

Лемма b). *Для каждой неопределенной* $(d > 0)$ *или положительно определенной* $(d < 0)$ *целочисленной формы* F *с дискриминантом* d *существует идеал* $\mathfrak{a}$ *такой, что* $F \to \mathfrak{a}$.

Прежде всего форма $F(x, y) = Ax^2 + Bxy + Cy^2$, где $B^2 - 4AC = d$, является примитивным полиномом, так как если p входит в A, B, C, то также $\frac{d}{p^2}$ должно быть еще дискриминантом, что для дискриминантов квадратичных полей может иметь место лишь при $p = \pm 1$. Рассмотрим теперь идеал

$$\mathfrak{m} = \left(A, \frac{B - \sqrt{d}}{2}\right),$$

где $\sqrt{d}$ имеет положительное или, соответственно, положительно мнимое значение. По теореме 87 $N(\mathfrak{m}) = \mathfrak{m}\mathfrak{m}'$ есть содержание формы

$$\left(Ax + \frac{B - \sqrt{d}}{2} y\right)\left(Ax + \frac{B + \sqrt{d}}{2} y\right) = AF(x, y),$$

$$N(\mathfrak{m}) = |A|.$$

Следовательно, пара чисел A, $\frac{B-\sqrt{d}}{2}$ из $\mathfrak{m}$ представляет собой базис идеала $\mathfrak{m}$, ибо квадрат их детерминанта имеет значение $N^2(\mathfrak{m})d$. Таким же точно образом

$$\alpha_1 = \lambda A, \quad \alpha_2 = \lambda\frac{B-\sqrt{d}}{2},$$

где λ — число из k ($\lambda \neq 0$), является базисом идеала $\lambda\mathfrak{m}$. Так как

$$\alpha_1\alpha_2' - \alpha_2\alpha_1' = \lambda\lambda' A\sqrt{d},$$

то этот базис имеет еще свойство (161), когда

$$\lambda\lambda' A > 0.$$

Мы выберем поэтому:

1) $\lambda = 1$, если $d < 0$ (ибо, по предположению, здесь $A > 0$);
2) $\lambda = 1$, если $d > 0$ и $A > 0$;
3) $\lambda = \sqrt{d}$, если $d > 0$ и $A < 0$.

Тогда во всех случаях

$$\lambda\lambda' A = N(\lambda\mathfrak{m}),$$

и $F \to \lambda\mathfrak{m}$.

Теорема 154. *Эквивалентные формы принадлежат эквивалентным (в узком смысле) идеалам и обратно.*

Пусть

$$\left.\begin{aligned} F(x, y) &= \frac{(\alpha_1 x + \alpha_2 y)(\alpha_1' x + \alpha_2' y)}{N(\mathfrak{a})}, \\ G(x, y) &= \frac{(\beta_1 x + \beta_2 y)(\beta_1' x + \beta_2' y)}{N(\mathfrak{b})} \end{aligned}\right\} \tag{162}$$

— формы, порожденные соответственно базисом α_1, α_2 идеала $\mathfrak{a}$ и базисом β_1, β_2 идеала $\mathfrak{b}$. Оба базиса обладают, таким образом, свойством (161).

Если $F \sim G$, то существуют целые рациональные a, b, c, d с $ad - bc = 1$ такие, что

$$\left.\begin{aligned} &F(ax + by, cx + dy) = G(x, y), \\ &\frac{((a\alpha_1 + c\alpha_2)x + (b\alpha_1 + d\alpha_2)y)((a\alpha_1' + c\alpha_2')x + (b\alpha_1' + d\alpha_2')y)}{N(\mathfrak{a})} = \\ &\qquad = \frac{(\beta_1 x + \beta_2 y)(\beta_1' x + \beta_2' y)}{N(\mathfrak{b})}. \end{aligned}\right\} \tag{163}$$

Так как отношения $-\frac{\beta_2}{\beta_1}$ и $-\frac{\beta_2'}{\beta_1'}$ однозначно (с точностью до порядка) определены как нули полинома $G(x, 1)$, то

$$\frac{a\alpha_1 + c\alpha_2}{b\alpha_1 + d\alpha_2} = \frac{\beta_1}{\beta_2} \quad \text{или} \quad \frac{\beta_1'}{\beta_2'}.$$

Следовательно, существует такое λ, что

$$\begin{aligned} a\alpha_1 + c\alpha_2 &= \lambda\beta_1 \quad \text{или} \quad = \lambda\beta_1' \\ b\alpha_1 + d\alpha_2 &= \lambda\beta_2 \quad\quad\;\; = \lambda\beta_2'. \end{aligned}$$

В обоих случаях, в силу (163),

$$\lambda\lambda' = \frac{N(\mathfrak{a})}{N(\mathfrak{b})} > 0.$$

Это показывает, что второй из названных случаев не может иметь места, так как тогда мы имели бы

$$(ad - bc)(\alpha_1\alpha_2' - \alpha_2\alpha_1') = -\lambda\lambda'(\beta_1\beta_2' - \beta_2\beta_1'),$$

в противоречие с предположением (161).

Теперь, так как $ad - bc = 1$, то также $\lambda\beta_1$, $\lambda\beta_2$ представляют собой базис идеала $\mathfrak{a}$, так что

$$\mathfrak{a} = \lambda(\beta_1, \beta_2) = \lambda\mathfrak{b},$$

$$\mathfrak{a} \approx \mathfrak{b}.$$

Пусть, обратно, $\mathfrak{a} \approx \mathfrak{b}$ и λ — число с положительной нормой, для которого $\mathfrak{a} = \lambda\mathfrak{b}$. Тогда $\lambda\beta_1$, $\lambda\beta_2$ должны представлять собой базис для $\mathfrak{a}$ и, значит, получаться из α_1, α_2 посредством целочисленного преобразования с определителем ± 1, следовательно, существуют целые рациональные a, b, c, d такие, что

$$a\alpha_1 + c\alpha_2 = \lambda\beta_1, \quad b\alpha_1 + d\alpha_2 = \lambda\beta_2.$$

Из свойства (161) обеих пар α_1, α_2 и β_1, β_2 и $N(\lambda) > 0$ вытекает тогда, что $ad - bc = +1$ и

$$\lambda\lambda' = \frac{N(\mathfrak{a})}{N(\mathfrak{b})},$$

а отсюда следует равенство (163), т. е. $F \sim G$.

В силу теоремы 154, h_0 классам идеалов поля $k(\sqrt{d})$ ставятся во взаимно однозначное соответствие классы форм с дискриминантом d (при $d < 0$ — лишь положительно определенные формы). Поэтому *число неэквивалентных целочисленных форм с дискриминантом d конечно и притом равно h_0 или, при $d < 0$, равно $2h_0$*, если засчитывать как положительно, так и отрицательно определенные классы форм. Например, каждая положительная форма с дискриминантом -4 эквивалентна форме $x^2 + y^2$, так как поле $k(\sqrt{-4})$ имеет число классов 1.

Таким образом можно значительную часть теории идеалов перевести на язык теории форм и обратно. Последнее представляет особый интерес для классической теории приведенных форм, с помощью которой возможно выделить посредством неравенств полную систему

неэквивалентных форм и дать тем самым способ определения всех классов идеалов, значительно более удобный, чем изложенный в § 44 [1]).

Теория единиц (с нормой $+1$) воспроизводится в теории форм в следующем виде: требуется определить все унимодулярные целочисленные преобразования, переводящие любую заданную форму в самое себя. Действительно, для каждой единицы ε с $N(\varepsilon) = +1$ вместе с α_1, α_2 также $\varepsilon\alpha_1$, $\varepsilon\alpha_2$ является базисом идеала $\mathfrak{a}$, так что имеет место соотношение

$$\varepsilon\alpha_1 = a\alpha_1 + c\alpha_2, \quad \varepsilon\alpha_2 = b\alpha_1 + \partial\alpha_2,$$

где a, b, c, ∂ — целые рациональные числа с определителем ± 1; тогда для формы $F(x, y)$ (162), очевидно, имеем

$$F(ax + by, cx + \partial y) = F(x, y).$$

Далее теория форм занимается вопросом о том, какие числа могут быть представлены данной формой $F(x, y)$, если x, y пробегают все пары целых рациональных значений. Это, очевидно, сводится к вопросу о том, какие числа могут быть представлены как нормы целых идеалов из заданного класса.

Громоздкая теория композиции классов форм может быть очень просто выражена на языке теории идеалов: композиция форм непосредственно определяется композицией классов идеалов.

Исследование тех форм, дискриминанты которых имеют вид Q^2d, где Q — целое рациональное число, сводится к исследованию числового кольца в $k(\sqrt{d})$ с ведущим идеалом Q (§ 36). При этом в рассматриваемых идеалах принимаются во внимание лишь те числа, которые принадлежат этому кольцу. Так возникает понятие идеала кольца и класса идеалов кольца, которые тогда ставятся в соответствие с классами форм дискриминанта Q^2d.

---

[1]) Эта теория приведения встречается точно так же в теории эллиптических модулярных функций, которая вообще тесно связана с теорией квадратичных числовых полей. См., например, Klein-Fricke, Vorlesungen über die Theorie der elliptischen Modulfunktionen, Leipzig, 1890/92, Bd. I, S. 243—269, Bd. II, S. 161—203, а также H. Weber, Elliptische Funktionen und algebraischen Zahlen (= Lehrbuch der Algebra, Bd. III), 2-е изд., Braunschweig, 1908.

ГЛАВА VIII

КВАДРАТИЧНЫЙ ЗАКОН ВЗАИМНОСТИ В ПРОИЗВОЛЬНЫХ ЧИСЛОВЫХ ПОЛЯХ

§ 54. Квадратичные характеры и суммы Гаусса в произвольных числовых полях

Суммы Гаусса впервые встретились нам при определении числа классов квадратичных полей. К выражениям подобного рода приходят во многих других проблемах, и Гаусс был первый, кто понял, какую большую роль они играют в арифметике. Он обратил внимание на связь между этими суммами и квадратичным законом взаимности и показал, как из определения значений этих сумм получить доказательство закона взаимности. В настоящее время известен целый ряд методов для вычисления этих сумм. Особый интерес для нас представляет трансцендентный метод Коши, поскольку он поддается обобщению.

В 1919 г. автор распространил понятие сумм Гаусса на произвольные алгебраические числовые поля [1]). Упомянутый метод Коши удалось применить и к вычислению этих сумм, и таким образом получилось трансцендентное доказательство квадратичного закона взаимности для любого алгебраического поля. Это доказательство и будет в дальнейшем изложено.

В основу исследования кладется алгебраическое числовое поле k степени n. Прежде всего мы перенесем на это поле k понятия и теоремы § 16 о квадратичных характерах. При этом мы сможем быть кратки, владея в достаточном объеме лежащими в основе этих рассмотрений общими теоретико-групповыми понятиями.

Целое число или целый идеал в k называются *нечетными*, если они взаимно просты с числом 2.

Определение. Пусть $\mathfrak{p}$ — нечетный простой идеал в k и α — произвольное целое число из k, не делящееся на $\mathfrak{p}$. Мы будем называть α *квадратичным вычетом* $\bmod \mathfrak{p}$ и писать

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = +1,$$

[1]) Обобщения в другом направлении представляют собой так называемые радикальные числа Лагранжа в теории деления круга.

если в k существует целое число ξ, удовлетворяющее сравнению $\alpha \equiv \xi^2 \pmod{\mathfrak{p}}$. В противоположном случае мы будем называть α *квадратичным невычетом* $\bmod \mathfrak{p}$ и писать

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = -1.$$

Наконец, мы положим

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = 0, \text{ если } \alpha \equiv 0 \pmod{\mathfrak{p}}.$$

В силу теоремы 84, мы получаем, как в § 16, что для каждого целого α символ $\left(\frac{\alpha}{\mathfrak{p}}\right)$ означает то из трех чисел 0, 1, -1, для которого удовлетворяется сравнение

$$\alpha^{\frac{N(\mathfrak{p})-1}{2}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right) \pmod{\mathfrak{p}}. \tag{164}$$

В случае, когда будут рассматриваться одновременно символы вычетов в различных числовых полях, мы будем сопровождать эти символы индексами, указывающими соответствующее поле.

Так же как и раньше, имеем

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = \left(\frac{\beta}{\mathfrak{p}}\right), \text{ если } \alpha \equiv \beta \pmod{\mathfrak{p}},$$

$$\left(\frac{\alpha\beta}{\mathfrak{p}}\right) = \left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\beta}{\mathfrak{p}}\right).$$

Пусть теперь $\mathfrak{n}$ — целый нечетный идеал и

$$\mathfrak{n} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r$$

— его разложение на простые идеалы. Мы полагаем тогда, по определению, для произвольного целого α (из k)

$$\left(\frac{\alpha}{\mathfrak{n}}\right) = \left(\frac{\alpha}{\mathfrak{p}_1}\right)\left(\frac{\alpha}{\mathfrak{p}_2}\right) \dots \left(\frac{\alpha}{\mathfrak{p}_r}\right). \tag{165}$$

Таким образом, если α не взаимно просто с $\mathfrak{n}$, то этот символ равен нулю, если же $(\alpha, \mathfrak{n}) = 1$, то он равен ± 1. Как и раньше, имеем

$$\left(\frac{\alpha}{\mathfrak{n}}\right) = \left(\frac{\beta}{\mathfrak{n}}\right), \text{ если } \alpha \equiv \beta \pmod{\mathfrak{n}},$$

$$\left(\frac{\alpha\beta}{\mathfrak{n}}\right) = \left(\frac{\alpha}{\mathfrak{n}}\right)\left(\frac{\beta}{\mathfrak{n}}\right).$$

В случае, когда k есть рациональное числовое поле, определения (164)—(165) совпадают с определениями, данными в § 16.

Теперь каждому отличному от нуля целому или дробному числу ω из k мы отнесем сумму следующим образом. Пусть $\mathfrak{d}$ — диферента поля k и $\mathfrak{d}\omega$ представлено в виде отношения целых взаимно простых идеалов:

$$\omega = \frac{\mathfrak{b}}{\mathfrak{a}\mathfrak{d}}, \quad (\mathfrak{a}, \mathfrak{b}) = 1.$$

По теореме 101 след $S(\nu\omega)$ является целым рациональным числом для каждого целого ν, делящегося на $\mathfrak{a}$. Тем самым для целого ν число $e^{2\pi i S(\nu\omega)}$ зависит лишь от класса вычетов $\bmod \mathfrak{a}$, к которому принадлежит ν. Образуя сумму

$$C(\omega) = \sum_{\mu \bmod \mathfrak{a}} e^{2\pi i S(\mu^2\omega)}, \tag{166}$$

где μ пробегает произвольную полную систему вычетов $\bmod \mathfrak{a}$, мы видим, что ее значение зависит только от числа ω, совершенно не завися от специального выбора системы вычетов. Подобную сумму мы будем называть *суммой Гаусса в k*, принадлежащей знаменателю $\mathfrak{a}$. При этом мы условимся, что приписка вроде „$\mu \bmod \mathfrak{a}$" к знаку суммы $\sum$ будет означать, что значок μ, по которому производится суммирование, должен пробежать полную систему вычетов $\bmod \mathfrak{a}$, с возможными дополнительными условиями.

В рациональном числовом поле эти суммы $C(\omega)$ формально отличаются от определенных в § 52 сумм Гаусса, однако последние, как мы скоро увидим, могут быть сведены к суммам $C(\omega)$.

Если знаменатель $\mathfrak{a} = 1$, то, очевидно, $C(\omega) = 1$.

Лемма а). *Пусть* $\mathfrak{d}\omega$ *имеет знаменатель* $\mathfrak{a} \neq 1$. *Тогда*

$$\sum_{\mu \bmod \mathfrak{a}} e^{2\pi i S(\mu\omega)} = 0.$$

В самом деле, вместе с μ также $\mu + \alpha$ при целом α пробегает полную систему вычетов $\bmod \mathfrak{a}$. Обозначая значения рассматриваемой суммы через A, имеем поэтому

$$A = Ae^{2\pi i S(\alpha\omega)}. \tag{167}$$

Здесь $e^{2\pi i S(\alpha\omega)}$ не может быть равно 1 при каждом целом α, ибо тогда $S(\alpha\omega)$ было бы при всех целых α целым рациональным числом и, значит, в силу теоремы 101, $\mathfrak{d}\omega$ должно было бы быть целым, вопреки предположению. Поэтому из (167) вытекает, что $A = 0$.

Если $\varkappa_1$, $\varkappa_2$, α — целые числа, взаимно простые со знаменателем $\mathfrak{a}$ числа $\mathfrak{d}\omega$, то

$$C(\varkappa_1\omega) = C(\varkappa_2\omega), \text{ если } \varkappa_1 \equiv \varkappa_2\alpha^2 \pmod{\mathfrak{a}}. \tag{168}$$

В самом деле, одновременно с μ также $\mu\alpha$ пробегает полную систему вычетов $\bmod \mathfrak{a}$, значит, $C(\varkappa_2\omega) = C(\varkappa_2\alpha^2\omega)$. Но тогда для целых μ число

$$S(\mu^2\varkappa_1\omega) - S(\mu^2\varkappa_2\alpha^2\omega) = S(\mu^2(\varkappa_1 - \varkappa_2\alpha^2)\omega)$$

является, в силу предположения, целым рациональным, следовательно,

$$C(\varkappa_2\alpha^2\omega) = C(\varkappa_1\omega).$$

Покажем, далее, что суммы Гаусса, принадлежащие знаменателю $\mathfrak{a}$, могут быть сведены к суммам Гаусса, принадлежащим к знаменателям $\mathfrak{a}_1$ и $\mathfrak{a}_2$, если $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$ и целые идеалы $\mathfrak{a}_1$, $\mathfrak{a}_2$ взаимно просты.

Пусть c_1, c_2 — такие целые идеалы, что

$$a_1c_1 = \alpha_1, \quad a_2c_2 = \alpha_2$$

суть целые числа и $(a, c_1c_2) = 1$. Положим в (166)

$$\omega = \frac{\beta}{\alpha_1\alpha_2}, \text{ где } \beta = \frac{\mathfrak{b}c_1c_2}{\mathfrak{d}}.$$

Представим полную систему вычетов $\bmod a$ в форме

$$\mu = \rho_1\alpha_2 + \rho_2\alpha_1,$$

где ρ_1, ρ_2 пробегают соответственно полные системы вычетов $\bmod a_1$, $\bmod a_2$. Так как

$$e^{2\pi iS(\mu^2\omega)} = e^{2\pi iS\left(\frac{\rho_1^2\alpha_2\beta}{\alpha_1}\right) + 2\pi iS\left(\frac{\rho_2^2\alpha_1\beta}{\alpha_2}\right)},$$

то получаем тогда

$$C(\omega) = C\left(\frac{\beta}{\alpha_1\alpha_2}\right) = C\left(\frac{\alpha_2\beta}{\alpha_1}\right)C\left(\frac{\alpha_1\beta}{\alpha_2}\right). \tag{169}$$

В силу этого равенства (169), вычисление $C(\omega)$ приводится к вычислению сумм Гаусса, знаменатели которых суть степени простых идеалов.

При нечетных знаменателях редукция может быть проведена еще дальше — до простых знаменателей.

Именно, пусть знаменатель a равен степени $\mathfrak{p}^a$ нечетного простого идеала $\mathfrak{p}$ и $a \geqslant 2$. Пусть c — не делящийся на $\mathfrak{p}$ целый идеал, такой, что $ac = \alpha$ есть целое число, так что

$$\omega = \frac{\beta}{\alpha^a}, \text{ где } \beta = \frac{\mathfrak{b}c^a}{\mathfrak{d}}.$$

Тогда имеет место рекуррентная формула

$$C\left(\frac{\beta}{\alpha^a}\right) = N(\mathfrak{p})\, C\left(\frac{\beta}{\alpha^{a-2}}\right), \tag{170}$$

где сумма в правой части, очевидно, принадлежит знаменателю $\mathfrak{p}^{a-2}$.

Для доказательства представим полную систему вычетов $\bmod \mathfrak{p}^a$ в форме

$$\mu + \rho\alpha^{a-1},$$

где μ, ρ пробегают соответственно полные системы вычетов $\bmod \mathfrak{p}^{a-1}$, $\bmod \mathfrak{p}$. Тогда [1])

$$C\left(\frac{\beta}{\alpha^a}\right) = \sum_{\mu \bmod \mathfrak{p}^{a-1}} \sum_{\rho \bmod \mathfrak{p}} \exp\left\{2\pi iS\left(\frac{(\mu + \rho\alpha^{a-1})^2\beta}{\alpha^a}\right)\right\} =$$

$$= \sum_{\mu \bmod \mathfrak{p}^{a-1}} \exp\left\{2\pi iS\left(\frac{\mu^2\beta}{\alpha^a}\right)\right\} \sum_{\rho \bmod \mathfrak{p}} \exp\left\{2\pi iS\left(\frac{2\mu\rho}{\alpha}\beta\right)\right\}.$$

В силу леммы а) сумма по ρ равна нулю, если 2μ не делится на $\mathfrak{p}$, т. е., так как $\mathfrak{p}$ нечетно, если μ не делится на $\mathfrak{p}$. В противном же

[1]) $\exp x = e^x$.

случае она равна $N(\mathfrak{p})$, так как каждый ее член равен 1. Тем самым

$$C\left(\frac{\beta}{\alpha^a}\right) = N(\mathfrak{p}) \sum_{\substack{\mu \bmod \mathfrak{p}^{a-1} \\ \mu \equiv 0 \,(\mathrm{mod}\, \mathfrak{p})}} \exp\left\{2\pi i S\left(\frac{\mu^2 \beta}{\alpha^a}\right)\right\}.$$

Так как здесь μ пробегает все значения $\nu\alpha$, где ν пробегает полную систему вычетов $\bmod \mathfrak{p}^{a-2}$, то мы и получаем утверждаемое равенство (170).

Повторно применяя эту формулу, мы приходим при четном a к сумме $C(\beta)$, принадлежащей знаменателю 1 и, следовательно, имеющей значение 1. Этим доказана

Лемма b). *Если знаменатель идеала* $\frac{\mathfrak{b}\beta}{\alpha^a}$ *равен* $\mathfrak{p}^a$, *где* $\mathfrak{p}$ — *нечетный простой идеал, входящий в* α *точно в первой степени, то*

$$C\left(\frac{\beta}{\alpha^a}\right) = N(\mathfrak{p})^{\frac{a}{2}}, \qquad \text{если } a \text{ четно},$$

$$C\left(\frac{\beta}{\alpha^a}\right) = N(\mathfrak{p})^{\frac{a-1}{2}} C\left(\frac{\beta}{\alpha}\right), \quad \text{если } a \text{ нечетно}.$$

Аналогичная редукция возможна также для простых идеалов $\mathfrak{p}$, входящих в 2, однако мы не будем излагать ее, так как в дальнейшем она нам не понадобится.

Теорема 155. *Пусть знаменатель* $\mathfrak{a}$ *идеала* $\mathfrak{b}\omega$ *есть нечетный идеал. Тогда для каждого целого числа* $\varkappa$, *взаимно простого с* $\mathfrak{a}$, *имеет место равенство*

$$C(\varkappa\omega) = \left(\frac{\varkappa}{\mathfrak{a}}\right) C(\omega).$$

Эта теорема верна прежде всего в случае, когда $\mathfrak{a}$ — простой идеал $\mathfrak{p}$. В самом деле, в силу леммы a)

$$\sum_{\mu \bmod \mathfrak{p}} \left(\frac{\mu}{\mathfrak{p}}\right) e^{2\pi i S(\mu\omega)} = \sum_{\mu \bmod \mathfrak{p}} \left(\left(\frac{\mu}{\mathfrak{p}}\right) + 1\right) e^{2\pi i S(\mu\omega)}.$$

Во второй сумме, кроме члена, соответствующего классу вычетов $\mu = 0$, отличны от нуля лишь те члены, где μ является квадратичным вычетом $\bmod \mathfrak{p}$. Поэтому она равна

$$1 + 2\sum_{\mu^2} e^{2\pi i S(\mu^2\omega)},$$

где μ^2 пробегает лишь различные квадратичные вычеты, исключая 0. Но это есть как раз сумма $C(\omega)$, так как в последнюю каждый квадрат, кроме 0, входит точно два раза. Таким образом

$$C(\omega) = \sum_{\mu \bmod \mathfrak{p}} \left(\frac{\mu}{\mathfrak{p}}\right) e^{2\pi i S(\mu\omega)}. \tag{171}$$

Заменяя здесь μ через $\mu\varkappa$, от чего значение суммы не изменится, мы и получаем утверждаемое равенство для $\mathfrak{a}=\mathfrak{p}$.

В силу леммы b) утверждение теоремы справедливо и тогда, когда знаменатель $\mathfrak{a}$ есть степень $\mathfrak{p}^a$ простого идеала. В самом деле, при четном a $\left(\frac{\varkappa}{\mathfrak{p}^a}\right)=\left(\frac{\varkappa}{\mathfrak{p}}\right)^a=1$, а суммы Гаусса для ω и $\varkappa\omega$ действительно имеют одинаковые значения. При нечетном же a по только что доказанному добавляется еще множитель $\left(\frac{\varkappa}{\mathfrak{p}}\right)=\left(\frac{\varkappa}{\mathfrak{p}^a}\right)$.

Наконец, формула (169) показывает справедливость нашей теоремы для любых нечетных знаменателей.

Из (171) мы заключаем, что определенные в § 52 для рационального числового поля суммы $G(1, d)$ действительно тесно связаны с суммами Гаусса $C(\omega)$ и одновременно с вычислением $C(\omega)$ будет также получено значение суммы $G(1, d)$.

Наконец, из (169) и леммы b) вытекает еще

Теорема 156. *Если сумма Гаусса $C(\omega)$ принадлежит к знаменателю $\mathfrak{a}$, являющемуся квадратом нечетного идеала, то*

$$C(\omega)=|\sqrt{N(\mathfrak{a})}|.$$

§ 55. Тэта-функции и их ряды Фурье

Аналитическим средством для вычисления сумм Гаусса нам послужат тэта-функции n переменных. Оба эти понятия связаны друг с другом следующим образом.

Рассмотрим в качестве простейшего случая поле $k=k(1)$. Тогда исследованию будет подлежать функция от τ, определяемая рядом

$$\vartheta(\tau)=\sum_{m=-\infty}^{+\infty} e^{-\pi\tau m^2}.$$

Этот ряд (так называемый простой тэта-ряд) сходится для всех τ с положительной вещественной частью. Мнимая ось оказывается натуральной границей аналитической функции $\vartheta(\tau)$. Исследование поведения $\vartheta(\tau)$ при приближении к особой точке $\tau=2ir$, где r — рациональное число, показывает, что $\vartheta(\tau)$ бесконечно возрастает, причем существует

$$\lim_{\tau\to 0}\sqrt{\tau}\,\vartheta(\tau+2ir).$$

Этот предел совпадает, с точностью до несущественных числовых множителей, с определенной в предыдущем параграфе суммой Гаусса $C(-r)$. Но поведение $\vartheta(\tau)$ может быть определено еще другим образом. Именно, имеет место следующая „формула преобразования“ для $\vartheta(\tau)$:

$$\vartheta\left(\frac{1}{\tau}\right)=\sqrt{\tau}\,\vartheta(\tau).$$

Тем самым поведение $\vartheta(\tau)$ в точке $\tau = 2ir$ оказывается связанным с поведением $\vartheta(\tau)$ в точке

$$\tau' = \frac{1}{2ir} = -\frac{2i}{4r}.$$

Последнее же, как было сказано выше, связано с поведением суммы Гаусса $C\left(\frac{1}{4r}\right)$, и сравнение обоих результатов приводит к соотношению между $C(r)$ и $C\left(-\frac{1}{4r}\right)$, из которого может быть определено $C(r)$ и из которого же, с помощью формул предыдущего параграфа, вытекает закон взаимности.

Если поле k имеет степень n, причем k вместе со всеми сопряженными полями вещественно, то вместо простого тэта-ряда мы имеем n-кратный ряд

$$\sum_{\mu} e^{-\pi(t_1\mu^{(1)2} + t_2\mu^{(2)2} + \ldots + t_n\mu^{(n)2})},$$

где $t_1, \ldots, t_n$ — переменные с положительной вещественной частью, и суммирование распространяется на все целые числа μ поля k. В этом ряде полагаем $t_p = w + 2i\omega^{(p)}$, где ω — число из k, и исследуем поведение суммы ряда при стремлении положительной величины w к нулю.

Наконец, если k — общее алгебраическое числовое поле, среди сопряженных к которому $k^{(1)}, \ldots, k^{(r_1)}$ вещественны, остальные невещественны, то снова надлежит исследовать n-кратный ряд. Однако в этом случае мы уже не можем обойтись одной и той же функцией от $t_1, \ldots, t_n$ для вычисления всех сумм $C(\omega)$. Приходится рассматривать зависящие от ω функции

$$\sum_{\mu} \exp\left\{-\pi \sum_{p=1}^{n} t_p |\mu^{(p)}|^2 + 2\pi i \sum_{p=1}^{n} \omega^{(p)}\mu^{(p)2}\right\}$$

вблизи точки $t_1 = t_2 = \ldots = t_n = 0$. При этом μ снова пробегает все целые числа поля k.

Уже из этого наброска доказательства видно, что́ у него общего с трансцендентными методами гл. VI: *знание поведения аналитической функции вблизи ее особых точек является источником арифметических предложений.*

Вхождение абсолютных значений $\mu^{(p)}$ усложняет вывод нужных формул в общем случае. Поэтому, чтобы сделать основную идею доказательства более понятной, мы рассмотрим сначала в ближайшем параграфе формально более легкий случай, когда все сопряженные с k поля вещественны.

Но прежде всего мы изложим ход идей, приводящий во всех случаях к определению и установлению тэта-рядов и формул их преобразования.

Под *квадратичной формой* n *переменных* $x_1, \ldots, x_n$ понимают выражение

$$Q(x_1, \ldots, x_n) = \sum_{i,k=1}^{n} a_{ik}x_i x_k = a_{11}x_1^2 + 2a_{12}x_1x_2 + \ldots,$$

где коэфициенты a_{ik} суть не зависящие от $x_1, \ldots, x_n$ вещественные или комплексные величины, причем $a_{ik} = a_{ki}$.

Квадратичная форма с вещественными коэфициентами называется *положительно определенной*, если для всех вещественных $x_1, \ldots, x_n$

$$Q(x_1, \ldots, x_n) \geqslant 0,$$

причем знак равенства имеет место только для $x_1 = x_2 = \ldots = x_n = 0$. Примером положительно определенной формы от $x_1, \ldots, x_n$ является форма $x_1^2 + x_2^2 + \ldots + x_n^2$.

Лемма а). *Для каждой положительно определенной формы $Q(x_1, \ldots, x_n)$ существует положительная величина c такая, что для всех вещественных $x_1, \ldots, x_n$*

$$Q(x_1, \ldots, x_n) \geqslant c(x_1^2 + \ldots + x_n^2). \tag{172}$$

В самом деле, для всех точек n-мерной сферы $y_1^2 + \ldots + y_n^2 = 1$, в силу предположения, $Q(y_1, \ldots, y_n) > 0$, следовательно, непрерывная функция Q имеет на этой сфере положительный минимум, т. е.

$$Q(y_1, \ldots, y_n) \geqslant C, \text{ если } y_1^2 + \ldots + y_n^2 = 1.$$

Полагая поэтому для произвольных вещественных x_i, не равных одновременно нулю,

$$y_i = \frac{x_i}{\sqrt{x_1^2 + \ldots + x_n^2}} \qquad (i = 1, \ldots, n),$$

получаем неравенство (172).

Теорема 157. *Пусть $Q(x_1, \ldots, x_n) = \sum_{i,k=1}^{n} a_{ik} x_i x_k$ — квадратичная форма с вещественными или комплексными коэфициентами такая, что ее вещественная часть положительно определенная. Тогда*

$$\sum_{m_1, \ldots, m_n = -\infty}^{+\infty} e^{-\pi Q(m_1 + u_1, \ldots, m_n + u_n)}, \tag{173}$$

где $u_1, \ldots, u_n$ — вещественные переменные, представляет собой абсолютно сходящийся ряд; пусть его сумма будет $T(u_1, \ldots, u_n)$. Эта функция непрерывна и неограниченно дифференцируема по u, причем по каждому переменному u имеет период 1.

Ряд (173) называется *n-кратным тэта-рядом*.

Переходя к доказательству, обозначим через Q_0 вещественную часть формы Q. В силу леммы а), существует такое положительное c, что

$$Q_0(m_1 + u_1, \ldots, m_n + u_n) \geqslant c((m_1 + u_1)^2 + \ldots + (m_n + u_n)^2).$$

Далее,

$$|e^{-\pi Q}| = e^{-\pi Q_0} \leqslant e^{-\pi c \sum_{i=1}^{n} (m_i + u_i)^2}.$$

Ограничиваясь рассмотрением некоторой области $|u_i| \leqslant \frac{C}{2}$ изменения вещественных переменных u, получаем

$$|e^{-\pi Q}| \leqslant e^{-\pi c \sum_{i=1}^{n} (m_i^2 - C|m_i|) + K},$$

где K — некоторая постоянная. Отсюда, в силу неравенства

$$|m_1| + \ldots + |m_n| \leqslant \sqrt{n(m_1^2 + \ldots + m_n^2)} \leqslant \varepsilon \sqrt{n}(m_1^2 + \ldots + m_n^2),$$

имеющего место при

$$m_1^2 + \ldots + m_n^2 > \frac{1}{\varepsilon^2} \qquad (\varepsilon > 0), \tag{174}$$

получаем оценку

$$|e^{-\pi Q}| \leqslant \exp\{-\pi c(1 - \varepsilon C\sqrt{n})(m_1^2 + \ldots + m_n^2) + K\}.$$

Беря теперь ε достаточно малым, мы будем иметь

$$a = c(1 - \varepsilon C\sqrt{n}) > 0,$$

и члены рассматриваемого ряда (за исключением конечного числа, для которых не выполняется (174)) будут по абсолютной величине не превосходить соответствующих членов очевидно сходящегося ряда с постоянными членами

$$\sum_{m_1, \ldots, m_n} e^{-\pi a(m_1^2 + \ldots + m_n^2) + K}$$

Поэтому ряд абсолютных значений членов ряда (173) равномерно сходится и сумма ряда (173) является поэтому непрерывной функцией от $u_1, \ldots, u_n$. Эта функция $T(u_1, \ldots, u_n)$ имеет по каждому переменному период 1, ибо, например, $T(u_1 + 1, u_2, \ldots, u_n)$ переходит в $T(u_1, u_2, \ldots, u_n)$, если заменить индекс суммирования m_1 через $m_1 - 1$.

Равномерная сходимость рядов, получающихся из T почленным одно- или многократным дифференцированием по переменным u, устанавливается таким же образом. Так как

$$Q(m_1 + u_1, \ldots, m_n + u_n) = Q(m_1, \ldots, m_n) + \\ + 2\sum_{i,k=1}^{n} a_{ik} m_i u_k + Q(u_1, \ldots, u_n),$$

то достаточно исследовать почленную диференцируемость ряда

$$\sum_{m_1, \ldots, m_n} \exp\left\{-\pi Q(m_1, \ldots, m_n) - 2\pi \sum_{i,k=1}^{n} a_{ik} m_i u_k\right\}.$$

При диференцировании в качестве множителей при отдельных членах появляются произведения степеней чисел $m_1, \ldots, m_n$ и их линейных комбинаций. Но так как $|m| < e^{|m|}$, то

$$|m_1^{c_1} \ldots m_n^{c_n}| < e^{c_1|m_1| + \ldots + c_n|m_n|} \qquad (c_i \geqslant 0),$$

и рассуждением, аналогичным проведенному выше, мы убеждаемся в равномерной сходимости ряда, получившегося в результате дифференцирования. Тем самым теорема полностью доказана.

Формулы преобразования для тэта-рядов, упоминавшиеся в начале этого параграфа, мы получим теперь, развертывая периодическую функцию T в ряд Фурье и основываясь на следующем предложении из анализа:

Пусть $\varphi(u_1, \ldots, u_n)$ — *(вещественная или комплексная) функция вещественных переменных* u, *имеющая относительно каждого аргумента период* 1. *Пусть, далее,* φ *имеет непрерывные частные производные до* $2n$*-го порядка включительно. Тогда* φ *может быть разложена в абсолютно сходящийся ряд Фурье*:

$$\varphi(u_1, \ldots, u_n) = \sum_{m_1, \ldots, m_n} a(m_1, \ldots, m_n)\, e^{-2\pi i (m_1 u_1 + \ldots + m_n u_n)}$$

с коэффициентами

$$a(m_1, \ldots, m_n) = \int_0^1 \ldots \int_0^1 e^{2\pi i (m_1 u_1 + \ldots + m_n u_n)}\, \varphi(u_1, \ldots, u_n)\, du_1 \ldots du_n.$$

При $n = 1$ эта теорема обычно доказывается в учебниках анализа. В общем случае она легко доказывается по индукции от n к $n+1$.

Пусть теперь φ здесь — сумма тэта-ряда, как мы видели, удовлетворяющая условиям приведенной сейчас теоремы. Тогда для коэффициентов ряда Фурье получаются выражения

$$a(m_1, \ldots, m_n) = \int_0^1 \ldots \int_0^1 e^{2\pi i (m_1 u_1 + \ldots + m_n u_n)} \sum_{k_1, \ldots, k_n = -\infty}^{+\infty} e^{-\pi Q(k_1 + u_1, \ldots, k_n + u_n)}\, dU,$$

где для краткости положено $dU = du_1 du_2 \ldots du_n$. Переменим здесь порядок суммирования и интегрирования, что в силу равномерной сходимости законно, и введем в каждом члене в качестве новых переменных интеграции $u_1 - k_1, \ldots, u_n - k_n$. Тогда $k_1, \ldots, k_n$ исчезнут в подинтегральных выражениях, появившись зато в пределах интеграции, и мы получим

$$a(m_1, \ldots, m_n) = \sum_{k_1, \ldots, k_n} \int_{-k_1}^{-k_1+1} \ldots \int_{-k_n}^{-k_n+1} e^{2\pi i (m_1 u_1 + \ldots + m_n u_n) - \pi Q(u_1, \ldots, u_n)}\, dU.$$

Сумма всех этих интегралов может быть объединена в одном интеграле, распространенном на все пространство; тем самым доказана

Теорема 158. *n-кратный тэта-ряд*

$$T(u_1, \ldots, u_n) = \sum_{m_1, \ldots\, m_n = -\infty}^{+\infty} e^{-\pi Q(m_1 + u_1, \ldots, m_n + u_n)}$$

допускает представление

$$T(u_1, \ldots, u_n) = \sum_{m_1, \ldots, m_n = -\infty}^{+\infty} a((m))\, e^{-2\pi i (m_1 u_1 + \ldots + m_n u_n)},$$

где

$$a((m)) = a(m_1, \ldots, m_n) = \int_{-\infty}^{+\infty} \ldots \int e^{-\pi Q(u_1, \ldots, u_n) + 2\pi i (m_1 u_1 + \ldots + m_n u_n)}\, du_1 du_2 \ldots du_n.$$

§ 56. Взаимность между суммами Гаусса во вполне вещественных полях

В этом параграфе мы будем предполагать, что алгебраическое числовое поле k, в котором исследуются суммы Гаусса из § 54, *вполне вещественно*, т. е. что вещественны все сопряженные поля $k^{(p)}$. Пусть $\mathfrak{a}\,(\neq 0)$ — идеал в k, с базисом $\alpha_1, \ldots, \alpha_n$. Тогда, понимая под $t_1, \ldots, t_n$ сначала n положительных вещественных переменных, мы выберем в качестве формы Q теоремы 158 форму

$$Q(x_1, \ldots, x_n) = \sum_{p=1}^{n} t_p (\alpha_1^{(p)} x_1 + \ldots + \alpha_n^{(p)} x_n)^2,$$

очевидно, положительную. Соответствующий тэта-ряд будет

$$\vartheta(t, z; \mathfrak{a}) = \sum_{\mu \text{ из } \mathfrak{a}} \exp\left\{-\pi \sum_{p=1}^{n} t_p (\mu^{(p)} + z_p)^2\right\}, \tag{175}$$

где

$$z_p = \sum_{q=1}^{n} \alpha_q^{(p)} u_q \qquad (p = 1, \ldots, n). \tag{176}$$

В ряде (175) μ пробегает все числа идеала $\mathfrak{a}$ точно по одному разу. Коэфициенты Фурье из теоремы 158 имеют здесь значения

$$a(m_1, \ldots, m_n) = \int_{-\infty}^{+\infty} \ldots \int \exp\left\{-\pi \sum_{p=1}^{n} t_p z_p^2 + 2\pi i \sum_{p=1}^{n} m_p u_p\right\} dU,$$

где z_p связаны с переменными интеграции u_p теми же соотношениями (176).

Сделаем теперь в этом интеграле замену переменных, введя в качестве переменных интеграции z_p. Обращение равенств (176) дает

$$u_k = \sum_{p=1}^{n} \beta_k^{(p)} z_p \qquad (k = 1, \ldots, n),$$

где числа $\beta_1, \ldots, \beta_n$ образуют, в силу теоремы 102, базис идеала $\frac{1}{\mathfrak{a}\mathfrak{d}}$ в k. Имеем тогда

$$\sum_{k=1}^{n} m_k u_k = \sum_{p=1}^{n} \lambda^{(p)} z_p, \tag{177}$$

где

$$\lambda = \sum_{k=1}^{n} \beta_k m_k — \text{число из } \frac{1}{\mathfrak{a}\mathfrak{d}}.$$

Далее,

$$a((m)) = \frac{1}{|N(\mathfrak{a}) \cdot \sqrt{d}|} \int_{-\infty}^{+\infty} \ldots \int \exp\left\{-\pi \sum_{p=1}^{n} t_p z_p^2 + 2\pi i \sum_{p=1}^{n} \lambda^{(p)} z_p\right\} dz_1 \ldots dz_n.$$

Но для положительных t и вещественных λ

$$\int_{-\infty}^{+\infty} e^{-\pi t z^2 + 2\pi i \lambda z} dz = e^{-\frac{\pi\lambda^2}{t}} \int_{-\infty}^{+\infty} e^{-\pi t\left(z - \frac{i\lambda}{t}\right)^2} dz = \frac{e^{-\frac{\pi\lambda^2}{t}}}{\sqrt{t}}, \tag{178}$$

где взято положительное значение $\sqrt{t}$. Следовательно, коэфициент a есть произведение n таких выражений, и тем самым из теоремы предыдущего параграфа получается, наконец,

Теорема 159. *Тэта-ряд, определенный формулой* (175), *допускает также представление*

$$\vartheta(t, z; \mathfrak{a}) =$$

$$= \frac{1}{N(\mathfrak{a})\,|\sqrt{d}\,|\sqrt{t_1 \ldots t_n}} \sum_{\lambda \text{ из } \frac{1}{\mathfrak{a}\mathfrak{d}}} \exp\left\{-\pi \sum_{p=1}^{n} \frac{\lambda^{(p)2}}{t_p} - 2\pi i \sum_{p=1}^{n} \lambda^{(p)} z_p\right\}. \tag{179}$$

При этом в правой части λ *пробегает все числа идеала* $\frac{1}{\mathfrak{a}\mathfrak{d}}$ *в* k.

Нетрудно видеть теперь, что равенство (179) имеет место также для невещественных t, если только вещественные части всех t_p положительны. В самом деле, тогда также вещественные части всех $\frac{1}{t_p}$ положительны, и ряды в обеих частях формулы, в силу равномерной сходимости относительно t, представляют собой аналитические функции от $t_1, \ldots, t_n$, регулярные при $\Re(t_p) > 0$ $(p = 1, \ldots, n)$. Таким образом формула (179) справедлива также для любых t из правой полуплоскости, если под $\sqrt{t_p}$ понимать те однозначные здесь аналитические функции, которые для положительных t положительны, амплитуды которых, следовательно, заключены между $-\frac{\pi}{4}$ и $+\frac{\pi}{4}$, и если считать

$$\sqrt{t_1 \ldots t_n} = \sqrt{t_1} \ldots \sqrt{t_n}.$$

Беря $z_1 = \ldots = z_n = 0$ и заменяя $\mathfrak{a}$ через $\mathfrak{f}$, мы получаем из теоремы 159 следующий результат:

Теорема 160. *Для функции от* $t_1, \ldots, t_n$

$$\vartheta(t; \mathfrak{f}) = \vartheta(t, 0; \mathfrak{f}) = \sum_{\mu \text{ из } \mathfrak{f}} \exp\left\{-\pi \sum_{p=1}^{n} t_p \mu^{(p)^2}\right\}.$$

имеет место формула преобразования

$$\vartheta(t; \mathfrak{f}) = \frac{1}{N(\mathfrak{f}) \sqrt{|d|} \sqrt{t_1 \ldots t_n}} \vartheta\left(\frac{1}{t}; \frac{1}{\mathfrak{f}\mathfrak{d}}\right). \tag{180}$$

Далее, из теоремы 159 вытекает

Лемма а). *Для всех* z

$$\lim_{t \to 0} \sqrt{t_1 \ldots t_n}\, \vartheta(t, z; \mathfrak{a}) = \frac{1}{N(\mathfrak{a}) \sqrt{|d|}},$$

в предположении, что комплексные переменные $t_1, \ldots, t_n$ *с положительными вещественными частями одновременно стремятся к нулю таким образом, что вещественные части величин* $\frac{1}{t_p}$ *безгранично возрастают.*

Действительно, обозначим наименьшее из n чисел $\Re\left(\frac{1}{t_p}\right)$ через r; тогда

$$\left|\exp\left\{-\pi \sum_{p=1}^{n} \frac{1}{t_p} \lambda^{(p)2}\right\}\right| \leqslant \exp\left\{-\pi r \sum_{p=1}^{n} \lambda^{(p)2}\right\} \leqslant e^{-\pi r c (m_1^2 + \ldots + m_n^2)},$$

где c — выбранная соответственно неравенству (172) положительная постоянная, не зависящая от переменных t_p. Поэтому сумма в правой части формулы (179), за исключением члена с $m_1 = m_2 = \ldots = m_n = 0$, по абсолютной величине

$$\leqslant \Big(\sum_{m=-\infty}^{+\infty} e^{-\pi r c m^2}\Big)^2 - 1 < \Big(1 + 2 \sum_{m=1}^{\infty} e^{-\pi r c m}\Big)^n - 1 = \left(1 + \frac{2e^{-\pi r c}}{1 - e^{-\pi r c}}\right)^n - 1,$$

откуда, беря $r \to \infty$, получаем утверждение леммы а).

Формула (180) и даст нам теперь искомое соотношение между двумя суммами Гаусса в k, если мы положим в ней $\mathfrak{f} = 1$. Пусть ω — отличное от нуля число поля k и $\mathfrak{d}\omega$ имеет знаменатель $\mathfrak{a}$ и числитель $\mathfrak{b}$:

$$\omega = \frac{\mathfrak{b}}{\mathfrak{a}\mathfrak{d}}, \quad (\mathfrak{a}, \mathfrak{b}) = 1.$$

Положим в (180)

$$t_p = x - 2i\omega^{(p)}, \quad \mathfrak{f} = 1,$$

где x — положительная величина, и определим по лемме а), как ведут себя обе стороны (180) при приближении x к нулю.

Прежде всего

$$\vartheta(x - 2i\omega; 1) = \sum_{\mu} \exp\left\{-\pi \sum_{p=1}^{n} (x - 2i\omega^{(p)}) \mu^{(p)2}\right\} =$$

$$= \sum_{\rho \bmod \mathfrak{a}} e^{2\pi i S(\omega\rho^2)} \sum_{\nu \text{ из } \mathfrak{a}} \exp\left\{-\pi \sum_{p=1}^{n} x(\nu^{(p)} + \rho^{(p)2})\right\},$$

ибо $\mu = \nu + \rho$ пробегает все целые числа поля, когда ρ пробегает полную систему вычетов mod $\mathfrak{a}$ и ν — все числа из $\mathfrak{a}$. Здесь внутренняя сумма (по ν) тоже представляет собой тэта-ряд, следовательно,

$$\vartheta(x - 2i\omega;\ 1) = \sum_{\rho \bmod \mathfrak{a}} e^{2\pi i S(\rho^2 \omega)}\, \vartheta(x, \rho;\ \mathfrak{a}).$$

И, наконец, по лемме а) получаем тогда

$$\lim_{x \to 0} x^{\frac{n}{2}}\, \vartheta(x - 2i\omega;\ 1) = \frac{C(\omega)}{N(\mathfrak{a})\,|\sqrt{d}\,|}, \tag{181}$$

где $C(\omega)$ означает сумму Гаусса, как она была определена в § 54.

Таким же образом мы определим поведение правой части равенства (180) при $x \to 0$. Имеем

$$\frac{1}{t_p} = \frac{i}{2\omega(p)} + \tau_p, \quad \text{где} \quad \tau_p = \frac{-ix}{2\omega(p)\,(x - 2i\omega(p))};$$

поэтому вещественная часть $\frac{1}{t_p}$ равна

$$\Re\left(\frac{1}{\tau_p}\right) = \frac{4\omega(p)^2}{x}$$

и, следовательно, безгранично возрастает при $x \to 0$. Пусть, далее, $\mathfrak{c}$ — целый идеал, такой, что $\mathfrak{c}\mathfrak{d}$ есть главный идеал, $\mathfrak{c}\mathfrak{d} = \delta$, и $(\mathfrak{c}, 2\mathfrak{b}) = 1$. Числа из $\frac{1}{\mathfrak{d}}$ мы получим тогда в форме $\frac{\mu}{\delta}$, где μ пробегает все числа из $\mathfrak{c}$. Следовательно,

$$\vartheta\left(\frac{1}{t};\ \frac{1}{\mathfrak{d}}\right) = \sum_{\mu \text{ из } \mathfrak{c}} \exp\left\{-\pi \sum_{p=1}^{n} \left(\tau_p + \frac{i}{2\omega(p)}\right) \frac{\mu(p)^2}{\delta(p)^2}\right\}.$$

Пусть теперь

$$\mathfrak{b}_1 — \text{знаменатель идеала } \frac{\mathfrak{d}\mathfrak{c}^2}{4\omega\delta^2} = \frac{\mathfrak{a}}{4\mathfrak{b}}. \tag{182}$$

Тогда μ в сумме для $\vartheta\left(\frac{1}{t};\ \frac{1}{\mathfrak{d}}\right)$ мы представляем в форме $\mu = \nu + \rho$, где ρ пробегает полную систему вычетов mod $\mathfrak{b}_1$, делящихся на $\mathfrak{c}$, а ν — все числа из $\mathfrak{b}_1\mathfrak{c}$, и получаем

$$\vartheta\left(\frac{1}{t};\ \frac{1}{\mathfrak{d}}\right) = \sum_{\substack{\rho \bmod \mathfrak{b}_1 \\ \rho \equiv 0\,(\mathfrak{c})}} e^{-2\pi i S\left(\frac{\rho^2}{4\omega\delta^2}\right)} \sum_{\nu \text{ из } \mathfrak{b}_1\mathfrak{c}} \exp\left\{-\pi \sum_{p=1}^{n} \frac{\tau_p}{\delta(p)^2} (\nu(p) + \rho(p))^2\right\} =$$

$$= \sum_{\substack{\rho \bmod \mathfrak{b}_1 \\ \rho \equiv 0\,(\mathfrak{c})}} e^{-2\pi i S\left(\frac{\rho^2}{4\omega\delta^2}\right)} \vartheta\left(\frac{\tau}{\delta^2}, \rho;\ \mathfrak{b}_1\mathfrak{c}\right).$$

Следовательно, по лемме а), при стремлении x и, значит, всех τ_p к нулю, получаем

$$\lim_{x \to 0} \sqrt{\frac{\tau_1 \dots \tau_n}{N(\delta)^2}}\, \vartheta\left(\frac{1}{t};\ \frac{1}{\mathfrak{d}}\right) = \frac{A}{N(\mathfrak{b}_1\mathfrak{c})\,|\sqrt{d}\,|},$$

где для краткости положено

$$A = \sum_{\substack{\rho \bmod \mathfrak{b}_1 \\ \rho \equiv 0\,(\mathfrak{c})}} e^{-2\pi i S\left(\frac{\rho^2}{4\omega\delta^2}\right)}. \tag{183}$$

В силу принятого соглашения о значении корней,

$$\lim_{x\to 0} \frac{1}{x^{\frac{n}{2}}} \sqrt{\frac{\tau_1 \dots \tau_n}{N(\delta)^2}} = \frac{1}{|N(2\omega\delta)|},$$

так что мы можем также написать

$$\lim_{x\to 0} x^{\frac{n}{2}}\, \vartheta\left(\frac{1}{t}; \frac{1}{\mathfrak{d}}\right) = \frac{|N(2\omega\delta)|}{|N(\mathfrak{b}_1\mathfrak{c})\sqrt{d}|} A. \tag{184}$$

Если, наконец, мы умножим обе части формул преобразования (180) при $\mathfrak{f}=1$ на $x^{\frac{n}{2}}$, возьмем $x\to 0$ и примем во внимание, что в знаменателе

$$\lim_{x\to 0} \sqrt{(x-2i\omega^{(1)})\dots(x-2i\omega^{(n)})} = |\sqrt{N(2\omega)}|\, e^{-\frac{\pi i}{4}(\operatorname{sgn}\omega^{(1)}+\dots+\operatorname{sgn}\omega^{(n)})},$$

то из (181) и (184), в силу $|d| = N(\mathfrak{d})$, получим

$$\frac{C(\omega)}{N(\mathfrak{a})} = |\sqrt{d}| \left|\frac{\sqrt{N(2\omega)}}{N(\mathfrak{b}_1)}\right| A e^{\frac{\pi i}{4} S(\operatorname{sgn}\omega)},$$

$$\frac{C(\omega)}{|\sqrt{N(\mathfrak{a})}|} = \left|\frac{\sqrt{N(2\mathfrak{b})}}{N(\mathfrak{b}_1)}\right| e^{\frac{\pi i}{4} S(\operatorname{sgn}\omega)} A \qquad \left(S(\operatorname{sgn}\omega) = \sum_{p=1}^{n} \operatorname{sgn}\omega^{(p)}\right).$$

Но величина A в свою очередь является суммой Гаусса и притом принадлежащей знаменателю $\mathfrak{b}_1$. В самом деле, если α — делящееся на $\mathfrak{c}$ целое число, такое, что $\frac{\alpha}{\mathfrak{c}}$ взаимно просто с $\mathfrak{b}_1$, то мы можем заменить в (183) ρ через $\rho\alpha$, заставляя тогда ρ пробегать полную систему вычетов $\bmod \mathfrak{b}_1$, и получим

$$A = C\left(-\frac{1}{4\omega}\,\frac{\alpha^2}{\mathfrak{d}^2}\right).$$

Таким образом, полагая $\frac{\alpha}{\mathfrak{d}} = \gamma$, получаем, наконец, следующую теорему:

Теорема 161. *Суммы Гаусса удовлетворяют соотношению взаимности*

$$\frac{C(\omega)}{|\sqrt{N(\mathfrak{a})}|} = \left|\frac{\sqrt{N(2\mathfrak{b})}}{N(\mathfrak{b}_1)}\right| e^{\frac{\pi i}{4} S(\operatorname{sgn}\omega)} C\left(-\frac{1}{4\omega}\gamma^2\right).$$

Здесь $\mathfrak{a}$ — *знаменатель идеала* $\mathfrak{d}\omega$, $\mathfrak{b}$ — *его числитель, далее,* $\mathfrak{b}_1$ — *знаменатель идеала* $\frac{\mathfrak{a}}{4\mathfrak{b}}$ *и* γ — *любое такое число поля, что* $\mathfrak{d}\gamma$ — *целое и взаимно простое с* $\mathfrak{b}_1$.

Проведенное нами доказательство станет нагляднее, если проделать его сначала применительно к специальному случаю, когда дифферента $\mathfrak{d}$ поля есть главный идеал и, в силу этого, введение идеала $\mathfrak{c}$ излишне.

§ 57. Взаимность между суммами Гаусса в произвольных алгебраических числовых полях

Пусть теперь k — произвольное числовое поле степени n; нумерацию сопряженных примем такую же, как в § 34, так что для всех чисел μ поля k

$\mu^{(p)}$ вещественно при $p = 1, 2, \ldots, r_1$,

$\mu^{(p)}$ комплексно сопряжено с $\mu^{(p+r_2)}$ при $p = r_1 + 1, \ldots, r_1 + r_2$.

Рассмотрим теперь функцию

$$\vartheta(t, z, \omega; \mathfrak{a}) = \sum_{\mu \text{ из } \mathfrak{a}} \exp\left\{-\pi \sum_{p=1}^{n} [t_p |\mu^{(p)} + z_p|^2 - 2i\omega^{(p)} (\mu^{(p)} + z_p)^2]\right\}, \quad (185)$$

где μ пробегает все числа произвольного фиксированного идеала $\mathfrak{a}\,(\neq 0)$ поля k и

$$t_p > 0 \quad \text{для всех } p = 1, \ldots, n,$$

$$t_{p+r_2} = t_p \quad \text{для } p = r_1 + 1, \ldots, r_1 + r_2,$$

$$z_p,\ \omega^{(p)} \quad \text{вещественны для } p = 1, \ldots, r_1,$$

$$\left.\begin{matrix} z_{p+r_2} \\ \omega^{(p+r_2)} \end{matrix}\right\} \text{комплексно сопряженные с } \left\{\begin{matrix} z_p \\ \omega^{(p)} \end{matrix}\right. \text{для } p = r_1 + 1, \ldots, r_1 + r_2.$$

Пусть снова $\alpha_1, \ldots, \alpha_n$ — базис $\mathfrak{a}$. Полагая

$$z_p = \sum_{k=1}^{n} \alpha_k^{(p)} u_k, \quad \mu^{(p)} = \sum_{k=1}^{n} \alpha_k^{(p)} m_k, \quad (186)$$

где $u_1, \ldots, u_n$ должны быть тогда вещественными, а $m_1, \ldots, m_n$ — целыми рациональными числами, убеждаемся в том, что показатель в (185) является квадратичной формой относительно $m_1 + u_1, \ldots, m_n + u_n$ с положительно определенной вещественной частью. Тем самым ряд (185) сходится и к нему применима теорема 158.

Коэфициенты Фурье имеют здесь следующее значение:

$$a((m)) = \int_{-\infty}^{+\infty} \ldots \int \exp\left\{-\pi \sum_{p=1}^{n} [t_p |z_p|^2 - 2i\omega^{(p)} z_p^2 - 2im_p u_p]\right\} dU, \quad (187)$$

где $z_1, \ldots, z_n$ связаны с переменными интеграции теми же соотношениями (186). Если мы выразим величины u через величины z, то показатель в (187), в силу теоремы 102, примет, как и в аналогичной формуле предыдущего параграфа, вид

$$-\pi \sum_{p=1}^{n} [t_p |z_p|^2 - 2i\omega^{(p)} z_p^2 - 2i\lambda^{(p)} z_p],$$

где

$$\lambda = \sum_{k=1}^{n} \beta_k m_k — \text{число из } \frac{1}{\mathfrak{ab}},$$

а β образуют базис $\frac{1}{\mathfrak{ab}}$, определенный соотношениями

$$\sum_{p=1}^{n} \beta_q^{(p)} \alpha_k^{(p)} = \begin{cases} 0 \text{ при } q \neq k, \\ 1 \text{ при } q = k. \end{cases}$$

Введем теперь в качестве вещественных переменных интеграции вместо u вещественные и мнимые части величин z: мы положим

$$\left.\begin{aligned} z_p &= x_p + iy_p \\ z_{p+r_2} &= x_p - iy_p \end{aligned}\right\} \quad p = r_1 + 1, \ldots, r_1 + r_2,$$

и

$$z_p = x_p, \qquad p = 1, \ldots, r_1.$$

Функциональный определитель величин $u_1, \ldots, u_n$ относительно величин x, y имеет, как мы уже видели в § 40, значение

$$\frac{2^{r_2}}{N(\mathfrak{a}) |\sqrt{d}|}; \tag{188}$$

показатель принимает вид

$$-\pi \sum_{p=1}^{r_1} (t_p - 2i\omega^{(p)})\, x_p^2 -$$

$$-\pi \sum_{p=r_1+1}^{r_1+r_2} \{2t_p (x_p^2 + y_p^2) - 2i [\omega^{(p)} (x_p + iy_p)^2 + \bar{\omega}^{(p)} (x_p - iy_p)^2]\} +$$

$$+ 2\pi i \sum_{p=1}^{r_1} \lambda^{(p)} x_p + 2\pi i \sum_{p=r_1+1}^{r_1+r_2} [\lambda^{(p)} (x_p + iy_p) + \bar{\lambda}^{(p)} (x_p - iy_p)].$$

Черточки над буквами означают переход к комплексно-сопряженным величинам.)

При этой подстановке интеграл (187) переходит в произведение r_1 простых интегралов соответственно по переменным $x_1, \ldots, x_{r_1}$, умноженное на произведение r_2 двойных интегралов по r_2 парам x_v, y_v.

При $p = 1, \ldots, r_1$ получаем

$$\int_{-\infty}^{+\infty} \exp \{-\pi (t_p - 2i\omega^{(p)})\, x^2 + 2\pi i \lambda^{(p)} x\}\, dx =$$

$$= \frac{1}{\sqrt{t_p - 2i\omega^{(p)}}}\, e^{-\pi \frac{\lambda^{(p)2}}{t_p - 2i\omega^{(p)}}}. \tag{189}$$

При этом корни берутся с положительной вещественной частью.

Двойные интегралы имеют следующий вид:

$$J=\int_{-\infty}^{+\infty}\int e^{\{-2\pi t(x^2+y^2)+2\pi i[\omega(x+iy)^2+\bar{\omega}(x-iy)^2+}$$

$$+\lambda(x+iy)+\bar{\lambda}(x-iy)]\}\,dx\,dy$$

Если теперь здесь $\omega=0$, то, как и выше, для интеграла получается значение

$$J=\frac{e^{-\frac{2\pi}{t}|\lambda|^2}}{2t}.$$

Если же $\omega\neq 0$, то мы приводим стоящую в показателе квадратичную форму переменных x, y к виду суммы квадратов путем введения вещественных переменных u, v:

$$\sqrt{\omega}\,(x+iy)=u+iv,$$

$$\sqrt{\bar{\omega}}\,(x-iy)=u-iv.$$

При этом значение корня $\sqrt{\omega}$ мы выбираем произвольно, а для $\sqrt{\bar{\omega}}$ берем тогда комплексно-сопряженное значение. Для функционального определителя получаем значение

$$\frac{\partial(x,y)}{\partial(u,v)}=\frac{1}{\sqrt{\omega}\sqrt{\bar{\omega}}}=\frac{1}{|\omega|};$$

показатель в подинтегральном выражении принимает теперь вид

$$-2\pi t\frac{u^2+v^2}{|\omega|}+4\pi i(u^2-v^2)+2\pi i\left(\frac{\lambda}{\sqrt{\omega}}(u+iv)+\frac{\bar{\lambda}}{\sqrt{\bar{\omega}}}(u-iv)\right)=$$

$$=\left(-\frac{2\pi t}{|\omega|}+4\pi i\right)u^2+2\pi i\left(\frac{\lambda}{\sqrt{\omega}}+\frac{\bar{\lambda}}{\sqrt{\bar{\omega}}}\right)u+$$

$$+\left(-\frac{2\pi t}{|\omega|}-4\pi i\right)v^2+2\pi i\left(\frac{i\lambda}{\sqrt{\omega}}-\frac{i\bar{\lambda}}{\sqrt{\bar{\omega}}}\right)v.$$

Тем самым J представляется в виде произведения двух простых интегралов и вычисление дает

$$J=\frac{1}{2\sqrt{t^2+4|\omega|^2}}\exp\left\{-\frac{2\pi t}{t^2+4|\omega|^2}|\lambda|^2-\frac{2\pi i}{t^2+4|\omega|^2}(\lambda^2\bar{\omega}+\bar{\lambda}^2\omega)\right\};\quad(190)$$

эта формула, очевидно, остается справедливой при $\omega=0$.

Если в этом выражении взять λ и ω вещественными, то показатель будет как раз равен удвоенному показателю из правой части формулы (189).

В итоге для $a(m_1, \ldots, m_n)$ получается значение

$$a(m_1, \ldots, m_n) = \frac{1}{N(\mathfrak{a})\,|\sqrt{d}|\,W(t,\omega)} \exp\left\{-\pi \sum_{p=1}^{n} \tau_p |\lambda^{(p)}|^2 + 2\pi i \sum_{p=1}^{n} \lambda^{(p)} \varkappa^{(p)}\right\},$$

где

$$\left.\begin{aligned} \tau_p &= \frac{t_p}{t_p^2 + 4|\omega^{(p)}|^2}, \\ \varkappa_p &= \frac{-\bar{\omega}^{(p)}}{t_p^2 + 4|\omega^{(p)}|^2}, \\ W(t,\omega) &= \prod_{p=1}^{r_1} \sqrt{t_p - 2i\omega^{(p)}} \prod_{p=r_1+1}^{r_1+r_2} \sqrt{t_p^2 + 4|\omega^{(p)}|^2}, \\ \lambda^{(p)} &= \sum_{q=1}^{n} \beta_q^{(p)} m_q. \end{aligned}\right\} \qquad (191)$$

При этом корни берутся с положительной вещественной частью.

Беря теперь в (185) $z_1, \ldots, z_n$, значит, также $u_1, \ldots, u_n$ равными нулю, мы прежде всего получаем из теоремы 158 следующую формулу преобразования:

Теорема 162. *Для функции, определенной рядом* (185), *имеет место формула преобразования*

$$\vartheta(t, 0, \omega; \mathfrak{f}) = \frac{1}{N(\mathfrak{f})\,|\sqrt{d}|\,W(t,\omega)}\, \vartheta\left(\tau, 0, \varkappa; \frac{1}{\mathfrak{f}\mathfrak{d}}\right), \qquad (192)$$

где t, ω *и* τ, $\varkappa$ *связаны соотношениями* (191).

Чтобы установить поведение обоих содержащихся здесь тэта-рядов при приближении к $t_1 = t_2 = \ldots = t_n = 0$, нужно знать поведение $\vartheta(t, z, \omega; \mathfrak{f})$ у этой точки. Оно определяется следующим предложением:

Лемма а). *Пусть* $\sigma_1(t_1)$, $\sigma_2(t_2)$, $\ldots$, $\sigma_n(t_n)$ — *такие функции соответственно от* $t_1, \ldots, t_n$, *что* $\sigma_{p+r_2} = \bar{\sigma}_p$ *при* $p = r_1 + 1, \ldots, r_1 + r_2$, σ_p *вещественны при* $p = 1, 2, \ldots, r_1$ *и* $\lim\limits_{t_p \to 0} \sigma_p(t_p) = 0$. *Тогда при одновременном стремлении* $t_1, \ldots, t_n$ *к нулю имеет место для всех* z *предельное соотношение*

$$\lim_{t \to 0} \sqrt{t_1 \ldots t_n}\, \vartheta(t_0, z, t\sigma; \mathfrak{f}) = \frac{1}{N(\mathfrak{f})\,|\sqrt{d}|}$$

Для доказательства мы должны лишь применить к ряду теорему 158 и подставить найденные выше значения для коэфициентов a. Именно, беря в качестве указателей отдельных членов числа λ вместо систем $m_1, \ldots, m_n$, мы получим тогда

$$\vartheta(t, z, t\sigma; \mathfrak{f}) = M \sum_{\lambda \text{ из } \frac{1}{\mathfrak{f}\mathfrak{d}}} b(\lambda)\, e^{2\pi i \sum_{p=1}^{n} \lambda^{(p)} z_p} \qquad (193)$$

где

$$M = \frac{1}{N(\mathfrak{f})\,|\sqrt{d}|\,W(t, t\sigma)},$$

$$b(\lambda) = \exp\left\{-\pi \sum_{p=1}^{n} \frac{|\lambda(p)|^2}{t_p(1+4|\sigma_p|^2)} - 2\pi i \sum_{p=1}^{n} \frac{\lambda(p)^2 \overline{\sigma_p}}{t_p(1+4|\sigma_p|^2)}\right\}.$$

Но

$$\lim_{t\to 0} \sqrt{t_1 \dots t_n}\, M = \frac{1}{N(\mathfrak{f})\,|\sqrt{d}|} \lim_{t\to 0} \frac{\sqrt{t_1 \dots t_n}}{W(t, t\sigma)} = \frac{1}{N(\mathfrak{f})\,|\sqrt{d}|},$$

а перенося в ряде (193) член с $\lambda = 0$ на другую сторону, мы получаем неравенство

$$|\vartheta(t, \dots) - M| \leqslant M \sum_{\substack{\lambda \text{ из } \frac{1}{\mathfrak{f}\mathfrak{d}} \\ \lambda \neq 0}} \exp\left\{-\pi \sum_{p=1}^{n} \frac{|\lambda(p)|^2}{t_p(1+4|\sigma_p|^2)}\right\},$$

из которого тогда, как и в предыдущем параграфе, вытекает утверждение леммы а).

Теперь, мы придем к сумме Гаусса, полагая в (192) ω равным отличному от нуля числу из k и $\mathfrak{f} = 1$;

$$\omega = \frac{\mathfrak{b}}{\mathfrak{a}\mathfrak{d}}, \quad (\mathfrak{a}, \mathfrak{b}) = 1.$$

Имеем

$$\vartheta(t, 0, \omega; 1) = \sum_{\rho \bmod \mathfrak{a}} e^{2\pi i S(\rho^2\omega)}\, \vartheta(t, \rho, 0; \mathfrak{a}).$$

В силу леммы а), получаем поэтому

$$\lim_{t\to 0} \sqrt{t_1 \dots t_n}\, \vartheta(t, 0, \omega; 1) = \frac{C(\omega)}{N(\mathfrak{a})\,|\sqrt{d}|}. \tag{194}$$

Для исследования правой части (192) мы введем целый идеал $\mathfrak{c}$, такой, что $\mathfrak{c}\mathfrak{d} = \delta$ — число из k, $(\mathfrak{c}, 4\mathfrak{b}) = 1$. Пусть, далее, $\mathfrak{b}_1$ — знаменатель идеала $\frac{\mathfrak{c}}{4\mathfrak{b}}$. Тогда, как и в предыдущем параграфе, из определения тэта-рядов непосредственно вытекает равенство

$$\vartheta\left(t, 0, \varkappa; \frac{1}{\mathfrak{d}}\right) = \vartheta\left(\frac{\tau}{|\delta^2|}, 0, \frac{\varkappa}{\delta^2}; \mathfrak{c}\right) = \sum_{\substack{\rho \bmod \mathfrak{b}_1 \\ \rho \equiv 0\ (\mathfrak{c})}} \vartheta\left(\frac{\tau}{|\delta^2|}, \rho, \frac{\varkappa}{\delta^2}; \mathfrak{b}_1\mathfrak{c}\right).$$

Но в силу (191),

$$\varkappa(p) = \frac{-\overline{\omega}(p)}{t_p^2 + 4|\omega(p)|^2} = -\frac{1}{4\omega(p)} + \frac{t_p^2}{4\omega(p)(t_p^2 + 4|\omega(p)|^2)},$$

$$\varkappa(p) = -\frac{1}{4\omega(p)} + \tau_p\sigma_p, \quad \text{где } \sigma_p = \frac{t_p}{4\omega(p)},$$

$$\vartheta\left(\frac{\tau}{|\delta|^2}, \rho, \frac{\varkappa}{\delta^2}; \mathfrak{b}_1\mathfrak{c}\right) = \vartheta\left(\frac{\tau}{|\delta|^2}, \rho, \frac{-1}{4\omega\delta^2} + \frac{\tau\sigma}{\delta^2}; \mathfrak{b}_1\mathfrak{c}\right) =$$

$$= e^{2\pi i S\left(\frac{-\rho^2}{4\omega\delta^2}\right)}\, \vartheta\left(\frac{\tau}{|\delta|^2}, \rho, \frac{\tau\sigma}{\delta^2}; \mathfrak{b}_1\mathfrak{c}\right).$$

К последнему же тэта-ряду применима лемма а) при t и, значит, τ, стремящихся к нулю. Это дает

$$\lim_{t\to 0} \sqrt{\frac{\tau_1 \dots \tau_\eta}{N(\mathfrak{d})^2}}\, \vartheta\left(\tau, 0, \varkappa; \frac{1}{\mathfrak{d}}\right) = \frac{1}{N(\mathfrak{d}_1\mathfrak{c})\,|\sqrt{d}|} \sum_{\substack{\rho \bmod \mathfrak{d}_1 \\ \rho \equiv 0\,(\mathfrak{c})}} e^{-2\pi i S\left(\frac{\rho^2}{4\omega\delta^2}\right)}. \quad (195)$$

Но сумма в правой части, как это было доказано в конце предыдущего параграфа, равна $C\left(\frac{-\gamma^2}{4\omega}\right)$, где γ — любое число из k, для которого

$$\mathfrak{d}\gamma \text{ — целое и взаимно простое с } \mathfrak{d}_1. \quad (196)$$

Поэтому равенство (195) может быть переписано в виде

$$\lim_{t\to 0} \sqrt{t_1 \dots t_n}\, \vartheta\left(\tau, 0, \varkappa; \frac{1}{\mathfrak{d}}\right) = \left|\frac{N(2\omega)\sqrt{d}}{N(\mathfrak{d}_1)}\right| \left(\frac{-\gamma^2}{4\omega}\right). \quad (197)$$

Наконец, если мы обе части формулы преобразования (192) умножим на $\sqrt{t_1 \dots t_n}$, возьмем $t \to 0$ и примем во внимание, что

$$\lim_{t\to 0} W(t, \omega) = |\sqrt{N(2\omega)}|\, e^{-\frac{\pi i}{4} S(\operatorname{sgn}\omega)},$$

где

$$S(\operatorname{sgn}\omega) = \operatorname{sgn}\omega^{(1)} + \dots + \operatorname{sgn}\omega^{(r_1)} \quad (=0, \text{ если } r_1 = 0), \quad (198)$$

то из (194), (197) получится

Теорема 163. *Для сумм Гаусса в k имеет место соотношение взаимности*

$$\frac{C(\omega)}{|\sqrt{N(\mathfrak{a})}|} = \left|\frac{\sqrt{N(2\mathfrak{b})}}{N(\mathfrak{d}_1)}\right| e^{\frac{\pi i}{4} S(\operatorname{sgn}\omega)}\, C\left(\frac{-\gamma^2}{4\omega}\right). \quad (199)$$

Здесь $\mathfrak{a}$, $\mathfrak{b}$ — целые взаимно простые идеалы, $\omega = \frac{\mathfrak{b}}{\mathfrak{a}\mathfrak{b}}$, $\mathfrak{d}_1$ — знаменатель идеала $\frac{\mathfrak{a}}{4\mathfrak{b}}$, а γ и $S(\operatorname{sgn}\omega)$ определены формулами (196) и (198).

Равенство (199) формально совпадает с равенством, данным в конце предыдущего параграфа, которое, однако, было доказано там лишь для вполне вещественных полей [1]).

§ 58. Определение знака сумм Гаусса в рациональном числовом поле

Формула (199) дает возможность определить значения сумм Гаусса. В настоящем параграфе мы выполним это для рационального число-

[1]) Это соотношение взаимности для квадратичных полей L. J. Mordell (1920) вывел без тэта-функций, используя лишь интегральную теорему Коши: On the reciprocity formula for the Gauss's sums in the quadratic field, Proc. of the London Mathem. Society, Ser. 2, vol. 20 (4). Родственная формула имеется уже у A. Krazer'a: Zur Theorie der mehrfachen Gaussschen Summen, Weber-Festschrift (1912).

вого поля и тем самым ответим на оставшийся еще нерешенным в § 52 (см. конец § 52, теорема 152) вопрос.

Дифферентой поля k является 1. Если поэтому a, b — взаимно простые целые рациональные числа, то

$$C\left(\frac{b}{a}\right)=\sum_{n \bmod a} e^{2\pi i \frac{n^2 b}{a}}.$$

Для нечетных a соотношение взаимности теоремы 163 дает

$$\frac{C\left(\frac{1}{a}\right)}{|\sqrt{a}|}=\frac{e^{\frac{\pi i}{4}\operatorname{sgn} a}}{2|\sqrt{2}|}C\left(\frac{-a}{4}\right)=\frac{e^{\frac{\pi i}{4}\operatorname{sgn} a}}{2\sqrt{2}}\sum_{a \bmod 4} e^{-2\pi i \frac{n^2 a}{4}},$$

$$C\left(\frac{-a}{4}\right)=2\left(1+e^{-\frac{\pi i}{2}a}\right)=2\left(1+(-i)^a\right)=2\left(1-i^a\right),$$

$$e^{\frac{\pi i}{4}\operatorname{sgn} a}=\frac{\sqrt{2}}{2}(1+i\operatorname{sgn} a),$$

$$\frac{C\left(\frac{1}{a}\right)}{|\sqrt{a}|}=\frac{1}{2}(1+i\operatorname{sgn} a)\left(1-i^a\right)=\begin{cases}1, & \text{если } a>0,\ a\equiv 1\ (4),\\ i, & \text{если } a>0,\ a\equiv 3\ (4),\end{cases}$$

$$C\left(\frac{1}{a}\right)=\sqrt{(-1)^{\frac{a-1}{2}}a} \quad \text{для } a>0,$$

где берется положительное, соответственно, положительно мнимое значение корня. С другой стороны, для простых a по формуле (171) (стр. 222)

$$C\left(\frac{1}{|a|}\right)=\sum_{n \bmod a}\left(\frac{n}{a}\right)e^{2\pi i \frac{n}{|a|}}.$$

Но для нечетного дискриминанта $a=d$, в силу (127),

$$\left(\frac{n}{a}\right)=\left(\frac{a}{n}\right) \quad \text{для } n>0.$$

Следовательно, для нечетных простых дискриминантов a

$$\sum_{n=1}^{|a|-1}\left(\frac{a}{n}\right)e^{2\pi i \frac{n}{|a|}}=(\operatorname{sgn} a)^{\frac{|a|-1}{2}}\sqrt{(-1)^{\frac{|a|-1}{2}}|a|}=\sqrt{a},$$

где берется положительное, соответственно, положительно мнимое значение корня.

Поэтому для сумм Гаусса $G(1, d)$, определенных в § 52 равенством (150), имеем

$$G(1, d)=\sqrt{d}, \text{ если } d \text{ — нечетное простое число,} \qquad (200)$$

причем для корня берется положительное, соответственно, положительно мнимое значение.

Далее, если d_1, d_2 — два нечетных взаимно простых дискриминанта, то, как показано в § 52,

$$G(1, d_1d_2) = \sum_{n \bmod d_1d_2} \left(\frac{n}{d_1}\right)\left(\frac{n}{d_2}\right) e^{2\pi i \frac{n}{|d_1d_2|}} = \left(\frac{|d_2|}{d_1}\right)\left(\frac{|d_1|}{d_2}\right) G(1, d_1)\, G(1, d_2) =$$

$$= (-1)^{\frac{\operatorname{sgn} d_1 - 1}{2} \cdot \frac{\operatorname{sgn} d_2 - 1}{2}} G(1, d_1)\, G(1, d_2).$$

Отсюда вытекает, что если (200) имеет место для двух нечетных взаимно простых дискриминантов d_1, d_2, то оно имеет место также для их произведения. Тем самым (200) справедливо для всех нечетных дискриминантов.

Остается еще вычислить $G(1, -4)$ и $G(1, \pm 8)$. Находим

$$G(1, -4) = 2i, \quad G(1, 8) = 2|\sqrt{2}|, \quad G(1, -8) = 2i|\sqrt{2}|. \quad (201)$$

Наконец, если u — нечетный дискриминант и q — дискриминант без нечетных простых множителей, то, в силу формул (152), (153) § 52,

$$G(1, qu) = \left(\frac{q}{u}\right)\left(\frac{u}{q}\right) G(1, q)\, G(1, u) = (-1)^{\frac{\operatorname{sgn} q - 1}{2} \cdot \frac{\operatorname{sgn} u - 1}{2}} G(1, q)\, G(1, u),$$

откуда, принимая во внимание (201), получаем в качестве окончательного результата следующую теорему:

Теорема 164. *Суммы Гаусса $G(1, d)$ для дискриминантов d квадратичных полей имеют значение*

$$G(1, d) = \sqrt{d}$$

с положительным, соответственно, положительно мнимым значением корня.

Тем самым числовой множитель ρ в формуле теоремы 152 для числа классов имеет, как уже было указано там, значение $+1$.

§ 59. Квадратичный закон взаимности и первая часть дополнительной теоремы

Теперь мы перейдем к выводу из формулы (199) квадратичного закона взаимности для любых алгебраических числовых полей. Введем прежде всего следующие определения:

Целое число поля k называется *примарным*, если оно нечетно и сравнимо с квадратом какого-либо числа из k по модулю 4.

Число α поля k называется *вполне положительным*, если r_1 его сопряженных $\alpha^{(1)}, \ldots, \alpha^{(r_1)}$ положительны.

Таким образом, если все сопряженные с k поля невещественны ($r_1 = 0$), то каждое число поля k вполне положительно. Не нужно

также упускать из виду, что выражение „α вполне положительно" имеет смысл лишь по отношению к заданному полю, содержащему α. Так, например, число -1 не является вполне положительным в $k(1)$ и, однако, вполне положительно в $k(i)$.

Для уяснения простой основной идеи нашего доказательства мы сделаем сначала *упрощающее предположение*, что диферента $\mathfrak{d}$ поля k является главным идеалом (в широком смысле), т. е. что в k существует число δ, для которого

$$(\delta) = \mathfrak{d}.$$

Пусть теперь α, β—целые нечетные взаимно простые числа. Полагая в (199)

$$\omega = \frac{1}{\alpha\beta\delta}, \quad \gamma = \frac{1}{\delta}, \quad \mathfrak{a} = \alpha\beta, \quad \mathfrak{b} = 1, \quad \mathfrak{b}_1 = 4,$$

получим

$$\frac{C\left(\frac{1}{\alpha\beta\delta}\right)}{|\sqrt{N(\alpha\beta)}|} = \frac{e^{\frac{\pi i}{4} S(\operatorname{sgn}\alpha\beta\delta)}}{|\sqrt{N(\delta)}|} C\left(\frac{-\alpha\beta}{4\delta}\right).$$

Кроме того, в силу (169) и теоремы 155,

$$C\left(\frac{1}{\alpha\beta\delta}\right) = \left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) C\left(\frac{1}{\alpha\delta}\right) C\left(\frac{1}{\beta\delta}\right).$$

Принимая теперь, что все суммы Гаусса с нечетным знаменателем или со знаменателем 4 отличны от нуля (ниже это будет доказано), мы можем применить ко всем трем суммам соотношение взаимности и получим

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = e^{\frac{\pi i}{4} S(\operatorname{sgn}\alpha\beta\delta - \operatorname{sgn}\alpha\delta - \operatorname{sgn}\beta\delta)} \frac{C\left(\frac{-\alpha\beta}{4\delta}\right)|\sqrt{N(\delta)}|}{C\left(\frac{-\alpha}{4\delta}\right) C\left(\frac{-\beta}{4\delta}\right)}. \tag{202}$$

Но если по крайней мере одно из чисел α, β, например α, примарно, то в силу (168)

$$C\left(\frac{-\alpha}{4\delta}\right) = C\left(\frac{-1}{4\delta}\right), \quad C\left(\frac{-\alpha\beta}{4\delta}\right) = C\left(\frac{-\beta}{4\delta}\right),$$

и из (202) при $\alpha\beta = 1$ вытекает

$$\frac{C\left(\frac{-1}{4\delta}\right)}{|\sqrt{N(\delta)}|} = e^{-\frac{\pi i}{4} S(\operatorname{sgn}\delta)}.$$

Таким образом мы получаем

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = e^{\frac{\pi i}{4} S(\operatorname{sgn}\alpha\beta\delta - \operatorname{sgn}\alpha\delta - \operatorname{sgn}\beta\delta + \operatorname{sgn}\delta)}.$$

Но для вещественных α, β, δ

$$\operatorname{sgn}\alpha\beta\delta - \operatorname{sgn}\alpha\delta - \operatorname{sgn}\beta\delta + \operatorname{sgn}\delta = (\operatorname{sgn}\alpha - 1)(\operatorname{sgn}\beta - 1)\operatorname{sgn}\delta \equiv 0 \pmod 4,$$

поэтому

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)=(-1)^{\sum_{p=1}^{r_1}\frac{\operatorname{sgn}\alpha(p)-1}{2}\cdot\frac{\operatorname{sgn}\beta(p)-1}{2}}$$

Это и есть квадратичный закон взаимности для пары нечетных взаимно простых чисел, из которых по крайней мере одно примарно.

Отбросим теперь ограничение, наложенное нами на поле k. Для общего случая, когда диферента поля k не является главным идеалом, доказательство усложнится необходимостью введения вспомогательного идеала.

Лемма a). *Все суммы Гаусса, принадлежащие нечетным знаменателям, отличны от нуля.*

В самом деле, пусть $C(\omega)$ — сумма, принадлежащая знаменателю $\mathfrak{a}$. Тогда все суммы, принадлежащие этому же знаменателю, мы получим в форме $C(\varkappa\omega)$, где $\varkappa$ пробегает приведенную систему вычетов mod $\mathfrak{a}$. Ибо, если $C(\omega_1)$ вместе с $C(\omega)$ принадлежит знаменателю $\mathfrak{a}$, то можно так определить целое число $\varkappa$, чтобы $\mathfrak{d}(\varkappa\omega-\omega_1)$ было целым идеалом, и тогда, в силу (168), $C(\varkappa\omega)=C(\omega_1)$. Но по теореме 155 $C(\varkappa\omega)$ отличается от $C(\omega)$ лишь множителем ± 1. Поэтому достаточно показать, что хотя бы одна сумма Гаусса, принадлежащая знаменателю $\mathfrak{a}$, отлична от нуля.

Выберем такой целый нечетный идеал $\mathfrak{c}$, взаимно простой с $\mathfrak{a}$, чтобы $\mathfrak{a}\mathfrak{c}\mathfrak{d}$ было целым числом поля k,

$$\mathfrak{a}\mathfrak{c}\mathfrak{d}=\varkappa.$$

В силу (169), сумма $C\left(\frac{1}{4\varkappa}\right)$ может быть тогда представлена в виде произведения трех сумм Гаусса, принадлежащих соответственно знаменателям 4, $\mathfrak{a}$, $\mathfrak{c}$. Таким образом для доказательства нашей леммы достаточно показать, что $C\left(\frac{1}{4\varkappa}\right)\neq 0$. Но это вытекает из формулы (199), написанной для $\omega=\frac{1}{4\varkappa}$, так как стоящая там справа сумма будет тогда принадлежать знаменателю 1, т. е. будет равна 1.

Лемма b). *Каждая сумма Гаусса, принадлежащая знаменателю 4, отлична от нуля.*

В самом деле, пусть $\mathfrak{a}$ — такой нечетный идеал, что $\mathfrak{a}\mathfrak{d}$ есть число поля, $\mathfrak{a}\mathfrak{d}=\varkappa$. Тогда для каждого нечетного целого числа μ, в силу леммы a), $C\left(\frac{1}{\mu\varkappa}\right)\neq 0$; поэтому вследствие равенства (199) также

$$C\left(\frac{-\gamma^2\varkappa\mu}{4}\right)\neq 0.$$

Но для любого числа φ поля k, такого, что $\mathfrak{d}\varphi$ имеет знаменатель 4, существует целое нечетное μ, для которого

$$\mathfrak{d}\left(\varphi+\frac{\gamma^2\varkappa\mu}{4}\right)\text{ есть целый идеал;}$$

в силу равенства

$$C(\varphi) = C\left(\frac{-\gamma^2\varkappa\mu}{4}\right),$$

необходимо $C(\varphi) \neq 0$.

Пусть теперь α, β — целые нечетные взаимно простые числа поля k. Пусть $\omega = \frac{\mathfrak{b}}{\mathfrak{d}}$, где $\mathfrak{b}$ — целый нечетный идеал, взаимно простой с $\alpha\beta$. В силу (169) и теоремы 155,

$$\left.\begin{aligned} C\left(\frac{\omega}{\alpha\beta}\right) = C\left(\frac{\beta\omega}{\alpha}\right) C\left(\frac{\alpha\omega}{\beta}\right) = \left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) C\left(\frac{\omega}{\alpha}\right) C\left(\frac{\omega}{\beta}\right), \\ \left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = \frac{C\left(\frac{\omega}{\alpha}\right) C\left(\frac{\omega}{\beta}\right)}{C\left(\frac{\omega}{\alpha\beta}\right)}. \end{aligned}\right\} \tag{203}$$

Применим теперь к каждой из этих трех сумм теорему 163, при этом $\mathfrak{b}_1 = 4\mathfrak{b}$, и мы получим

$$\frac{C\left(\frac{\omega}{\alpha}\right) C\left(\frac{\omega}{\beta}\right)}{C\left(\frac{\omega}{\alpha\beta}\right)} = \frac{1}{|\sqrt{N(8\mathfrak{b})}|} \frac{C\left(\frac{-\gamma^2\alpha}{4\omega}\right) C\left(\frac{-\gamma^2\beta}{4\omega}\right)}{C\left(\frac{-\gamma^2\alpha\beta}{4\omega}\right)} e^{\frac{\pi i}{4} S(\operatorname{sgn}\omega\alpha + \operatorname{sgn}\omega\beta - \operatorname{sgn}\omega\alpha\beta)}.$$

И здесь мы выразим $\sqrt{N(8\mathfrak{b})}$ через сумму Гаусса, полагая $\alpha = \beta = 1$, от чего левая часть обратится в 1; подставляя найденное выражение, получим

$$\frac{C\left(\frac{\omega}{\alpha}\right) C\left(\frac{\omega}{\beta}\right)}{C\left(\frac{\omega}{\alpha\beta}\right)} = v(\alpha, \beta) \frac{C\left(\frac{-\gamma^2\alpha}{4\omega}\right) C\left(\frac{-\gamma^2\beta}{4\omega}\right)}{C\left(\frac{-\gamma^2\alpha\beta}{4\omega}\right) C\left(\frac{-\gamma^2}{4\omega}\right)}, \tag{204}$$

где

$$v(\alpha, \beta) = e^{\frac{\pi i}{4} S(\operatorname{sgn}\omega\alpha + \operatorname{sgn}\omega\beta - \operatorname{sgn}\omega\alpha\beta - \operatorname{sgn}\omega)}$$

совершенно не зависит от ω, ибо для вещественных ω, α, β

$$\operatorname{sgn}\omega\alpha + \operatorname{sgn}\omega\beta - \operatorname{sgn}\omega\alpha\beta - \operatorname{sgn}\omega = -\operatorname{sgn}\omega(\operatorname{sgn}\alpha - 1)(\operatorname{sgn}\beta - 1)$$

делится на 4 и, следовательно,

$$v(\alpha, \beta) = (-1)^{\sum_{p=1}^{r_1} \frac{\operatorname{sgn}\alpha(p) - 1}{2} \frac{\operatorname{sgn}\beta(p) - 1}{2}}. \tag{205}$$

Характер зависимости правой части равенства (204) от ω мы сделаем более ясным, разлагая каждую сумму Гаусса со знаменателем $4\mathfrak{b}$ на две суммы со знаменателями соответственно 4 и $\mathfrak{b}$. Именно, представим γ в виде отношения двух целых идеалов:

$$\gamma = \frac{\mathfrak{c}}{\mathfrak{d}}, \text{ где } (\mathfrak{c}, 4\mathfrak{b}) = 1,$$

и выберем целый идеал $\mathfrak{m}$ так, чтобы $\mathfrak{b}\mathfrak{m}$ было равно нечетному числу μ; положим

$$\mu\frac{\gamma^2}{\omega}=\frac{\mathfrak{m}\mathfrak{c}^2}{\mathfrak{b}}=\varkappa.$$

Тогда, в силу (169) и теоремы 155,

$$C\left(\frac{-\gamma^2\alpha}{4\omega}\right)=C\left(\frac{-\varkappa\alpha}{4\mu}\right)=C\left(\frac{-\varkappa\mu\alpha}{4}\right)C\left(\frac{-4\varkappa\alpha}{\mu}\right)=$$
$$=\left(\frac{\alpha}{\mathfrak{b}}\right)C\left(\frac{-\varkappa\mu\alpha}{4}\right)C\left(-\frac{4\varkappa}{\mu}\right),$$

и, заменяя здесь α через 1, β, $\alpha\beta$, мы получим еще три аналогичных равенства. Далее, $\varkappa\mu=\omega\sigma^2$, где $\sigma=\mathfrak{m}\mathfrak{c}$ есть целый идеал. Поэтому в суммах со знаменателем 4 можно заменить $\varkappa\mu$ через ω. Таким образом из (203), (204) получаем, наконец,

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)=v(\alpha,\beta)\frac{C\left(\frac{-\omega\alpha}{4}\right)C\left(\frac{-\omega\beta}{4}\right)}{C\left(\frac{-\omega}{4}\right)C\left(\frac{-\omega\alpha\beta}{4}\right)},\qquad(206)$$

где ω — любое число поля, для которого $\mathfrak{b}\omega$ есть целый нечетный идеал.

Если мы предположим теперь, что здесь по крайней мере одно из чисел α, β, например α, примарно, то, в силу (16), получим

$$C\left(\frac{-\omega\alpha\beta}{4}\right)=C\left(\frac{-\omega\beta}{4}\right),\quad C\left(\frac{-\omega\alpha}{4}\right)=C\left(\frac{-\omega}{4}\right),$$

а из этого в соединении с (206) вытекает

Теорема 165. (Квадратичный закон взаимности.) *Для двух нечетных взаимно простых чисел α, β, из которых по крайней мере одно примарно, имеет место соотношение*

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)=(-1)^{\sum_{p=1}^{r_1}\frac{\operatorname{sgn}\alpha^{(p)}-1}{2}\cdot\frac{\operatorname{sgn}\beta^{(p)}-1}{2}}$$

Если по крайней мере одно из чисел α, β вполне положительно, то в правой части будет стоять $+1$.

Отсюда можно извлечь выводы относительно квадратичных характеров чисел некоторых специальных типов. Если β — единица или квадрат нечетного идеала, то для каждого нечетного α, взаимно простого с β, по самому определению, $\left(\frac{\alpha}{\beta}\right)=+1$. Если теперь для данного идеала $\mathfrak{a}$ существует такое вполне положительное примарное α, что $\alpha=\mathfrak{a}\mathfrak{c}^2$, то по теореме 164

$$\left(\frac{\beta}{\mathfrak{a}}\right)=\left(\frac{\beta}{\alpha}\right)=\left(\frac{\alpha}{\beta}\right)=+1.$$

Тем самым мы получили следующий результат:

Теорема 166. *Каждый нечетный идеал* $\mathfrak{a}$, *который в произведении с квадратом какого-нибудь идеала дает вполне положительное примарное число, обладает тем свойством, что для всех единиц или квадратов идеалов* ε, *взаимно простых с* $\mathfrak{a}$,

$$\left(\frac{\varepsilon}{\mathfrak{a}}\right)=+1.$$

Что эта теорема допускает обращение, будет доказано лишь в следующем параграфе.

Впрочем, равенство (206) дает значение $\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)$ и для всех нечетных непримарных α, β. Полагая, при фиксированном ω,

$$r(\alpha)=\frac{C\left(\frac{\omega}{4}\alpha\right)}{C\left(\frac{\omega}{4}\right)},$$

имеем

$$r(\alpha_1)=r(\alpha_2), \quad \text{если} \quad \alpha_1\equiv\alpha_2\xi^2 \pmod 4$$

при каком-либо нечетном ξ. Тогда (206) переходит в равенство

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)=v(\alpha,\ \beta)\frac{r(\alpha)\,r(\beta)}{r(\alpha\beta)}, \tag{207}$$

справедливое для всех нечетных взаимно простых α, β.

Вторая дополнительная теорема относится к случаю, когда одно из чисел α, β уже не является нечетным.

Пусть $\lambda=\mathfrak{l}\mathfrak{r}$ — разложение целого числа λ такое, что $\mathfrak{r}$ — нечетный идеал, а $\mathfrak{l}$ совсем не имеет нечетных простых множителей, т. е. $(2,\ \mathfrak{r})=1$. Пусть α — нечетное число, взаимно простое с λ, $\omega=\frac{\mathfrak{b}}{\mathfrak{d}}$, $(\mathfrak{b},\ 2\alpha\lambda)=1$. Из равенства

$$C\left(\frac{\lambda\omega}{\alpha}\right)=\left(\frac{\lambda}{\alpha}\right)C\left(\frac{\omega}{\alpha}\right),$$

справедливого в силу теоремы 155, получаем, применяя соотношение взаимности (199),

$$\left(\frac{\lambda}{\alpha}\right)=\frac{C\left(\frac{\lambda\omega}{\alpha}\right)}{C\left(\frac{\omega}{\alpha}\right)}=\frac{C\left(\frac{-\gamma^2\alpha}{4\omega\lambda}\right)}{C\left(\frac{-\gamma^2\alpha}{4\omega}\right)}\frac{e^{\frac{\pi i}{4}S(\operatorname{sgn}\lambda\omega\alpha-\operatorname{sgn}\omega\alpha)}}{|\sqrt{N(\lambda)}|}. \tag{208}$$

Полагая здесь, в частности, $\alpha=1$, получаем

$$1=\frac{C\left(\frac{-\gamma^2}{4\omega\lambda}\right)}{C\left(\frac{-\gamma^2}{4\omega}\right)}\frac{e^{\frac{\pi i}{4}S(\operatorname{sgn}\lambda\omega-\operatorname{sgn}\omega)}}{|\sqrt{N(\lambda)}|}. \tag{209}$$

Но, как и в предшествующем доказательстве, так как 4λ и $\mathfrak{b}$ взаимно просты, то

$$C\left(\frac{-\gamma^2\alpha}{4\omega\lambda}\right)=C\left(\frac{-\varkappa\mu\alpha}{4\lambda}\right)C\left(\frac{-4\lambda\varkappa\alpha}{\mu}\right)=\left(\frac{\alpha}{\mathfrak{b}}\right)C\left(\frac{-4\lambda\varkappa}{\mu}\right)C\left(\frac{-\varkappa\mu\alpha}{4\lambda}\right),$$

$$C\left(\frac{-\gamma^2\alpha}{4\omega}\right)=\left(\frac{\alpha}{\mathfrak{b}}\right)C\left(\frac{-4\varkappa}{\mu}\right)C\left(\frac{-\varkappa\mu\alpha}{4}\right),$$

и, снова при $\alpha=1$, почленно деля, получаем

$$\left.\begin{aligned}\frac{C\left(\frac{-\gamma^2}{4\omega\lambda}\right)}{C\left(\frac{-\gamma^2}{4\omega}\right)}&=\frac{C\left(\frac{-4\lambda\varkappa}{\mu}\right)}{C\left(\frac{-4\varkappa}{\mu}\right)}\,\frac{C\left(\frac{-\varkappa\mu}{4\lambda}\right)}{C\left(\frac{-\varkappa\mu}{4}\right)},\\ \frac{C\left(\frac{-\gamma^2\alpha}{4\omega\lambda}\right)}{C\left(\frac{-\gamma^2\alpha}{4\omega}\right)}&=\frac{C\left(\frac{-\gamma^2}{4\omega\lambda}\right)}{C\left(\frac{-\gamma^2}{4\omega}\right)}\,\frac{C\left(\frac{-\varkappa\mu\alpha}{4\lambda}\right)C\left(\frac{-\varkappa\mu}{4}\right)}{C\left(\frac{-\varkappa\mu}{4\lambda}\right)C\left(\frac{-\varkappa\mu\alpha}{4}\right)}\end{aligned}\right\}\qquad(210)$$

причем мы можем еще заменить $\varkappa\mu$ через ω. Деля почленно (210) на (209) и принимая во внимание (208), получаем

$$\left(\frac{\lambda}{\alpha}\right)=v(\alpha,\ \lambda)\,\frac{C\left(\frac{-\omega\alpha}{4\lambda}\right)C\left(\frac{-\omega}{4}\right)}{C\left(\frac{-\omega}{4\lambda}\right)C\left(\frac{-\omega\alpha}{4}\right)}.\qquad(211)$$

Но суммы Гаусса со знаменателем $4\lambda=4\mathfrak{l}\mathfrak{r}$, как и выше, могут быть выражены, в силу (169), через суммы Гаусса со знаменателями соответственно $4\mathfrak{l}$ и $\mathfrak{r}$. Выберем тогда нечетные и взаимно простые с $\mathfrak{r}\alpha$ идеалы $\mathfrak{m}$, $\mathfrak{n}$, так чтобы

$$\mathfrak{l}\mathfrak{m}=\lambda_1,\quad \mathfrak{r}\mathfrak{n}=\rho,\quad \mathfrak{m}\mathfrak{n}=\frac{\lambda_1\rho}{\lambda}=\sigma.$$

Тогда

$$C\left(\frac{-\omega\alpha}{4\lambda}\right)=C\left(\frac{-\omega\sigma\alpha}{4\lambda_1\rho}\right)=C\left(\frac{-\omega\sigma\rho\alpha}{4\lambda_1}\right)C\left(\frac{-4\lambda_1\omega\sigma\alpha}{\rho}\right)=$$
$$=\left(\frac{\alpha}{\mathfrak{r}}\right)C\left(\frac{-\omega\sigma\rho\alpha}{4\lambda_1}\right)C\left(\frac{-4\lambda_1\omega\sigma}{\rho}\right)=\left(\frac{\alpha}{\mathfrak{r}}\right)C\left(\frac{-\omega\rho^2\alpha}{4\lambda}\right)C\left(\frac{-4\lambda_1\omega\sigma}{\rho}\right).$$

Наконец, полагая здесь $\alpha=1$ и внося результат в (211), получаем

$$\left(\frac{\lambda}{\alpha}\right)\left(\frac{\alpha}{\mathfrak{r}}\right)=v(\alpha,\ \lambda)\,\frac{C\left(\frac{-\omega\rho^2\alpha}{4\lambda}\right)C\left(\frac{-\omega}{4}\right)}{C\left(\frac{-\omega\rho^2}{4\lambda}\right)C\left(\frac{-\omega\alpha}{4}\right)}.$$

Здесь ρ — любое нечетное число, делящееся на $\mathfrak{r}$. Последние суммы зависят только от поведения α mod $4\mathfrak{l}$. Выбирая, в частности, α квадратичным вычетом mod $4\mathfrak{l}$, получаем следующий результат:

Теорема 167. *Пусть* $\mathfrak{l}$ — *целый идеал без нечетных простых множителей и* λ — *целое число, могущее быть представленным*

в виде $\lambda = \mathfrak{l}\mathfrak{r}$, *где* $\mathfrak{r}$ — *целый нечетный идеал. Тогда для всякого нечетного* α, *взаимно простого с* λ *и являющегося квадратичным вычетом* mod $4\mathfrak{l}$, *имеет место равенство*

$$\left(\frac{\lambda}{\alpha}\right)\left(\frac{\alpha}{\mathfrak{r}}\right) = (-1)^{\sum_{\mathfrak{p}=1}^{\mathfrak{r}_1} \frac{\operatorname{sgn}\alpha^{(\mathfrak{p})}-1}{2}\,\frac{\operatorname{sgn}\lambda^{(\mathfrak{p})}-1}{2}}.$$

§ 60. Относительно квадратичные поля и их применение к теории квадратичных вычетов

Рассмотрим относительное поле $K = K(\sqrt{\mu},\ k)$, произведенное присоединением к полю k квадратного корня числа μ из k. Для этого поля имеют место теоремы § 39 с $l = 2$. Здесь целесообразно ввести квадратичный характер, несколько отличающийся от символа квадратичных вычетов.

Определение. Пусть $\mathfrak{p}$ — любой простой идеал поля k. Тогда

$$Q(\mu,\ \mathfrak{p}) = \begin{cases} 1, & \text{если } \mathfrak{p} \text{ в } K(\sqrt{\mu},\ k) \text{ разлагается на два различных множителя,} \\ -1, & \text{„ } \mathfrak{p} \text{ „ } K(\sqrt{\mu},\ k) \text{ остается неразложимым,} \\ 0, & \text{„ } \mathfrak{p} \text{ „ } K(\sqrt{\mu},\ k) \text{ является квадратом простого идеала.} \end{cases}$$

В силу результатов § 39, $Q(\mu,\ \mathfrak{p})$ получает, таким образом, определенный смысл для всех простых идеалов, если к k принадлежит μ и не принадлежит $\sqrt{\mu}$. Кроме того,

$$Q(\mu,\ \mathfrak{p}) = \left(\frac{\mu}{\mathfrak{p}}\right), \text{ если } \mathfrak{p} \text{ нечетно и не делит } \mu, \tag{212}$$

$$Q(\mu\alpha^2,\ \mathfrak{p}) = Q(\mu,\ \mathfrak{p}) \text{ для всех } \alpha \neq 0 \text{ из } k.$$

Положим, далее, для любого отличного от нуля целого идеала $\mathfrak{a} = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\ldots\mathfrak{p}_m^{a_m}$ из k

$$Q(\mu,\ \mathfrak{a}) = Q(\mu,\ \mathfrak{p}_1)^{a_1} Q(\mu,\ \mathfrak{p}_2)^{a_2} \ldots Q(\mu,\ \mathfrak{p}_m)^{a_m}, \tag{213}$$

и для каждого квадрата μ^2 из k

$$Q(\mu^2,\ \mathfrak{a}) = 1.$$

В силу (213), имеем для двух целых идеалов $\mathfrak{a}$, $\mathfrak{b}$ из k

$$Q(\mu,\ \mathfrak{a}\mathfrak{b}) = Q(\mu,\ \mathfrak{a})\,Q(\mu,\ \mathfrak{b}).$$

Наконец, для нечетного $\mathfrak{a}$, взаимно простого с целыми числами μ и ν,

$$Q(\mu\nu,\ \mathfrak{a}) = Q(\mu,\ \mathfrak{a})\,Q(\nu,\ \mathfrak{a}).$$

В рациональном числовом поле введение подобного символа было бы излишним, так как в этом поле мы всегда можем предполагать число

освобожденным от ненужных квадратных множителей. Однако в других полях, в случае если число классов в них четно, μ может также иметь неустранимые квадратные множители.

С помощью символа Q дзета-функция поля K может быть выражена через дзета-функцию поля k и еще один ряд, с чем мы уже встретились в § 49 при изучении квадратичных полей. Именно, пусть $\mathfrak{P}$ — простой идеал поля K. Тогда, в обозначениях теоремы 108,

$$N_k(\mathfrak{P}) = \mathfrak{p} \text{ или } \mathfrak{p}^2 \text{ и } N(\mathfrak{P}) = n(\mathfrak{p}) \text{ или } n(\mathfrak{p}^2),$$

где $\mathfrak{p}$ — делящийся на $\mathfrak{P}$ простой идеал из k. Выделим в бесконечном произведении

$$\zeta_K(s) = \prod_{\mathfrak{P}} \frac{1}{1 - N(\mathfrak{P})^{-s}}$$

часть, распространенную на простые множители $\mathfrak{P}$ некоторого фиксированного $\mathfrak{p}$. Она может быть представлена в виде

$$\prod_{\mathfrak{P}|\mathfrak{p}} (1 - N(\mathfrak{P})^{-s})^{-1} = (1 - n(\mathfrak{p})^{-s})^{-1} (1 - Q(\mu, \mathfrak{p})\, n(\mathfrak{p})^{-s})^{-1},$$

и поэтому

$$\zeta_K(s) = \zeta_k(s)\, Z(s),$$

где

$$Z(s) = \prod_{\mathfrak{p}} \frac{1}{1 - Q(\mu, \mathfrak{p})\, n(\mathfrak{p})^{-s}} = \sum_{\mathfrak{a}} \frac{Q(\mu, \mathfrak{a})}{n(\mathfrak{a})^s}.$$

Так как, в силу формулы теоремы 123 для числа классов,

$$\lim_{s \to 1} \frac{\zeta_K(s)}{\zeta_k(s)}$$

равен конечному отличному от нуля числу, то имеет место

Теорема 168.

$$\lim_{s \to 1} \ln Z(s) \text{ } \textit{конечен.}$$

Из этого факта мы выведем аналог теоремы 147:

Теорема 169. *Пусть* $\mu_1, \ldots, \mu_m$ — *целые числа поля* k, *такие, что произведение их степеней* $\mu_1^{x_1} \ldots \mu_m^{x_m}$ *лишь тогда является квадратом числа из* k, *когда все показатели* $x_1, \ldots, x_m$ *четны. Пусть* $c_1, \ldots, c_m$ — *произвольно заданные значения* ± 1. *Тогда в поле* k *существует бесконечное множество простых идеалов* $\mathfrak{p}$, *удовлетворяющих* m *условиям*

$$\left(\frac{\mu_1}{\mathfrak{p}}\right) = c_1, \ldots, \left(\frac{\mu_m}{\mathfrak{p}}\right) = c_m.$$

В самом деле, в силу предположения теоремы, квадратный корень каждого из $2^m - 1$ произведений степеней $\mu = \mu_1^{x_1} \ldots \mu_m^{x_m}$ ($x_i =$

$=0$ или 1, и не все $x_i=0$) порождает относительно квадратичное поле $K(\sqrt{\mu}, k)$. Но, как и в § 49, при $s>1$, очевидно,

$$\ln\prod_{\mathfrak{p}}\left(1-\frac{Q(\mu,\mathfrak{p})}{n(\mathfrak{p})^s}\right)=-\sum_{\mathfrak{p}}\frac{Q(\mu,\mathfrak{p})}{n(\mathfrak{p})^s}+\varphi(\mu,s),$$

где $\varphi(\mu, s)$ при $s\to 1$ стремится к конечному пределу. А тогда по теореме 168 первая сумма в правой части также обладает этим свойством, и, значит,

$$L(s,\chi)=\sum_{\mathfrak{p}}{}'\left(\frac{\mu}{\mathfrak{p}}\right)\frac{1}{n(\mathfrak{p})^s},$$

где штрих при сумме указывает, что $\mathfrak{p}$ пробегает лишь нечетные простые идеалы, не входящие в $\mu_1, \ldots, \mu_m$, остается конечной, так как, в силу (212), обе суммы отличаются друг от друга лишь конечным числом членов. С другой стороны, из неограниченного возрастания $\zeta_k(s)$ при $s\to 1$ вытекает, как и прежде, что

$$L(s,1)=\sum_{\mathfrak{p}}{}'\frac{1}{n(\mathfrak{p})^s}\to\infty.$$

Отсюда следует, что в равенстве

$$\sum_{x_1,\ldots,x_m=0;\,1} c_1^{x_1}\ldots c_m^{x_m}L(s,\chi_1^{x_1}\ldots\chi_m^{x_m})=$$

$$=\sum_{\mathfrak{p}}{}'\left(1+c_1\left(\frac{\mu_1}{\mathfrak{p}}\right)\right)\ldots\left(1+c_m\left(\frac{\mu_m}{\mathfrak{p}}\right)\right)\frac{1}{n(\mathfrak{p})^s}$$

при $s\to 1$ левая часть неограниченно возрастает. Но в правой части не обращаются в нуль лишь члены, у которых $\mathfrak{p}$ удовлетворяют требованиям утверждения нашей теоремы. Следовательно, должно существовать бесконечное множество таких $\mathfrak{p}$.

Эта теорема существования послужит важнейшим вспомогательным средством при доказательстве обращения теорем 166 и 167, к которому мы теперь перейдем.

§ 61. Группы чисел и группы идеалов. Сингулярные примарные числа

В дальнейшем исследовании мы будем иметь дело с факторгруппами абелевых групп, определяемыми квадратами элементов. Пусть $\mathfrak{G}$ — абелева группа, $\mathfrak{U}_2$ — подгруппа квадратов всех элементов из $\mathfrak{G}$. Смежные классы по подгруппе $\mathfrak{U}_2$ мы будем называть *соединениями* элементов из $\mathfrak{G}$. По § 9 факторгруппа $\mathfrak{G}/\mathfrak{U}_2$ есть группа соединений. Единичным элементом в этой факторгруппе служит *главное соединение*, т. е. система элементов из $\mathfrak{U}_2$. Квадрат каждого соединения является главным соединением, и если $\mathfrak{G}$ — конечная группа, то существует точно 2^e различных соединений, где e — базисное число

группы $\mathfrak{G}$, принадлежащее 2. Число независимых соединений, т. е. независимых элементов группы $\mathfrak{G}/\mathfrak{U}_2$, будет тогда e.

Введем теперь ряд важных групп, соединений и связанных с ними констант.

1. Единицы поля k образуют группу по умножению. Число различных *единичных соединений* равно 2^m, где $m = \frac{n + r_1}{2}$. Действительно, имеется $r_1 + r_2 - 1 = m - 1$ основных единиц, и к ним прибавляется еще содержащийся в k корень из 1, квадратный корень из которого уже не содержится в k.

2. Совокупность всех чисел поля k, отличных от нуля, образуют группу по умножению. Числовое соединение есть система всех чисел $\alpha\xi^2$, где α фиксировано, а ξ пробегает все числа из k, отличные от нуля. Называя последовательностью знаков числа ω поля k систему r_1 чисел $\operatorname{sgn}\omega^{(1)}, \ldots, \operatorname{sgn}\omega^{(r_1)}$ (причем если $r_1 = 0$, то под этим разумеется число $+1$), мы видим, что все числа из одного и того же соединения имеют одну и ту же последовательность знаков. В группе всех числовых соединений группа *вполне положительных числовых соединений* образует подгруппу индекса 2^{r_1}, ибо при $r_1 > 0$ в поле k существуют числа ω с любой наперед заданной последовательностью знаков. Последнее вытекает из того, что r_1 выражений

$$a_0 + a_1\vartheta^{(i)} + \ldots + a_{r_1-1}\vartheta^{(i)r_1-1} \qquad (i = 1, \ldots, r_1),$$

где ϑ — производящее число поля k, образуют при должном выборе вещественных a любую систему вещественных значений и, значит, при рациональных a — любую комбинацию знаков.

3. В группе классов идеалов поля k имеется точно 2^e различных соединений классов, где e — принадлежащее 2 базисное число группы классов.

4. Числовые соединения, числа которых являются квадратами идеалов поля k, образуют подгруппу группы всех числовых соединений. Порядок ее есть 2^{m+e}. В самом деле, в силу п. 3, существует e идеалов $\mathfrak{a}_1, \ldots, \mathfrak{a}_e$, определяющих e независимых соединений классов, причем квадраты этих идеалов суть главные идеалы, $\mathfrak{a}_i^2 = \mathfrak{a}_i\,(i = 1, \ldots, e)$. e чисел $\alpha_1, \ldots, \alpha_e$ определяют e независимых числовых соединений. Если теперь ω — число, являющееся квадратом некоторого идеала с поля k, то с эквивалентен некоторому произведению степеней идеалов $\mathfrak{a}_1, \ldots, \mathfrak{a}_e$ и поэтому ω, по умножении на некоторую единицу, отличается от соответствующего произведения степеней чисел $\alpha_1, \ldots, \alpha_e$ множителем, являющимся квадратом числа.

Будем называть число поля k *сингулярным*, если оно является квадратом идеала из k. Таким образом существует $m + e$ независимых сингулярных числовых соединений. Они представляются числами $\alpha_1, \ldots, \alpha_e$ и m единицами из независимых соединений.

5. Пусть p — количество независимых сингулярных числовых соединений, состоящих из вполне положительных чисел. Тогда существует 2^p *сингулярных вполне положительных числовых соединений.*

В силу этого, во всех 2^{m+e} сингулярных числовых соединениях содержатся числа лишь с 2^{m+e-p} различными последовательностями знаков.

6. Будем причислять два различных не равных нулю идеала $\mathfrak{a}$, $\mathfrak{b}$ к одному и тому же *классу идеалов в узком смысле* и называть $\mathfrak{a}$ и $\mathfrak{b}$ *эквивалентными в узком смысле*, если $\frac{\mathfrak{a}}{\mathfrak{b}}$ может быть приравнено какому-нибудь вполне положительному числу поля. Будем в этом случае, как и прежде, писать $\mathfrak{a} \approx \mathfrak{b}$. Классы в узком смысле, как и прежде, образуют абелеву группу — группу классов в узком смысле. Классы в узком смысле, содержащие главные идеалы в широком смысле, образуют в этой группе подгруппу индекса h. Главные идеалы, очевидно, определяют не более 2^{r_1} различных классов в узком смысле. Поэтому порядок группы классов в узком смысле не превышает $2^{r_1}h$. Пусть e_0 — принадлежащее 2 базисное число этой группы классов в узком смысле. Обозначим через $\mathfrak{J}_0$ *группу соединений классов идеалов в узком смысле*. Порядок ее, таким образом, равен 2^{e_0}. Вычисляя порядок группы $\mathfrak{J}_0$ другим способом, мы получим равенство

$$e_0 = p + r_1 - m. \tag{214}$$

Именно, пусть $\mathfrak{H}$ — подгруппа группы $\mathfrak{J}_0$, соединения классов которой могут быть представлены главными идеалами (в широком смысле). Из общих теоретико-групповых теорем следует, что порядок группы $\mathfrak{J}_0$ равен произведению порядка факторгруппы $\mathfrak{J}_0/\mathfrak{H}$ на порядок группы $\mathfrak{H}$. Но факторгруппа $\mathfrak{J}_0/\mathfrak{H}$ имеет порядок 2^e. В самом деле, если $\mathfrak{b}_1, \ldots, \mathfrak{b}_e$ — представители e независимых соединений классов (в широком смысле), то 2^e произведений степеней $\mathfrak{b} = \mathfrak{b}_1^{x_1} \ldots \mathfrak{b}_e^{x_e}$ ($x_i = 0$ или 1) определяют точно 2^e различных смежных систем в $\mathfrak{J}_0$ по $\mathfrak{H}$. С другой стороны, для каждого идеала $\mathfrak{a}$ существуют произведение степеней $\mathfrak{b}$ и квадрат идеала $\mathfrak{c}^2$ такие, что $\mathfrak{a} \sim \mathfrak{b}\mathfrak{c}^2$ и, следовательно, $\mathfrak{a} = \alpha\mathfrak{b}\mathfrak{c}^2$ для некоторого числа α. Следовательно, соединение, которому принадлежит $\mathfrak{a}$, отличается от соединения, которому принадлежит $\mathfrak{b}$, соединением, которому принадлежит α, т. е. некоторым соединением из группы $\mathfrak{H}$. Таким образом группа $\mathfrak{J}_0/\mathfrak{H}$ имеет порядок 2^e.

Но теперь главный идеал (γ) принадлежит единичному элементу группы $\mathfrak{J}_0$ тогда и только тогда, когда (γ) эквивалентно в узком смысле квадрату какого-нибудь идеала, т. е. если γ равно произведению вполне положительного числа на сингулярное, т. е. если γ может быть дополнено до вполне положительного числа путем умножения на некоторое сингулярное. В силу п. 5, из 2^{r_1} возможных для γ последовательностей знаков сингулярными числами реализуются точно 2^{m+e-p}, так что, таким образом, главными идеалами определяются точно $2^{r_1-(m+e-p)}$ различных соединений классов идеалов в узком смысле. Следовательно, этому числу равен порядок группы $\mathfrak{H}$, и утверждение (214) доказано.

7. Совокупность нечетных классов вычетов mod 4 содержит точно 2^n *различных соединений классов вычетов* mod 4. В самом деле,

из $\xi^2 \equiv 1 \pmod 4$ вытекает $\xi \equiv 1 \pmod 2$, $\xi = 1 + 2\omega$ с целым ω. А среди этих чисел имеется $N(2) = 2^n$ несравнимых mod 4.

8. Будем причислять два числа α, β к одному и тому же классу вычетов в узком смысле mod $\mathfrak{a}$, если $\alpha \equiv \beta \pmod{\mathfrak{a}}$ и $\frac{\alpha}{\beta}$ вполне положительно. Но в каждом классе вычетов mod $\mathfrak{a}$ существуют числа α, сопряженные которых $\alpha^{(1)}, \ldots, \alpha^{(r_1)}$ имеют те же знаки, что и произвольно заданное целое число ω. В самом деле, $\alpha + xN(\mathfrak{a})\omega$ для каждого целого рационального x принадлежит тому же классу mod $\mathfrak{a}$, что и α, и для всех достаточно больших x, очевидно, обладает требуемым свойством. Таким образом каждый класс вычетов mod $\mathfrak{a}$ распадается точно на 2^{r_1} классов вычетов в узком смысле mod $\mathfrak{a}$. В частности, существует 2^{n+r_1} *различных соединений классов вычетов в узком смысле* mod 4.

9. Пусть $\mathfrak{l}$ — простой множитель числа 2. Совокупность нечетных классов вычетов mod $4\mathfrak{l}$ содержит 2^{n+1} *различных соединений классов вычетов* mod $4\mathfrak{l}$. В самом деле, из $\xi^2 \equiv 1 \pmod{4\mathfrak{l}}$ вытекает, что $\xi = 1 + 2\omega$ с целым ω, удовлетворяющим условию $\omega(\omega + 1) \equiv 0 \pmod{\mathfrak{l}}$, следовательно, $\omega \equiv 0$ или $1 \pmod{\mathfrak{l}}$. Это дает для ξ точно $2N(2) = 2^{n+1}$ несравнимых mod $4\mathfrak{l}$ чисел. Соответственно существует 2^{n+r_1+1} различных соединений классов вычетов в узком смысле mod $4\mathfrak{l}$.

10. Главный интерес представляют сингулярные числа, являющиеся одновременно примарными и вместе с тем не являющиеся квадратами чисел. Такие числа называются *сингулярными примарными числами*. В силу теоремы 120, сингулярные примарные числа ω порождают поля $K(\sqrt{\omega}, k)$, имеющие относительно k дискриминант 1. Пусть имеется q *независимых соединений сингулярных примарных чисел*. Тогда, в силу п. 4, $q \leqslant m + e$. Таким образом 2^{m+e} различных сингулярных числовых соединений определяют 2^{m+e-q} различных соединений классов вычетов mod 4, так как точно 2^q этих числовых соединений примарны, т. е. принадлежат главному соединению классов вычетов mod 4.

11. Точно так же пусть q_0 означает *число независимых соединений сингулярных примарных вполне положительных чисел*. 2^{m+e} различных сингулярных числовых соединений определяет, таким образом, лишь 2^{m+e-q_0} различных соединений классов вычетов в узком смысле mod 4, так как по 2^{q_0} сингулярных числовых соединений определяют одно и то же соединение классов вычетов в узком смысле mod 4.

12. Наконец, теорема 166 приводит к новому разбиению всех нечетных идеалов на классы по модулю 4. Мы будем причислять два целых нечетных идеала к одному и тому же „*классу идеалов* mod 4“, если в k существует такой квадрат идеала $\mathfrak{c}^2$, что $\mathfrak{a} \sim \mathfrak{b}\mathfrak{c}^2$ и могут быть выбраны целые числа α, β, удовлетворяющие условиям $\alpha\mathfrak{a} = \beta\mathfrak{b}\mathfrak{c}^2$ и $\alpha \equiv \beta \equiv 1 \pmod 4$. Определяя композицию этих классов с помощью умножения идеалов, получаем „*группу классов* mod 4“; будем обозначать ее через $\mathfrak{B}$.

Для определения порядка группы $\mathfrak{B}$ введем подгруппу $\mathfrak{H}$ тех классов из $\mathfrak{B}$, которые могут быть представлены целыми нечетными главными идеалами. В силу общих теоретико-групповых теорем, порядок $\mathfrak{B}$ будет равен произведению порядка $\mathfrak{H}$ на порядок факторгруппы $\mathfrak{B}/\mathfrak{H}$. Но эта факторгруппа имеет порядок 2^e. В самом деле, пусть $\mathfrak{b}_1, \ldots, \mathfrak{b}_e$ — нечетные представители e независимых соединений классов идеалов. Тогда 2^e произведений степеней $\mathfrak{b}_1^{x_1} \ldots \mathfrak{b}_e^{x_e} = \mathfrak{b}$ ($x_i = 0$ или 1) определяют точно 2^e различных смежных классов $\mathfrak{B}$ по $\mathfrak{H}$. С другой стороны, для каждого нечетного идеала $\mathfrak{a}$ существуют произведение $\mathfrak{b}$ и нечетный квадрат идеала $\mathfrak{c}^2$ такие, что $\mathfrak{a} \sim \mathfrak{b}\mathfrak{c}^2$, следовательно, имеет место равенство $\alpha\mathfrak{a} = \beta\mathfrak{b}\mathfrak{c}^2$ с нечетными числами α, β. Путем почленного умножения этого равенства на некоторое число можно добиться выполнения сравнения $\alpha \equiv 1 \pmod 4$, следовательно, $\mathfrak{a}$ и $\beta\mathfrak{b}$ будут принадлежать одному и тому же классу идеалов mod 4. Но $\beta\mathfrak{b}$ и $\mathfrak{b}$ различаются лишь идеалом из $\mathfrak{H}$, следовательно, также каждый смежный класс $\mathfrak{B}$ по $\mathfrak{H}$ представим произведением $\mathfrak{b}$, т. е. $\mathfrak{B}/\mathfrak{H}$ действительно имеет порядок 2^e.

Для нахождения, далее, порядка группы $\mathfrak{H}$ заметим, что два целых нечетных числа γ_1, γ_2 во всяком случае определяют главные идеалы (γ_1) и (γ_2) из одного класса идеалов mod 4, когда γ_1 и γ_2 принадлежат одному и тому же соединению классов вычетов mod 4. Класс идеалов mod 4, содержащий идеал (1), состоит из всех нечетных идеалов (γ), где γ сравнимо mod 4 с каким-либо сингулярным числом. Но по п. 10 сингулярные числа определяют точно 2^{m+e-q} различных соединений классов вычетов mod 4. Следовательно, 2^n соединений классов вычетов mod 4 распределяются по 2^{m+e-q} на один и тот же класс идеалов mod 4. Поэтому порядок группы $\mathfrak{H}$ равен $2^{n-(m+e-q)}$. В итоге получаем, что

$$\text{порядок } \mathfrak{B} \text{ равен } 2^{n-m+q} = 2^{m-r_1+q}.$$

13. Если $r_1 > 0$, то соответственно определяем группу $\mathfrak{B}_0$ „*классов идеалов в узком смысле* mod 4“. Мы причисляем два нечетных идеала $\mathfrak{a}$, $\mathfrak{b}$ к одному и тому же классу идеалов в узком смысле mod 4, если существует квадрат идеал $\mathfrak{c}^2$ такой, что $\mathfrak{a} \sim \mathfrak{b}\mathfrak{c}^2$ и можно выбрать вполне положительные числа α, β, удовлетворяющие условиям $\alpha\mathfrak{a} = \beta\mathfrak{b}\mathfrak{c}^2$, $\alpha \equiv \beta \equiv 1 \pmod 4$.

Порядок группы $\mathfrak{B}_0$ определяется аналогично порядку группы $\mathfrak{B}$. Пусть $\mathfrak{H}_0$ — подгруппа группы $\mathfrak{B}_0$, представимая нечетными главными идеалами. Тогда порядок факторгруппы $\mathfrak{B}_0/\mathfrak{H}_0$ снова равен 2^e. Порядок же группы $\mathfrak{H}_0$, в силу п. 11, оказывается равным $2^{n+r_1-(m+e-q_0)}$, ибо среди 2^{n+r_1} соединений классов вычетов в узком смысле mod 4 по 2^{m+e-q_0} соединений различаются между собой сингулярным числовым соединением. Поэтому

$$\text{порядок } \mathfrak{B}_0 \text{ равен } 2^{n+r_1-m+q_0} = 2^{m+q_0}.$$

§ 62. Существование сингулярных примарных чисел и дополнительные теоремы к закону взаимности

Теперь значения чисел q и q_0 определяются с помощью очень простого подсчета.

Лемма a). $q_0 \leqslant e$ *и* $q \leqslant e_0$.

В самом деле, пусть даны q_0 независимых вполне положительных сингулярных примарных чисел $\omega_1, \ldots, \omega_{q_0}$. Рассмотрим q_0 функций

$$\chi_i(\mathfrak{a}) = Q(\omega_i, \mathfrak{a}), \quad i = 1, \ldots, q_0,$$

нечетного идеала $\mathfrak{a}$. Они зависят лишь от соединения классов идеалов, к которому принадлежит $\mathfrak{a}$. Действительно, если $\mathfrak{a} \sim \mathfrak{b}\mathfrak{c}^2$ с нечетными $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ и α, β — нечетные числа, удовлетворяющие равенству $\alpha\mathfrak{a} = \beta\mathfrak{b}\mathfrak{c}^2$, то, предполагая, что ω_i взаимно просты с $\alpha\mathfrak{a}$, будем иметь

$$\chi_i(\alpha\mathfrak{a}) = \chi_i(\beta\mathfrak{b}\mathfrak{c}^2) = \left(\frac{\omega_i}{\alpha\mathfrak{a}}\right) = \left(\frac{\omega_i}{\beta\mathfrak{b}\mathfrak{c}^2}\right) = \left(\frac{\omega_i}{\beta\mathfrak{b}}\right).$$

Но для каждого целого числа γ, взаимно простого с $2\omega_i$, по закону взаимности имеем

$$\left(\frac{\omega_i}{\gamma}\right) = \left(\frac{\gamma}{\omega_i}\right),$$

ибо ω_i примарно и вполне положительно; последний же символ равен $+1$, так как ω_i сингулярно. Таким образом, действительно имеем

$$\chi_i(\mathfrak{a}) = \left(\frac{\omega_i}{\mathfrak{a}}\right) = \left(\frac{\omega_i}{\mathfrak{b}}\right) = \chi_i(\mathfrak{b}), \quad \text{если } \mathfrak{a} \sim \mathfrak{b}\mathfrak{c}^2.$$

Так как, далее, $\chi_i(\mathfrak{a}_1\mathfrak{a}_2) = \chi_i(\mathfrak{a}_1)\chi_i(\mathfrak{a}_2)$, то по § 10 q_0 функций $\chi_i(\mathfrak{a})$ представляют собой групповые характеры группы соединений классов идеалов. По теореме 169 эти характеры независимы. С другой стороны, по теореме 33 группа соединений классов идеалов, будучи порядка 2^e, имеет точно e независимых характеров. Следовательно, $q_0 \leqslant e$.

Аналогично, кладя в основу понятие эквивалентности в узком смысле, докажем неравенство $q \leqslant e_0$.

Лемма b). *Пусть* $\varepsilon_1, \ldots, \varepsilon_{m+e}$ *будут* $m + e$ *независимых сингулярных чисел. Тогда* $m + e$ *функций нечетного идеала* $\mathfrak{a}$

$$Q(\varepsilon_i, \mathfrak{a}) \quad (i = 1, \ldots, m+e)$$

образуют систему независимых групповых характеров группы $\mathfrak{B}_0$.

Что эти функции являются групповыми характерами для $\mathfrak{B}_0$, вытекает снова из теоремы 165. Что они независимы, показывает теорема 169.

Таким образом, в силу общих теоретико-групповых теорем § 10,

$$m + e \leqslant m + q_0,$$

ибо, в силу п. 13, $m + q_0$ есть порядок группы $\mathfrak{B}_0$. Следовательно, $q_0 \geqslant e$ и, значит, в силу леммы a), $q_0 = e$. Тем самым доказаны следующие две теоремы:

Теорема 170. *Существует точно e независимых вполне положительных сингулярных примарных чисел $\omega_1, \ldots, \omega_e$, где e — принадлежащее 2 базисное число группы классов идеалов поля в широком смысле e характеров $Q(\omega_i, \mathfrak{a})$ образуют полную систему характеров группы соединений классов.*

Теорема 171. *Для того чтобы нечетный идеал $\mathfrak{a}$ можно было дополнить путем умножения на квадрат идеала до вполне положительного и примарного числа поля, необходимо и достаточно, чтобы для каждого сингулярного числа ε выполнялось условие*

$$Q(\varepsilon, \mathfrak{a}) = +1.$$

Аналогичным образом, рассматривая вместо $\mathfrak{B}_0$ группу $\mathfrak{B}$, получаем следующий результат:

Лемма c). *Пусть $\varepsilon_1, \ldots, \varepsilon_p$ будут $p = e_0 + m - r_1$ независимых вполне положительных сингулярных чисел. Тогда p функций $Q(\varepsilon_i, \mathfrak{a})$ $(i = 1, \ldots, p)$ образуют при нечетном $\mathfrak{a}$ систему независимых групповых характеров группы $\mathfrak{B}$.*

Так как $\mathfrak{B}$ имеет порядок 2^{m-r_1+q}, то отсюда также получаем

$$m - r_1 + q \geqslant p = m - r_1 + e_0,$$

$$e_0 \leqslant q,$$

и, значит, в силу леммы a), $e_0 = q$, и $\mathfrak{B}$ имеет порядок 2^p. Тем самым доказаны:

Теорема 172. *Существует точно e_0 независимых примарных чисел, $\omega_1, \ldots, \omega_{e_0}$, где e_0 — принадлежащее 2 базисное число группы классов идеалов поля в узком смысле. e_0 характеров $Q(\omega_i, \mathfrak{a})$ образуют для нечетных $\mathfrak{a}$ полную систему характеров группы соединений классов в узком смысле.*

Теорема 173. *Для того чтобы нечетный идеал $\mathfrak{a}$ можно было дополнить путем умножения на квадрат идеала до примарного числа поля, необходимо и достаточно, чтобы для каждого вполне положительного сингулярного числа ε выполнялось условие*

$$Q(\varepsilon, \mathfrak{a}) = +1.$$

Теоремы 172 и 173 обычно объединяют названием *первой дополнительной теоремы.*

Аналогичным образом мы придем к обращению теоремы 167, относящейся к характерам вычетов по модулям, не являющимся нечетными. Мы назовем нечетное целое число α *гиперпримарным* по $\mathfrak{l}$, где $\mathfrak{l}$ — простой множитель числа 2, если сравнение $\alpha \equiv \xi^2 \pmod{4\mathfrak{l}}$ удовлетворяется числом ξ поля k. Таким образом гиперпримарные числа по $\mathfrak{l}$ определяют главное соединение классов вычетов $\bmod 4\mathfrak{l}$. По п. 9 предыдущего параграфа существует 2^{n+1} различных соединений $\bmod 4\mathfrak{l}$ и только 2^n различных соединений $\bmod 4$, следовательно, каждое со-

единение mod 4 содержит точно два различных соединения mod 4$\mathfrak{l}$. Таким образом примарные числа определяют точно два различных соединения классов вычетов mod 4$\mathfrak{l}$; обозначим их через R_1 и R_2, выбирая при этом в качестве R_1 главное соединение mod 4$\mathfrak{l}$.

Теорема 174. *Если простой идеал* $\mathfrak{l}$, *входящий множителем в* 2, *принадлежит главному соединению классов в узком смысле, то все* e_0 *независимых сингулярных примарных чисел также гиперпримарны по* $\mathfrak{l}$; *в противном же случае лишь* $e_0 - 1$ *независимых сингулярных примарных чисел также гиперпримарны по* $\mathfrak{l}$.

Доказательство. Пусть $\mathfrak{c}$ — такой нечетный идеал, что $\mathfrak{l}^2 = \lambda$ — вполне положительное число; в первом из указанных в теореме 174 случаев такой идеал существует. Тогда по теореме 167 для каждого нечетного числа α, сначала взаимно простого с $\mathfrak{l}\mathfrak{c}$, имеем

$$\left(\frac{\lambda}{\alpha}\right) = \left(\frac{\lambda}{\ }\right)\left(\frac{\alpha}{\mathfrak{l}^2}\right) = +1,$$

если α принадлежит соединению R_1. Рассматривая функцию $\left(\frac{\lambda}{\alpha}\right) = Q(\lambda, \alpha)$ лишь для примарных чисел α, мы видим, что $Q(\lambda, \alpha_1) = Q(\lambda, \alpha_2)$, если α_1 и α_2 принадлежат одному и тому же соединению R_1 или R_2, далее, $Q(\lambda, \alpha_1\alpha_2) = Q(\lambda, \alpha_1)\,Q(\lambda, \alpha_2)$, и, значит, $Q(\lambda, \alpha)$ является групповым характером группы второго порядка, образованной элементами R_1, R_2 ($R_2^2 = R_1$). Но этот характер не является главным, ибо по теореме 169 существует бесконечное множество простых идеалов $\mathfrak{p}$, для которых $\left(\frac{\lambda}{\mathfrak{p}}\right) = -1$, тогда как характеры $Q(\varepsilon, \mathfrak{p})$ для каждого из p независимых вполне положительных квадратов идеала ε равны $+1$.

По теореме 173 мы можем тогда дополнить $\mathfrak{p}$ путем умножения на подходящее выбранное $\mathfrak{m}^2$ до примарного числа, $\alpha = \mathfrak{p}\mathfrak{m}^2$, и получим $Q(\lambda, \alpha) = \left(\frac{\lambda}{\mathfrak{p}}\right) = -1$. Следовательно, $Q(\lambda, \alpha)$ является однозначно определенным групповым характером группы (R_1, R_2), отличным от главного характера, следовательно, $Q(\lambda, \alpha) = 1$ тогда и только тогда, когда примарное число α принадлежит R_1, т. е. когда α также гиперпримарно по $\mathfrak{l}$. Но для каждого сингулярного примарного числа ω имеем $Q(\lambda, \omega) = +1$, следовательно, нечетные сингулярные примарные числа также гиперпримарны по $\mathfrak{l}$.

Пусть теперь $\mathfrak{l}$ не принадлежит главному соединению классов в узком смысле. Выберем тогда нечетный идеал $\mathfrak{r}$ так, чтобы $\lambda = \mathfrak{l}\mathfrak{r}$ было вполне положительным числом. Так как также $\mathfrak{r}$ не принадлежит главному соединению классов в узком смысле, то по теореме 172 среди e_0 сингулярных примарных чисел имеется точно $e_0 - 1$ независимых, скажем, $\omega_2, \ldots, \omega_{e_0}$, для которых $Q(\omega_i, \mathfrak{r}) = +1$ ($i = 2, 3, \ldots, e_0$), и один не зависящий от них, ω_1, для которого $Q(\omega_1, \mathfrak{r}) = -1$. Это ω_1 тогда наверное не гиперпримарно по $\mathfrak{l}$, так как в противном случае мы имели бы по теореме 167

$$\left(\frac{\omega_1}{\mathfrak{r}}\right) = \left(\frac{\lambda}{\omega_1}\right)\left(\frac{\omega_1}{\mathfrak{r}}\right) = +1,$$

тогда как это произведение, в силу определения числа ω_1, равно -1. Таким образом ω_1 принадлежит соединению $R_2 \bmod 4\mathfrak{l}$. Поэтому каждое примарное число принадлежит соединению ω_1 или $\omega_1^2 \bmod 4\mathfrak{l}$. Но если нечетные числа α и β принадлежат одному и тому же соединению $\bmod 4\mathfrak{l}$, то, полагая $\chi(\alpha) = \left(\frac{\lambda}{\alpha}\right)\left(\frac{\alpha}{\mathfrak{r}}\right)$, имеем

$$\chi(\alpha)\chi(\beta) = \chi(\alpha\beta) = 1,$$

ибо $\alpha\beta$ гиперпримарно $\bmod \mathfrak{l}$, т. е.

$$\chi(\alpha) = \chi(\beta).$$

Следовательно, никакое из чисел $\omega_2, \ldots, \omega_{e_0}$ не может принадлежать представляемому числом ω_1 соединению R_2, ибо тогда было бы $\chi(\omega_2) = -1$, тогда как, по определению числа ω_2, $\chi(\omega_2) = +1$. Тем самым $\omega_2, \ldots, \omega_{e_0}$ гиперпримарны по $\mathfrak{l}$, а ω_1 — не гиперпримарно, и теорема 174 доказана.

Теорема 175. *Пусть* $\lambda = \mathfrak{l}\mathfrak{r}$ — *вполне положительное число,* $\mathfrak{r}$ — *нечетный идеал,* $\mathfrak{l}$ — *простой множитель числа* 2. *Для того чтобы примарное взаимно простое с* λ *целое число* α *было гиперпримарно по* $\mathfrak{l}$, *необходимо и достаточно, чтобы было*

$$\chi(\alpha) = \left(\frac{\lambda}{\alpha}\right)\left(\frac{\alpha}{\mathfrak{r}}\right) = +1.$$

Что это условие необходимо — утверждается теоремой 167. Достаточность его следующим образом получается из доказательства предыдущей теоремы. Пусть сначала $\mathfrak{l}$ эквивалентно в узком смысле квадрату идеала. Тогда можно найти такие целые числа β, ρ, λ, что β нечетно и взаимно просто с $\alpha\mathfrak{r}$, $\lambda\beta^2 = \lambda_0\rho$, $\lambda_0 = \mathfrak{l}\mathfrak{r}_1^2$, $\rho = \mathfrak{r}\mathfrak{r}_1^2$, λ_0, ρ вполне положительны. Тогда

$$\chi(\alpha) = \left(\frac{\lambda\beta^2}{\alpha}\right)\left(\frac{\alpha}{\mathfrak{r}}\right) = \left(\frac{\lambda_0\rho}{\alpha}\right)\left(\frac{\alpha}{\mathfrak{r}}\right) = \left(\frac{\lambda_0}{\alpha}\right)\left(\frac{\alpha}{\rho}\right)\left(\frac{\alpha}{\mathfrak{r}}\right) = \left(\frac{\lambda_0}{\alpha}\right),$$

и выполнение равенства $\left(\frac{\lambda_0}{\alpha}\right) = +1$, как было выше показано, является необходимым и достаточным условием того, чтобы примарное число α было также гиперпримарно.

Если теперь $\mathfrak{l}$ не принадлежит главному соединению классов в узком смысле, то существует такое сингулярное примарное число ω_1, для которого $\left(\frac{\omega_1}{\mathfrak{r}}\right) = -1$; числа 1, ω_1 представляют тогда два различных соединения классов вычетов $\bmod 4\mathfrak{l}$, возникающих из примарных чисел. Если α и ω_1^a ($a = 0$ или 1) принадлежат одному и тому же соединению $\bmod 4\mathfrak{l}$, то по теореме 166 $\chi(\alpha) = \chi(\omega_1^a) = (-1)^a$ и, следовательно, $\chi(\alpha) = +1$, если α гиперпримарно по $\mathfrak{l}$, и $= -1$ в противном случае.

Теорема 175 называется *второй дополнительной теоремой.*

§ 63. Одно свойство диференты поля. Гильбертово поле классов относительной степени 2

В заключение дадим два применения закона взаимности. Первое касается класса идеалов, к которому принадлежит диферента поля $\mathfrak{d}$.

ТЕОРЕМА 176. *Диферента $\mathfrak{d}$ поля k всегда эквивалентна квадрату некоторого идеала в k.*

Пусть ω — целое число поля k, делящееся на $\mathfrak{d}$, с разложением $\omega = \mathfrak{a}\mathfrak{d}$, $\mathfrak{a}$ нечетно. Тогда, в силу теоремы 170, для доказательства нашей теоремы нужно лишь показать, что для каждого сингулярного вполне положительного примарного числа ε, взаимно простого с $\mathfrak{a}$, $\left(\frac{\varepsilon}{\mathfrak{a}}\right) = +1$.

Для этой цели мы используем формулу (199) для сумм Гаусса и теорему 156, определяющую значение сумм Гаусса, принадлежащих знаменателю, который является квадратом нечетного идеала. Разложим сумму $C\left(\frac{\varepsilon}{4\omega}\right)$, принадлежащую знаменателю $4\mathfrak{a}$, где $(\varepsilon, \mathfrak{a}) = 1$, по формуле (169) в произведение суммы со знаменателем 4 на сумму со знаменателем $\mathfrak{a}$. Вводя для этого нечетный идеал $\mathfrak{c}$ такой, что $\mathfrak{a}\mathfrak{c} =$ числу α, $\gamma = \frac{\alpha}{\omega} = \frac{\mathfrak{c}}{\mathfrak{d}}$, имеем по (169)

$$C\left(\frac{\varepsilon}{4\omega}\right) = C\left(\frac{\varepsilon\gamma}{4\alpha}\right) = C\left(\frac{4\varepsilon\gamma}{\alpha}\right) C\left(\frac{\alpha\varepsilon\gamma}{4}\right),$$

и если ε примарно, то правая часть равна $\left(\frac{\varepsilon}{\mathfrak{a}}\right) C\left(\frac{\gamma}{\alpha}\right) C\left(\frac{\alpha\gamma}{4}\right)$.

В частности, для $\varepsilon = 1$ получаем $C\left(\frac{1}{4\omega}\right) = C\left(\frac{\gamma}{\alpha}\right) C\left(\frac{\alpha\gamma}{4}\right)$, откуда

$$\left(\frac{\varepsilon}{\mathfrak{a}}\right) = \frac{C\left(\frac{\varepsilon}{4\omega}\right)}{C\left(\frac{1}{4\omega}\right)}. \tag{215}$$

Применяя теперь к последним суммам соотношение взаимности (199), мы преобразуем их в суммы со знаменателем ε, значения которых сможем непосредственно определить по теореме 156. Имеем

$$\frac{C\left(\frac{\varepsilon}{4\omega}\right)}{|\sqrt{N(4\mathfrak{a})}|} = \left|\sqrt{N\left(\frac{2}{\varepsilon}\right)}\right| e^{\frac{\pi i}{4} S(\operatorname{sgn}\omega\varepsilon)} C\left(\frac{-\gamma^2\omega}{\varepsilon}\right).$$

Точно так же

$$\frac{C\left(\frac{1}{4\omega}\right)}{|\sqrt{N(4\mathfrak{a})}|} = |\sqrt{N(2)}|\, e^{\frac{\pi i}{4} S(\operatorname{sgn}\omega)}.$$

Поэтому из (215) получаем равенство

$$\left(\frac{\varepsilon}{\mathfrak{a}}\right) = e^{\frac{\pi i}{4} S(\operatorname{sgn}\omega\varepsilon - \operatorname{sgn}\omega)} \frac{C\left(\frac{-\gamma^2\omega}{\varepsilon}\right)}{|\sqrt{N(\varepsilon)}|},$$

справедливое для всех примарных чисел ε, взаимно простых с $\mathfrak{a}$. Предполагая теперь, что ε, кроме того, сингулярно, мы получаем по теореме 156 для суммы $C\left(\frac{-\gamma^2\omega}{\varepsilon}\right)$ значение $|\sqrt{N(\varepsilon)}|$ и, следовательно,

$$\left(\frac{\varepsilon}{\mathfrak{a}}\right) = i^{\frac{\pi i}{4} S(\operatorname{sgn}\omega\varepsilon - \operatorname{sgn}\omega)}, \quad \text{если } \omega = \mathfrak{a}\mathfrak{d},\ \mathfrak{a} \text{ нечетно.}$$

Наконец, если ε, сверх того, еще вполне положительно, то получаем $\left(\frac{\varepsilon}{\mathfrak{a}}\right) = +1$, а отсюда, в силу теоремы 170, заключаем, что $\mathfrak{a}$, а значит, и диферента $\mathfrak{d}$, принадлежит главному соединению классов.

Так как диференты относительных полей связаны соотношением (75) теоремы 111, то из только что доказанного вытекает также следующий результат:

Относительная диферента $\mathfrak{D}_k$ поля K относительно под-поля k всегда эквивалентна квадрату идеала в K.

Так как, далее, относительная норма относительной диференты $\mathfrak{D}_k$ равна дискриминанту K относительно k, то получаем, что этот последний и в k эквивалентен квадрату. Тем самым доказана

Теорема 177. *Если идеал $\mathfrak{d}_k$ в k является дискриминантом некоторого поля относительно k, то $\mathfrak{d}_k$ эквивалентен квадрату идеала в k.*

В качестве второго применения закона взаимности исследуем гильбертово поле классов поля k относительной степени 2. Будем вместе с Гильбертом называть поле *неразветвленным* относительно k, если его относительный дискриминант равен 1. Неразветвленные поля, порождаемые присоединением к k квадратного корня числа из k, можно указать: в силу теоремы 120, такие поля получаются путем присоединения к k квадратного корня из сингулярного примарного числа поля k. Но число различных соединений сингулярных примарных чисел поля k по теореме 172 равно $2^{e_0} - 1$ (квадраты не причисляются к сингулярным примарным числам). Следовательно, имеет место

Теорема 178. *Существует точно $2^{e_0} - 1$ различных неразветвленных относительно k полей относительной степени 2.*

Тем самым эти поля находятся в связи с классами идеалов в k. Если число классов в узком смысле в k нечетно, то вообще не существует неразветвленных полей относительной степени 2.

Связь с классами идеалов еще отчетливее выступает в формулировке законов разложения.

Теорема 179. *Пусть ω — сингулярное примарное число. Тогда в группе h_0 классов идеалов в узком смысле существует такая подгруппа $\mathfrak{G}(\omega)$ порядка $\frac{h_0}{2}$, что простой идеал $\mathfrak{p}$ тогда и только тогда разлагается в поле $K(\sqrt{\omega}, k)$, когда он принадлежит к $\mathfrak{G}(\omega)$.*

В самом деле, совокупность нечетных идеалов $\mathfrak{r}$, для которых $Q(\omega, \mathfrak{r}) = +1$, по теореме 172 определяет в группе соединений классов в узком смысле подгруппу порядка 2^{e_0-1}. Так как каждое соединение классов состоит из $\frac{h_0}{2^{e_0}}$ классов в узком смысле, то нечетные идеалы $\mathfrak{r}$ с $Q(\omega, \mathfrak{r}) = +1$ совпадают с нечетными идеалами, лежащими в $\frac{h_0}{2}$ классах в узком смысле этой группы $\mathfrak{H}(\omega)$.

Но то же имеет место и для простых идеалов $\mathfrak{l}$, входящих в 2. Действительно, в силу теоремы 119, определенный в § 60 символ $Q(\omega, \mathfrak{l})$ равен $+1$, если нечетное число ω сравнимо с квадратом числа из $k \bmod \mathfrak{l}^{2e+1}$, где $\mathfrak{l}^e$ — наибольшая степень $\mathfrak{l}$, входящая в 2, и равен -1 для нечетных ω в противном случае. Но ω примарно и $\mathfrak{l}^{2e-1}$ взаимно просто с $\frac{4}{\mathfrak{l}^{2e}}$, следовательно, $Q(\omega, \mathfrak{l})$ тогда и только тогда равно $+1$, когда ω есть квадратичный вычет $\bmod 4\mathfrak{l}$. По теореме же 175 это действительно зависит лишь от класса идеалов, которому принадлежит $\mathfrak{l}$. Именно, если $\lambda = \mathfrak{l}\mathfrak{r}$ вполне положительно и $\mathfrak{r}$ нечетно, то ω тогда и только тогда гиперпримарно по $\mathfrak{l}$, когда $\left(\frac{\omega}{\mathfrak{r}}\right) = +1$.

Вследствие этой тесной связи с классами идеалов поле $K(\sqrt{\omega}, k)$ и называют *полем классов* поля k.

При принятом вами способе обоснования теории относительно квадратичных полей, закон взаимности выступает как нечто первичное, а существование поля классов — как следствие из него. При классических обоснованиях Гильберта и Фуртвенглера (с исследованием также высших степенных вычетов) ход идей как раз обратен нашему. Сперва доказывается существование поля классов другим, притом очень сложным, путем, затем исследуется связь его с классами идеалов, и отсюда уже выводится закон взаимности. При этом необходимым вспомогательным средством, без которого до сих пор на этом пути не удалось обойтись, является закон взаимности *Эйзенштейна*. Этим путем приходится итти во всех тех случаях, когда речь идет о поле относительной степени, большей чем 2. До сих пор не открыты такие трансцендентные функции, которые бы, подобно тэта-функциям нашей теории, доставляли соотношение взаимности между суммами, появляющимися для высших степенных вычетов вместо сумм Гаусса. Новый родственный гильбертовому и очень плодотворный подход предложен Takagi [1]), которому с его помощью удалось также получить полный обзор всех относительно-абелевых полей, т. е. полей, находящихся в таком же отношении к k, в каком поле деления круга стоит к $k(1)$.

---

[1]) Über eine Theorie des relativ-Abelschen Zahlkörpers, Journal of the College of Science, Imperial University of Tokyo, Vol. XLI (1920).

ОПЕЧАТКИ

Страница	Строка	Напечатано	Должно быть	По чьей вине
155	13 сверху	точка	тогда	корр.
225	1 снизу	$(m_i + _i)^2$	$(m_i + u_i)^2$	тип.

Зак. 1386 Гекке. Теория алгебр. чисел