Н. Г. ЧЕБОТАРЕВ

ОСНОВЫ ТЕОРИИ ГАЛУА

Часть вторая

ГЛАВНАЯ РЕДАКЦИЯ ТЕХНИКО-ТЕОРЕТИЧЕСКОЙ ЛИТЕРАТУРЫ
ЛЕНИНГРАД 1937 МОСКВА

МАТЕМАТИКА В МОНОГРАФИЯХ

ПОД РЕДАКЦИЕЙ
акад. С. Н. БЕРНШТЕЙНА, акад. И. М. ВИНОГРАДОВА,
проф. А. Н. КОЛМОГОРОВА, проф. Л. А. ЛЮСТЕРНИКА,
проф. А. И. ПЛЕСНЕРА, проф. В. А. ТАРТАКОВСКОГО,
проф. Н. Г. ЧЕБОТАРЕВА

ОСНОВНАЯ СЕРИЯ

КНИГА 5

Н. Г. ЧЕБОТАРЕВ

ОСНОВЫ ТЕОРИИ ГАЛУА

Часть вторая

3 р., переплет 1 р. 50 к.

ОБЪЕДИНЕННОЕ
НАУЧНО-ТЕХНИЧЕСКОЕ ИЗДАТЕЛЬСТВО НКТП СССР

Т—23—5—4
Тк к № 111 от 19/VIII 1937 г.

Настоящая книга является продолжением части I „Основы теории Галуа", изданной ОНТИ в 1935 г., и посвящена исследованию свойств алгебраических чисел в связи с теорией Галуа. Она предназначена для научных работников и аспирантов-специалистов.

ПРЕДИСЛОВИЕ

Настоящая вторая часть „Основ теории Галуа" должна была по замыслу содержать все главнейшие современные результаты, посвященные приложениям теории Галуа к алгебраическим числам, и поэтому должна была содержать теорию абелевых полей, в частности полей классов, а также теорию алгебр (или гиперкомплексных чисел) в приложении к полям классов. Однако оказалось, что методическая обработка имеющегося по этим вопросам журнальноro материала потребует много времени и повлечет за собой дальнейшую задержку выхода в свет этой части книги. В виду этого я решил опубликовать в виде отдельной книги эту часть, содержащую элементы теории алгебраических чисел и идеалов, но пронизанную связью с теорией Галуа, а также элементы аналитической теории идеалов, доведенные до определения плотности простых чисел, принадлежащих к отдельным классам подстановок (автоморфизмов поля).

Выход в свет теории алгебраических чисел отдельной книгой может быть оправдан особенно потому, что книг на русском языке по теории чисел почти нет. Существуют лишь: литографированный курс Д. А. Граве, Арифметическая теория алгебраических величин, ч. I — Квадратичная область, Вельмин, Теория алгебраических чисел, являющаяся почти библиографической редкостью, и недавно вышедший на украинском языке перевод книги Гекке (E. Hecke, Vorlesungen über die Theorie der algebraischen Zahlen).

Однако и во всей мировой литературе трудно указать книгу, которая по материалу была бы близка к этой книге. Почти все выходящие теперь книги по теории алгебраических чисел избегают ставить ее в связь с теорией групп и теорией Галуа; книга Гекке ограничивается случаем абелевых групп. Ближе всего материал настоящей книги лежит к материалу второго тома „Учебника алгебры" Вебера (H. Weber), но содержит много упрощений, выработанных после 1899 г., когда вышла книга Вебера (например несравненно проще доказана теорема Кронекера-Вебера; геометрическая теорема Минковского заменена простой алгебраической теоремой Гурвица), а также более поздние результаты, например о плотностях простых чисел (Фробениус), каковые у Вебера изложены только для случая абелевых полей (теорема Дирихле о простых числах в арифметической прогрессии).

Книга состоит из двух глав. Первая посвящена элементарной теории идеалов. Обычно все курсы теории идеалов принимают за основу или Кронекеровскую теорию функционалов (Вебер) или Дедекиндову теорию модулей (Дирихле-Дедекинд, Бахман, Ландау, Гекке); я выбрал теорию Золотарева, которая быстрее вводит читателя в курс дела и отличается большей наглядностью. В дальнейшем я доказал эквивалентность определений Золотарева и Дедекинда.

В § 5-я привожу новое доказательство теоремы Дедекинда о критических простых числах. Это простое по идее доказательство пользуется аппаратом теории Галуа, в частности теоремой Силова из теории групп.

В §§ 6—7 доказывается теорема Минковского при помощи леммы Гурвица, доказательство которой проводится более подробно, чем у самого Гурвица.

В § 8 вводится понятие группы инерции, при помощи которого из теоремы Минковского легко выводится так называемая теорема монодромии, с помощью которой многие формулировки и выводы значительно упрощаются.

В § 9 доказана теорема Кронекера-Вебера об абелевых полях и полях деления круга. В общем доказательство построено по Гильберту. Для наиболее трудного случая иррегулярных критических чисел доказательство заменено новым, идея которого принадлежит Фуэтеру (R. Fueter).

§§ 10—12 посвящены группе разложения с приложением к выводу теоремы Штикельбергера-Вороного, а также к выводу квадратичного закона взаимности по Мириманову и Гензелю (K. Hensel).

Глава вторая, посвященная аналитической теории идеалов, имеет целью получение результатов аналитической теории, которые имеют важные приложения в общей теории идеалов. Руководствуясь этим принципом выбора, я избегал помещения результатов, касающихся тонкостей оценки остаточных членов, и не поместил весьма важной формулы Гекке, как не имеющей непосредственного приложения к излагаемым вопросам приложения теории Галуа к алгебраическим числам.

В § 1 доказывается конечность числа идеальных классов и излагается связь эквивалентности идеалов с подобием соответствующих матриц (см. Шур).

§ 2 посвящен теории единиц алгебраического поля, изложенной по ван-дер-Вардену (B. L. van der Waerden). Здесь в виде примера изложена связь единиц вещественного квадратичного поля с непрерывными дробями.

В § 3 изложена теория Дирихле о простых числах в арифметической прогрессии. Вместо доказательства необращения в нуль выражений h (1) я, руководствуясь примером Вебера, отсылаю читателей к следующему параграфу, в котором тот же результат получается при помощи рассмотрения высших полей деления круга.

§ 4 посвящен рассмотрению Дедекиндовой ζ-функции и содержит доказательство результата Кронекера о существовании бесчисленного множества простых идеалов первой степени.

В § 5 выводится результат Фробениуса относительно простых чисел, принадлежащих к отделам подстановок группы Галуа поля.

В § 6 результат Фробениуса обобщается на классы подстановок. Изложение значительно отличается от изложения первоначальной журнальной статьи. Внесены упрощения, предложенные М. Ф. Кравчуком и Шрейером (O. Schreier).

Характер изложения второй части отличается от такового в первой большей сжатостью, неизбежно связанной с обилием материала и с тем, что вторая часть предназначена для более высокого уровня читателей, главным образом для специалистов по алгебре и теории чисел и для аспирантов, пишущих диссертации в этой области.

Н. Чеботарев.

ВВЕДЕНИЕ

Как мы видели в первой части, теория Галуа дает возможность привести изучение ряда свойств полей алгебраических чисел, в первую очередь перечисление всевозможных делителей этих полей, к изучению структуры групп этих полей, состоящих из конечного числа элементов. Но, как известно, структура группы Галуа не определяет всех его свойств: имеется немалое число арифметических свойств этих полей, не определяемых вполне их группами, но тем не менее стоящих в тесной связи с последними. Я позволю себе привести в виде примера такой связи замечательную теорему, впервые высказанную Кронекером (Kronecker) и доказанную Вебером (H. Weber):

> Всякое поле, группа Галуа которого абелева (будет говорить: *абелево поле*), если область рациональности есть поле рациональных чисел, является *полем деления* круга, т. е. его величины рационально выражаются через некоторые корни из единиц).

Эта часть „Основ теории Галуа" как раз имеет в виду изложить эту связь. Для этого необходимо глубокое знакомство с арифметикой алгебраических полей, каковой и посвящается главным образом настоящая книга.

Глава I

ЭЛЕМЕНТАРНАЯ ТЕОРИЯ ИДЕАЛОВ

§ 1. Целые алгебраические числа

1. *Целым алгебраическим* числом называется число, удовлетворяющее неприводимому уравнению с целыми рациональными коэфициентами, причем коэфициент при старшем члене равен единице.

2. Докажем, что число, являющееся корнем какого бы то ни было уравнения с целыми рациональными коэфициентами и единицей при старшем члене, есть целое алгебраическое число, т. е. что то неприводимое уравнение, корнем которого является это число, будет того же типа. Для этого достаточно доказать следующую теорему Гаусса:

> **Теорема 1.** Если полином $a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n$ с целыми рациональными коэфициентами разлагается на два множителя с рациональными коэфициентами: $a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + x^n = (b_0 + b_1 x + \ldots + b_{u-1} x^{u-1} + x^u)(c_0 + c_1 x + \ldots + c_{v-1} x^{v-1} + x^v)$; $(u + v = n)$, то коэфициенты b_i, c_j этих множителей суть тоже целые рациональные числа.

Доказательство. Допустим противное: пусть коэфициенты, представленные в виде несократимых дробей, содержат в знаменателях простой множитель p самое большее в s-ой степени $(s > 0)$, и пусть b_k будет первый из этих коэфициентов, содержащих в знаменателях точно p^s. Пусть также коэфициенты c_j содержат в своих знаменателях p самое большее в t-ой степени $(t \geqq 0)$ и пусть c_r будет первый из этих коэфициентов, содержащих в своих знаменателях точно p^t. Рассмотрим коэфициент a_{k+r}:

$$a_{k+r} = b_k c_r + b_{k+1} c_{r-1} + \ldots + b_{k-1} c_{r+1} + \ldots$$

В этом выражении слагаемое $b_k c_r$ будет содержать в знаменателе точно p^{s+t}, в то время как остальные слагаемые должны содержать в знаменателях меньшие, чем $(s+t)$-ая степени. В самом деле, слагаемые первой строки суть произведения чисел b_{k+i}, содержащих в знаменателях p в степенях $\leqq s$,

и чисел c_{r-t}, содержащих в знаменателях p в степенях $<t$ (в случае $t=0$ мы должны полагать $r=0$, так что этих слагаемых вовсе не будет). Слагаемые же второй строки суть произведения чисел b_{k-s}, содержащих в знаменателях p в степенях $<s$, и чисел c_{r+s}, содержащих в знаменателях p в степенях $\leqq t$. Таким образом, дробная часть слагаемого $b_k c_r$ не может быть уничтожена прибавлением остальных слагаемых, и сумма a_{k+r} должна быть равна дробному числу, что противоречит условию. Таким образом, коэфициенты b_i, c_j должны быть целыми числами, что и требовалось доказать.

Следствие. Рациональное целое алгебраическое число есть целое рациональное число.

3. Имеет место

Теорема 2. Сумма и произведение двух или нескольких целых алгебраических чисел есть целое алгебраическое число.

Доказательство. Докажем более общую теорему: если α, β — целые алгебраические числа, удовлетворяющие соответственно уравнениям

$$x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m = 0 \qquad (1.1)$$

$$y^n + b_1 y^{n-1} + \ldots + b_{n-1} y + b_n = 0 \qquad (1.2)$$

с целыми рациональными коэфициентами, то $\varphi(\alpha, \beta)$, где $\varphi(x, y)$ есть произвольный целочисленный полином, есть целое алгебраическое число. Очевидно, что теорема легко распространяется на случай большего числа целых алгебраических чисел.

Пусть $\alpha_1, \alpha_2, \ldots, \alpha_m$ и $\beta_1, \beta_2, \ldots, \beta_n$ будут полные системы корней соответственно уравнений (1.1) и (1.2). Из свойств этих уравнений следует, что элементарно-симметрические функции от этих систем суть целые алгебраические числа. Но $\varphi(\alpha, \beta)$ является корнем уравнения

$$F(u) = \prod_{i=1}^{m} \prod_{j=1}^{n} \{u - \varphi(\alpha_i, \beta_j)\} = 0. \qquad (1.3)$$

Вместе с тем в части I, стр. 63,3° мы убедились, что всякий целочисленный симметрический полином от корней выражается целочисленным полиномом от их элементарно-симметрических функций. Поэтому все коэфициенты при различных степенях u полинома $F(u)$ являются целыми рациональными числами, а коэфициент при u^{mn} равен единице. Из теоремы 1 следует, что $\varphi(\alpha, \beta)$ есть целое алгебраическое число, ч. и т. д.

4. Отметим еще одну теорему:

Теорема 3. Если ω есть корень уравнения $f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0$, коэфициенты которого суть целые алгебраические числа, то ω есть целое алгебраическое число.

Доказательство. Будем называть сопряженным с $f(x)$ полиномом такой полином $f^{(k)}(x)$, в котором хотя бы один коэфициент полинома $f(x)$ заменен сопряженной с ним величиной, т. е. другим корнем того неприводимого уравнения с рациональными коэфициентами, которому удовлетворяет этот полином. Тогда произведение

$$\Phi(x) = \prod_k f^{(k)}(x)$$

является полиномом с рациональными коэфициентами. Рассуждая так же, как при доказательстве теоремы 2, мы убедимся, что они должны быть целыми числами. Так как старший коэфициент в $\Phi(x)$ есть единица, то величина ω, являющаяся корнем уравнения $\Phi(x) = 0$, есть в силу теоремы 1 целое алгебраическое число, ч. и т. д.

5. Из теоремы 2 следует, что совокупность целых (алгебраических) чисел рассматриваемого поля воспроизводится при сложении, вычитании и умножении, т. е. что сумма, разность и произведение двух чисел этой совокупности тоже принадлежат к совокупности. Такого рода совокупности называются *кольцами*. В дальнейшем мы познакомимся с другими примерами колец.

6. Пусть величина α удовлетворяет неприводимому уравнению

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0.$$

Все корни $\alpha_1, \alpha_2, \ldots, \alpha_n$ этого уравнения образуют систему *сопряженных с* α величин. Среди их элементарно-симметрических функций особо важное значение имеют две, для которых введены специальные наименования и обозначения. *Следом* величины α называется сумма

$$S(\alpha) = \alpha_1 + \alpha_2 + \ldots + \alpha_n. \qquad (1.4)$$

Нормой величины α называется произведение

$$N(\alpha) = \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_n. \qquad (1.5)$$

Рассмотрим поле $K(\alpha)$, образованное рациональными функциями с рациональными коэфициентами от α. Известно (см. часть 1, стр. 73, теорема 46, и стр. 74, теорема 48), что полином

$$g(t) = [t - R(\alpha_1)][t - R(\alpha_2)] \ldots [t - R(\alpha_n)],$$

где $R(\alpha)$ — произвольная рациональная функция от α — есть степень неприводимого полинома от t, которая просто равна неприводимому полиному в том и только в том случае, если $\Theta = R(\alpha)$ есть *примитивная величина* поля, т. е. если α, а с нею любая величина поля $K(\alpha)$, рационально выражается через Θ. Если мы теперь условимся под следом и нормой величины $\Theta = R(\alpha)$ внутри $K(\alpha)$ разуметь соответственно величины

$$S[R(\alpha)] = R(\alpha_1) + R(\alpha_2) + \ldots + R(\alpha_n)$$
$$N[R(\alpha)] = R(\alpha_1) \cdot R(\alpha_2) \cdot \ldots \cdot R(\alpha_n)$$

(так что, например, для рациональной величины a мы имеем $S(a)=n\cdot a$, $N(a)=a^n$), то имеют место следующие формулы

$$S(\alpha+\beta)=S(\alpha)+S(\beta) \tag{1.6}$$
$$N(\alpha\cdot\beta)=N(\alpha)\cdot N(\beta). \tag{1.7}$$

7. В заключение отметим одну полезную для дальнейшего формулу. Пусть примитивная величина α поля удовлетворяет неприводимому уравнению $f(x)=0$. Имеет место тождество

$$f(t)=(t-\alpha_1)(t-\alpha_2)\dots(t-\alpha_n)=N(t-\alpha), \tag{1.8}$$

где t — произвольная (переменная) величина, которой можно придавать любые численные значения, если мы только условимся, что при переходе к сопряженным величинам в выражении $t-\alpha$ значение t будет оставаться неизменным.

§ 2. Базис и дискриминант поля

1. В части 1 (стр. 74, теорема 49) мы убедились, что всякую величину поля можно, и притом однозначно, представить в форме

$$c_0+c\alpha+\dots+c_{n-1}\alpha^{n-1}, \tag{2.1}$$

где $c_0, c_1, \dots, c_{n-1}$ — рациональные числа. Будем называть систему чисел $[\omega_0, \omega_1, \dots, \omega_{n-1}]$ *базисом поля*, если всякая величина поля может быть представлена в форме

$$c_0\omega_0+c_1\omega_1+\dots+c_{n-1}\omega_{n-1} \tag{2.2}$$

с рациональными *координатами* $c_0, c_1, \dots, c_{n-1}$. Базис типа $[1, \alpha, \alpha^2, \dots, \alpha^{n-1}]$ будем называть *степенным базисом поля*.

2. Чтобы узнать, является ли заданная система чисел $[\omega_0, \omega_1, \dots, \omega_{n-1}]$ базисом нашего поля, будем исходить из некоторого степенного базиса $[1, \alpha, \dots, \alpha^{n-1}]$, где α — любая примитивная величина поля. Выразим элементы заданной системы при помощи степенного базиса:

$$\left.\begin{aligned}
\omega_0&=c_{00}+c_{01}\alpha+\dots+c_{0,n-1}\alpha^{n-1},\\
\omega_1&=c_{10}+c_{11}\alpha+\dots+c_{1,n-1}\alpha^{n-1},\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
\omega_{n-1}&=c_{n-1,0}+c_{n-1,1}\alpha+\dots+c_{n-1,n-1}\alpha^{n-1}.
\end{aligned}\right\} \tag{2.3}$$

Этот переход мы будем также записывать так:

$$[\omega_0, \omega_1, \dots, \omega_{n-1}]=\begin{pmatrix} c_{0,0}, & \dots, & c_{0,n-1}\\ \dots\dots & \dots\dots & \dots\dots\\ c_{n-1,0}, & \dots, & c_{n-1,n-1}\end{pmatrix}[1, \alpha, \dots, \alpha^{n-1}]. \tag{2.3'}$$

Теорема 4. Система $[\omega_0, \omega_1, \dots, \omega_{n-1}]$ является базисом поля тогда и только тогда, если определитель $|c_{ik}|$ отличен от нуля.

Доказательство. 1. Условие достаточно. В самом деле, если $|c_{ik}|\neq 0$, то систему равенств можно разрешить относительно $1, \alpha, \dots, \alpha^{n-1}$, и тогда каждая из этих величин будет линейно (с рациональными коэфициентами) выражаться через $\omega_0, \omega_1, \dots, \omega_{n-1}$. В таком же виде сможет быть выражена и каждая их линейная комбинация (2.1), т. е. каждая величина нашего поля.

2. Условие необходимо. В самом деле, если $|c_{ik}|=0$, то из равенств (2.3) следует, что величины $\omega_0, \omega_1, \dots, \omega_{n-1}$ связаны зависимостью

$$b_0\omega_0+b_1\omega_1+\dots+b_{n-1}\omega_{n-1}=0 \tag{2.4}$$

с рациональными коэфициентами, из которых хотя бы один, например b_{n-1}, не равен нулю. Предположим, что $[\omega_0, \omega_1, \dots, \omega_{n-1}]$ есть базис. Тогда каждая из величин $1, \alpha, \dots, \alpha^{n-1}$ линейно выразится через $\omega_0, \omega_1, \dots, \omega_{n-1}$. В этих выражениях мы при помощи (2.4) можем в силу $b_{n-1}\neq 0$ освободиться от величины ω_{n-1}. Исключая из этих выражений $\omega_0, \omega_1, \dots, \omega_{n-2}$ мы получим по крайней мере одну линейную зависимость между $1, \alpha, \dots, \alpha^{n-1}$ с рациональными коэфициентами. Это, однако, противоречит неприводимости полинома n-ой степени, корнем которого является α.

Из приведенного рассуждения вытекает также следующий критерий для базиса:

Теорема 5. Для того чтобы система n чисел $[\omega_0, \omega_1, \dots, \omega_{n-1}]$ была базисом поля n-ой степени, необходимо и достаточно, чтобы между $\omega_0, \omega_1, \dots, \omega_{n-1}$ не имела места зависимость типа (2.4).

3. Чтобы получить критерий базиса, независимый от степенных базисов и эффективный, т. е. могущий быть примененным к примерам, введем понятие *дискриминанта* системы чисел $\omega_0, \omega_1, \dots, \omega_{n-1}$. Обозначая числа, сопряженные с α, так: $\alpha, \alpha', \dots, \alpha^{(n-1)}$ [причем, если $\Theta=R(\alpha)$, то $R(\alpha^{(i)})$ мы будем обозначать через $\Theta^{(i)}$], рассмотрим определитель

$$\begin{vmatrix} \omega_0, & \omega_1, & \dots, & \omega_{n-1}\\ \omega_0', & \omega_1', & \dots, & \omega_{n-1}'\\ \dots\dots & \dots\dots & \dots\dots & \dots\dots\\ \omega_0^{(n-1)}, & \omega_1^{(n-1)}, & \dots, & \omega_{n-1}^{(n-1)}\end{vmatrix}. \tag{2.5}$$

Его квадрат мы и будем называть *дискриминантом системы* $[\omega_0, \omega_1, \dots, \omega_{n-1}]$. Помножив этот определитель сам на себя

(по колоннам), мы получим для дискриминанта следующее выражение:

$$\Delta[\omega_0, \omega_1, \ldots, \omega_{n-1}] = \begin{vmatrix} S(\omega_0\omega_0), & S(\omega_0\omega_1), & \ldots, & S(\omega_0\omega_{n-1}) \\ S(\omega_1\omega_0), & S(\omega_1\omega_1), & \ldots, & S(\omega_1\omega_{n-1}) \\ \ldots & \ldots & \ldots & \ldots \\ S(\omega_{n-1}\omega_0), & S(\omega_{n-1}\omega_1), & \ldots, & S(\omega_{n-1}\omega_{n-1}) \end{vmatrix}, \quad (2.6)$$

показывающее, что дискриминанты равны рациональным числам.

Нетрудно убедиться, что дискриминант степенного базиса $[1, \alpha, \alpha^2, \ldots, \alpha^{n-1}]$ равен дискриминанту уравнения, корнем которого является α.

4. Даны базис $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ и система чисел $[\eta_0, \eta_1, \ldots, \eta_{n-1}]$, выражаемых через базис так:

$$[\eta_0, \eta_1, \ldots, \eta_{n-1}] = \begin{pmatrix} c_{00}, & \ldots, & c_{0,n-1} \\ \ldots & \ldots & \ldots \\ c_{n-1,0}, & \ldots, & c_{n-1,n-1} \end{pmatrix} [\omega_0, \omega_1, \ldots, \omega_{n-1}].$$

Составляя для обеих систем определители (2.5), мы на основании теоремы об умножении определителей будем иметь:

$$\begin{vmatrix} 1, & \eta_0, & \ldots, & \eta_{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ \eta_0^{(n-1)}, & \ldots, & \eta_{n-1}^{(n-1)} \end{vmatrix} =$$

$$= \begin{vmatrix} c_{00}, & \ldots, & c_{0,n-1} \\ \ldots & \ldots & \ldots \\ c_{n-1,0}, & \ldots, & c_{n-1,n-1} \end{vmatrix} \cdot \begin{vmatrix} \omega_0, & \ldots, & \omega_{n-1} \\ \ldots & \ldots & \ldots \\ \omega_0^{(n-1)}, & \ldots, & \omega_{n-1}^{(n-1)} \end{vmatrix}.$$

Возводя эту формулу в квадрат, мы приходим к следующей важной формуле:

$$\Delta[\eta_0, \eta_1, \ldots, \eta_{n-1}] = \begin{vmatrix} c_{00}, & \ldots, & c_{0,n-1} \\ \ldots & \ldots & \ldots \\ c_{n-1,0}, & \ldots, & c_{n-1,n-1} \end{vmatrix}^2 \cdot \Delta[\omega_0, \omega_1, \ldots, \omega_{n-1}]. \quad (2.7)$$

Беря в качестве $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ степенной базис $[1, \alpha, \ldots, \alpha^{n-1}]$ и принимая во внимание, что дискриминанты неприводимых уравнений, как не имеющих кратных корней, отличны от нуля, а также теорему 4, мы приходим к

Теореме 6. Система $[\eta_0, \eta_1, \ldots, \eta_{n-1}]$ является базисом тогда и только тогда, если ее дискриминант отличен от нуля.

5. Если элементы базиса $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ являются целыми алгебраическими числами, то в силу теоремы 2 все числа вида $c_0\omega_0 + c_1\omega_1 + \ldots + c_{n-1}\omega_{n-1}$, где $c_0, c_1, \ldots, c_{n-1}$ — целые рациональные числа, суть целые алгебраические числа. Возникает вопрос, все ли целые алгебраические числа нашего поля мы

получим, если заставим числа $c_0, c_1, \ldots, c_{n-1}$ пробегать всевозможные целые рациональные значения. Оказывается, что это имеет место не для всех базисов поля, но что для всякого поля можно найти базис, который бы обладал этим свойством. Такого рода базис носит название *фундаментального* (или *минимального*) *базиса* поля.

Докажем существование фундаментального базиса. Рассмотрим произвольный базис $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ (например степенной), составленный из целых чисел поля. Если он не является фундаментальным, то найдется целое алгебраическое число η, выражающееся через этот базис с дробными координатами:

$$\eta = c_0\omega_0 + c_1\omega_1 + \ldots + c_{n-1}\omega_{n-1}.$$

Пусть $c_i = \frac{r}{s}$ есть дробное число, причем r и s суть взаимно простые целые рациональные числа. Решая неопределенное уравнение

$$rx + sy = 1,$$

выразим через базис $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ целое число $\eta' = \eta x + \omega_i y$:

$$\eta' = \eta x + \omega_i y = c_0 x \cdot \omega_0 + \ldots$$
$$\ldots + c_{i-1} x \cdot \omega_{i-1} + \frac{1}{s}\omega_i + c_{i+1} x \cdot \omega_{i+1} + \ldots + c_{n-1} x \omega_{n-1}.$$

Определитель перехода от базиса $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ к системе $[\omega_0, \ldots, \omega_{i-1}, \eta', \omega_{i+1}, \ldots, \omega_{n-1}]$

$$\begin{vmatrix} 1, & 0, & \ldots & 0 \\ 0, & 1, & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ c_0 x, & c_1 x, & \ldots, \frac{1}{s}, & \ldots, c_{n-1} x \\ \ldots & \ldots & \ldots & \ldots \\ 0, & 0, & \ldots & 1, \end{vmatrix} = \frac{1}{s},$$

откуда при помощи формулы (2,7) мы получаем:

$$\Delta[\omega_0, \ldots, \omega_{i-1}, \eta', \omega_{i+1}, \ldots, \omega_{n-1}] = \frac{1}{s^2} \cdot \Delta[\omega_0, \omega_1, \ldots, \omega_{n-1}].$$

Таким образом, если какой-нибудь целочисленный (т. е. составленный из целых алгебраических чисел) базис не является фундаментальным, то от него можно перейти к другому целочисленному базису, дискриминант которого будет иметь меньшее численное значение. Но дискриминант целочисленного базиса есть целое рациональное число, а потому, применяя этот процесс последовательно к получающимся базисам, мы после конечного числа шагов придем к невозможности дальнейшего пони-

жения дискриминанта. Это служит признаком того, что полученный базис является фундаментальным.

6. Как найти для данного поля фундаментальный базис? Оказывается, что изложенный только-что прием может служить также методом для построения фундаментального базиса при помощи конечного числа действий. Чтобы убедиться в этом, достаточно показать, что при помощи конечного числа действий можно узнать, является ли заданный базис $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ фундаментальным или нет. Последнее можно показать, исходя из того, что в знаменателях координат $c_0, c_1, \ldots, c_{n-1}$ целого числа $\alpha = c_0\omega_0 + c_1\omega_1 + \ldots + c_{n-1}\omega_{n-1}$ могут стоять только делители заранее известного числа (дискриминанта базиса). В самом деле, выпишем выражения для всех сопряженных с α чисел:

$$\begin{aligned}
\alpha &= c_0\omega_0 + c_1\omega_1 + \ldots + c_{n-1}\omega_{n-1},\\
\alpha' &= c_0\omega'_0 + c_1\omega'_1 + \ldots + c_{n-1}\omega_{n-1},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\alpha^{(n-1)} &= c_0\omega_0^{(n-1)} + c_1\omega_1^{(n-1)} + \ldots + c_{n-1}\omega_{n-1}^{(n-1)}.
\end{aligned}$$

Найдем отсюда выражения для c_i:

$$c_i = \frac{\begin{vmatrix} \omega_0 & \alpha & \omega_{n-1} \\ \omega_0^{(n-1)} & \alpha^{(n-1)} & \omega_{n-1}^{(n-1)} \end{vmatrix}}{\begin{vmatrix} \omega_0 & \omega_{n-1} \\ \omega_0^{(n-1)} & \omega_{n-1}^{(n-1)} \end{vmatrix}} \cdot (i = 0, 1, \ldots n-1).$$

Умножая числитель и знаменатель на $\begin{vmatrix} \omega_0, \ldots, \omega_{n-1} \\ \ldots\ldots\ldots \\ \omega_0^{(n-1)}, \ldots, \omega_{n-1} \end{vmatrix}$, мы получим в знаменателе дискриминант Δ базиса $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$, а в числителе целое алгебраическое число, которое, будучи рационально, должно быть целым рациональным числом.

Таким образом, чтобы узнать, существуют ли целые числа $c_0\omega_0 + c_1\omega_1 + \ldots + c_{n-1}\omega_{n-1}$ с дробными координатами $c_0, c_1, \ldots, c_{n-1}$, достаточно проверить, нет ли целых чисел вида

$$\frac{f_0\omega_0 + f_1\omega_1 + \ldots + f_{n-1}\omega_{n-1}}{\Delta}.$$

Выделяя в f_i части, кратные Δ: $f_i = \Delta q_i + r_i (0 \leqq r_i < \Delta; i = 0, 1, \ldots, n-1)$, мы получим:

$$\frac{f_0\omega_0 + f_1\omega_1 + \ldots + f_{n-1}\omega_{n-1}}{\Delta} = q_0\omega_0 + q_1\omega_1 + \ldots + q_{n-1}\omega_{n-1} + \frac{r_0\omega_0 + \ldots + r_{n-1}\omega_{n-1}}{\Delta}.$$

Числа

$$\frac{f_0\omega_0 + \ldots + f_{n-1}\omega_{n-1}}{\Delta} \text{ и } \frac{r_0\omega_0 + \ldots + r_{n-1}\omega_{n-1}}{\Delta}$$

должны быть или одновременно целыми или одновременно дробными. Поэтому достаточно проверить, нет ли целых чисел среди чисел вида $\frac{r_0\omega_0 + \ldots + r_{n-1}\omega_{n-1}}{\Delta}$, где r_i пробегают значения $0, 1, \ldots, \Delta - 1$. Таким образом чисел всего Δ^n, т. е. конечное число. Мы узнаем, является ли каждое из этих чисел целым, если составим для него уравнение (см., например, часть I, стр. 75—76, п. 9). Таким образом мы убеждаемся, что нахождение фундаментального базиса достигается путем конечного числа действий.

7. Применение описанного приема на практике весьма громоздко и требует большого числа по существу лишних операций. В виду этого для полей низших степеней, квадратичных и кубических, были даны приемы, основанные на арифметических свойствах полей и приводящие нахождение фундаментального базиса в каждом данном случае к нескольким весьма несложным операциям. Решение этой задачи для кубических полей принадлежит Г. Ф. Вороному.

8. Пусть квадратичное поле K задано производящей величиной $\sqrt{d}$, где d можно считать целым рациональным числом, не имеющим квадратичных множителей. Чтобы найти фундаментальный базис этого поля, исследуем, каковы должны быть числа x, y для того, чтобы $x + y\sqrt{d}$ было целым алгебраическим числом. Это число удовлетворяет уравнению

$$t^2 - 2xt + (x^2 - y^2 d) = 0.$$

Таким образом $2x$ и $x^2 - y^2 d$ должны быть целыми рациональными числами. Отсюда прежде всего $x = \xi + \frac{\varepsilon}{2}$, где ξ — целое рациональное число, $\varepsilon = 0$ или $\varepsilon = 1$. Второе условие дает нам: $\frac{\varepsilon}{4} - y^2 d$ должно быть целым числом. Из того, что d не имеет квадратичных множителей, следует, что y может иметь в знаменателе только двойку, притом в первой степени. Полагая аналогично $y = \eta + \frac{\varepsilon'}{2}$ и подставляя во второе условие, мы убедимся, что $\frac{\varepsilon}{4} - \frac{\varepsilon'}{4} d$ должно быть целым числом. Отсюда $\varepsilon' = \varepsilon$. Кроме того $\varepsilon = 1$ может иметь место только в том случае, если $d \equiv 1 \pmod 4$. Таким образом задача расчленяется на два случая в зависимости от арифметических свойств числа d:

1. $d \equiv 2$ или $d \equiv 3 \pmod 4$ [Случай $d \equiv 0 \pmod 4$ исключается, так как тогда d содержало бы квадратичный множитель 2^2]. Условию $\varepsilon(1 - d) \equiv 0 \pmod 4$ можно удовлетворить, только нола-

гая $\varepsilon = 0$. Всякое целое число поля может быть представлено в виде $\xi + \eta\sqrt{d}$ с целыми ξ, η · $[1, \sqrt{d}]$ есть фундаментальный базис. Его дискриминнант равен

$$\begin{vmatrix} S(\omega_0^2), & S(\omega_0\omega_1) \\ S(\omega_1\omega_0), & S(\omega_1^2) \end{vmatrix} = \begin{vmatrix} 2, & 0 \\ 0, & 2d \end{vmatrix} = 4d.$$

2. $d \equiv 1 \pmod 4$. Условие $\varepsilon(1-d) \equiv 0 \pmod 4$ удовлетворяется при всяком ε, а потому всякое целое число поля может быть представлено в виде $\xi + \eta\sqrt{d} + \varepsilon \cdot \frac{1+\sqrt{d}}{2}$ с целыми ξ, η. Число $\omega = \frac{1+\sqrt{d}}{2}$ есть целое число (оно есть корень уравнения $t^2 - t - \frac{d-1}{4} = 0$). Образуя при его помощи базис $[1, \omega]$ и выражая $\sqrt{d}$ через ω: $\sqrt{d} = 2\omega - 1$, мы видим, что всякое целое число поля выражается так: $\xi + \eta(2\omega - 1) + \varepsilon\omega = (\xi - \eta) + (2\eta + \varepsilon)\omega$, т. е. с целыми координатами при 1 и ω, откуда следует, что $1, \omega]$ есть фундаментальный базис. Его дискриминант равен

$$\begin{vmatrix} S(1), & S(\omega) \\ S(\omega), & S(\omega^2) \end{vmatrix} = \begin{vmatrix} 2, & 1 \\ 1, & \frac{d+1}{2} \end{vmatrix} = d.$$

6. Два фундаментальных базиса $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ и $[\eta_0, \eta_1, \ldots \ldots \eta_{n-1}]$ одного и того же поля должны переходить друг в друга при помощи целочисленных линейных подстановок:

$$[\eta_0, \eta_1, \ldots, \eta_{n-1}] = \begin{pmatrix} c_{00}, & \ldots, c_{0,\,n-1} \\ \ldots\ldots\ldots\ldots \\ c_{n-1,\,0} \ldots, & c_{n-1,\,n-1} \end{pmatrix} [\omega_0, \omega_1, \ldots, \omega_{n-1}],$$

$$[\omega_0, \omega_1, \ldots, \omega_{n-1}] = \begin{pmatrix} f_{00}, \ldots\ldots, f_{0,\,n-1} \\ \ldots\ldots\ldots\ldots \\ f_{n-1,\,0}, \ldots, f_{n-1,\,n-1} \end{pmatrix} [\eta_0, \eta_1, \ldots, \eta_{n-1}],$$

откуда

$$[\omega_0, \omega_1, \ldots, \omega_{n-1}] = \begin{pmatrix} f_{00}, \ldots\ldots, f_{0,\,n-1} \\ \ldots\ldots\ldots\ldots \\ f_{n-1,\,0}, \ldots, f_{n-1,\,n-1} \end{pmatrix} \times$$

$$\times \begin{pmatrix} c_{00}, \ldots\ldots, c_{0,\,n-1} \\ \ldots\ldots\ldots\ldots \\ c_{n-1,\,0}, \ldots, c_{n-1,\,n-1} \end{pmatrix} [\omega_0, \omega, \ldots, \omega_{n-1}]$$

или

$$\begin{pmatrix} f_{00}, \ldots\ldots, f_{0,\,n-1} \\ \ldots\ldots\ldots\ldots \\ f_{n-1,\,0}, \ldots, f_{n-1,\,n-1} \end{pmatrix} \begin{pmatrix} c_{00}, \ldots\ldots, c_{0,\,n-1} \\ \ldots\ldots\ldots\ldots \\ c_{n-1,\,0}, \ldots c_{n-1,\,n-1} \end{pmatrix} = \begin{pmatrix} 1\ 0\ \ldots\ 0 \\ 0\ 1\ \ldots\ 0 \\ \ldots\ldots \\ 0\ 0\ \ldots\ 1 \end{pmatrix}.$$

Поэтому произведение двух целочисленных определителей $|c_{ik}|$ и $|f_{ik}|$ равно единице, откуда следует, что

$$|c_{ik}| = \pm 1, \quad |f_{ik}| = \pm 1.$$

Формула (2.7) убеждает нас, что дискриминанты обоих базисов равны:

$$\Delta[\eta_0, \eta_1, \ldots, \eta_{n-1}] = \Delta[\omega_0, \omega, \ldots, \omega_{n-1}].$$

Таким образом величина дискриминанта фундаментального базиса одного и того же поля зависит не от выбора этого базиса, а исключительно от свойств поля. В связи с этим дискриминант фундаментального базиса носит название *дискриминанта D поля*.

Из этой же формулы (2.7) вытекает, что дискриминанты целочисленных (не фундаментальных) базисов $[\eta_0, \eta_1, \ldots, \eta_{n-1}]$ отличаются на множители, равные квадратам целых рациональных чисел:

$$\Delta[\eta_0, \eta_1, \ldots, \eta_{n-1}] = k^2 \cdot D.$$

Такого рода множитель называется *индексом базиса* $[\eta_0, \eta_1, \ldots, \eta_{n-1}]$. Если, в частности, базис степенной: $[1, \alpha, \ldots, \ldots, \alpha^{n-1}]$, то соответствующее ему число k называется *индексом числа* α.

Базис $[\eta_0, \eta_1, \ldots, \eta_{n-1}]$ является фундаментальным тогда и только тогда, если его индекс $k = 1$. Если поле содержит фундаментальные степенные базисы, то оно называется *простейшим*.

Общий наибольший делитель индексов всевозможных степенных базисов поля носит название *индекса поля*.

§ 3. Идеалы

1. Основываясь на понятии целого алгебраического числа, нетрудно развить теорию делимости и разложения на множители целых алгебраических чисел.

Будем говорить, что α *делится* на β, если частное $\alpha : \beta$ есть целое алгебраическое число.

Если α делится на β и β делится на α, то будем называть α и β *ассоциированными*. α и β ассоциированы тогда и только тогда, если частное $\alpha : \beta = \varepsilon$, равно как и $\frac{1}{\varepsilon}$, есть целое алгебраическое число. В этом случае ε называют *алгебраической единицей*.

Теорема 7. Чтобы целое число ε было алгебраической единицей, необходимо и достаточно, чтобы его норма была равна ± 1.

Доказательство. 1. Условие необходимо, так как в случае $|N(\varepsilon)|>1$ норма числа $\frac{1}{\varepsilon}$, равная $\frac{1}{N(\varepsilon)}$, является правильной дробью, в силу чего $\frac{1}{\varepsilon}$ не может быть целым числом.

2. Условие достаточно. В самом деле, если $N(\varepsilon)=\pm 1$, то ε удовлетворяют уравнению вида

$$\varepsilon^n + a_1\varepsilon^{n-1} + \ldots + a_{n-1}\varepsilon \pm 1 = 0.$$

Тогда $\eta=\frac{1}{\varepsilon}$ будет корнем уравнения

$$\pm\eta^n + a_{n-1}\eta^{n-1} + \ldots + a_1\eta + 1 = 0,$$

где $a_{n-1},\ldots,a_1$, 1 целые числа. Отсюда следует, что η есть целое алгебраическое число, ч. и т. д.

2. Если целое алгебраическое число α может быть представлено в виде произведения двух множителей: $\alpha=\beta\gamma$, и при этом $|N(\beta)|>1$, $|N(\gamma)|>1$, то такое разложение мы будем называть существенным. В этом случае можно было бы сказать, что α не есть простое число. Случай же, когда один из множителей есть алгебраическая единица, должен считаться тривиальным, так как любое целое α можно представить как произведение двух целых чисел $\alpha\varepsilon$ и $\frac{1}{\varepsilon}$, где ε — произвольная единица поля. Разлагая множители β и γ и продолжая процесс, мы замечаем, что получающиеся множители имеют все меньшие нормы. Но так как число целых рациональных чисел, меньших данного числа, ограничено, то после конечного числа шагов мы придем к разложению числа α на множители, не поддающиеся дальнейшему разложению. Такие множители не играют, однако, той роли, которую играют простые числа в теории рациональных полей, так как разложение алгебраических чисел на неразложимые множители не всегда однозначно.

Пример: Дано поле $K(\sqrt{-5})$. В нем

$$9 = 3\cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5}). \qquad (3.1)$$

Если бы число 9 разлагалось однозначно, то каждое из чисел 3, $2\pm\sqrt{-5}$ должно было бы допускать дальнейшее разложение. Из того, что внутри $K(\sqrt{-5})$

$$N(3)=N(2\pm\sqrt{-5})=9,$$

следует, что нормы чисел, на которые разлагались бы $3, 2\pm\sqrt{-5}$, должны быть равны 3. Вместе с тем фундаментальный базис поля $K(\sqrt{-5})$ есть $[1, \sqrt{-5}]$ (см. § 2, 8), а потому каждый из множителей этих чисел должен иметь вид $x+y\sqrt{-5}$, где x, y — целые рациональные числа. Итак, должно иметь место

$$N(x+y\sqrt{-5}) = x^2+5y^2 = 3.$$

Но это неопределенное уравнение очевидно не имеет решений.

Другой подобный пример из того же поля:

$$21 = 7\cdot 3 = (4+\sqrt{-5})(4-\sqrt{-5}). \qquad (3.2)$$

3. С целью восстановить однозначность разложения целых чисел в иррациональных алгебраических полях и тем самым приблизить их теорию к теории целых рациональных чисел, Куммер (G. Kummer) ввел в рассмотрение фиктивные множители, названные им *идеальными числами*. Так, по Куммеру, для чисел примера (3.1) число 3 нужно представить в виде произведения двух идеальных чисел $3=\alpha\cdot\beta$, откуда следует:

$$2+\sqrt{-5}=\alpha^2,\quad 2-\sqrt{-5}=\beta^2.$$

В примере (3.2) надо, кроме того, положить $7=\gamma\delta$, откуда

$$4+\sqrt{-5}=\alpha\gamma,\quad 4-\sqrt{-5}=\beta\delta.$$

Для теории идеальных чисел Дедекинд (R. Dedekind) и Кронекер (L. Kronecker) подвели логическую базу, введя понятие *идеала*. Но еще несколько раньше их Е. И. Золотарев предложил теорию, эквивалентную теории идеалов и основанную на рассмотрении *локальных свойств* алгебраических чисел (термин, введенный совсем недавно). Ввиду особого изящества теории Золотарева, а также простоты связанных с ней выводов, мы изложим теорию идеалов по Золотареву.

4. Золотарев берет в основу произвольное рациональное простое число p и вводит понятие *делимости по модулю p* (или, как мы для краткости будем выражаться, *p-делимости*) следующим образом:

> Будем говорить, что α *p-делится* на β, если можно подобрать такое взаимно простое с p целое рациональное число c, что $\frac{c\alpha}{\beta}$ было бы целым алгебраическим числом.

Нетрудно видеть, что в качестве c мы можем взять делитель числа $N(\beta)$, взаимно простой с p. В самом деле, пусть $\frac{c\alpha}{\beta}$ есть целое алгебраическое число и $(c, p)=1$. Вместе с тем $\frac{N(\beta)}{\beta}$, будучи произведением сопряженных с β чисел, отличных от β (β целое), есть тоже целое алгебраическое число. Общий наибольший делитель d чисел c и $N(\beta)$ есть взаимно простой с p делитель $N(\beta)$. Решим в целых числах неопределенное уравнение

$$cx + N(\beta)y = d.$$

Число

$$\frac{c\alpha}{\beta}x+\frac{N(\beta)}{\beta}\alpha y=\frac{d\alpha}{\beta}$$

есть целое алгебраическое число, что доказывает наше утверждение.

Чтобы проверить, что α p-делится на β, достаточно составить неприводимое уравнение, корнем которого является $\frac{\alpha}{\beta}$. Пусть это будет $x^n+b_1x^{n-1}+\ldots+b_{n-1}x+b_n=0$. Чтобы α p-делилось на β, необходимо и достаточно, чтобы p не входило в знаменатели коэфициентов $b_1, b_2, \ldots, b_n$. Условие достаточно, так как, если c есть общий знаменатель коэфициентов $b_1, b_2, \ldots, b_n$, то коэфициенты $b_1c, b_2c^2, \ldots, b_nc^n$ уравнения, которому удовлетворяет $\frac{c\alpha}{\beta}$, суть целые числа. Это условие и необходимо, так как, если в знаменателях $b_1, b_2, \ldots, b_n$ содержится множитель p, то, каково бы ни было взаимно простое с p число c, число p не может быть изгнано из знаменателей чисел $b_1c, b_2c^2, \ldots, b_nc^n$.

5. Для p-делимости имеют место следующие легко доказываемые теоремы:

Если α p-делится на β и β p-делится на γ, то α p-делится на γ.

Если α и β p-делятся на γ, то и $\alpha+\beta$ p-делятся на γ.

6. Имея дело с понятием p-делимости, можно установить понятие общего наибольшего делителя. Для этого, называя *p-порядком* целого алгебраического числа ω наивысшую степень p, входящую в $N(\omega)$, докажем следующую теорему Золотарева, центральную для всей его теории:

Теорема 7а. Если среди всех чисел типа $\omega+p^\nu\cdot\omega'$, где ω заданное целое алгебраическое число и ω' пробегает все целые числа поля, число ω имеет наименьший p-порядок, то p^ν p-делится на ω.

Доказательство. Представим уравнение, которому удовлетворяет ω, так:

$$\omega^n+p^{\lambda n-1}\cdot c_1\omega^{n-1}+p^{\lambda n-2}\cdot c_2\omega^{n-2}+\ldots+p^{\lambda_1}c_{n-1}\omega+p^{\lambda}c_n=0, \quad (3.3)$$

где $c_1, c_2, \ldots, c_n$ — взаимно просты с p. Очевидно p-порядок числа ω есть p^λ. Выберем среди чисел

$$\frac{\lambda-\lambda_1}{1}, \frac{\lambda-\lambda_2}{2}, \ldots, \frac{\lambda-\lambda_{n-1}}{n-1}, \frac{\lambda}{n}$$

наибольшее. Пусть это будет $\mu=\frac{r}{s}$, где $(r, s)=1$. Докажем, что p^μ p-делится на ω; именно, что $\frac{p^\mu c_n}{\omega}$ есть целое число. Для

этого сделаем в уравнении (3.3) подстановку $\omega=\frac{p^\mu c_n}{z}$. Уравнение для z можно представить в виде:

$$z^n+p^{\lambda_1-\lambda+\mu}c_{n-1}z^{n-1}+p^{\lambda_2-\lambda+2\mu}c_{n-1}c_nz^{n-2}+\ldots+$$
$$+p^{\lambda_{n-1}-\lambda+\mu(n-1)}c_1c_n^{n-2}z+p^{-\lambda+\mu n}c_n^{n-1}=0. \quad (3.3^1)$$

В силу определения числа μ имеет место неравенство $\lambda_i-\lambda+i\mu\geqslant 0$, откуда, применяя в случае дробных показателей теорему 3, мы убедимся, что $\frac{p^\mu c_n}{\omega}$ есть целое число.

Для доказательства нашей теоремы достаточно показать, что $\nu\geqslant\mu$. Допустим противное, т. е. что $\mu=\frac{r}{s}>\nu$. Из того, что $\left(\frac{p^\mu c_n}{\omega}\right)^s=\frac{p^r c_n^s}{\omega^s}$ есть целое число, следует, что p-порядки чисел $\zeta_i=\omega-p^\nu\left(\frac{p^r c_n}{\omega^s}\right)^i$ $(i=1, 2, 3, \ldots)$ не ниже, чем p^ν. Но

$$N(\zeta_1)=N\left(\omega-\frac{p^{ri+\nu}c_n^{si}}{\omega^{si}}\right)=\frac{N(\omega^{si+1}-p^{ri+\nu}c_n^{si})}{[N(\omega)]^{si}},$$

откуда следует, что порядок числа $\omega^{si+1}-p^{ri+\nu}\cdot c_n^{si}$ равен по меньшей мере $p^{\lambda(si+1)}$.

Преобразуем выражение $N(\omega^{si+1}-p^{ri+\nu}\cdot c_n^{si})$.

Для этого применим тождество

$$x^{si+1}-y^{si+1}=(x-y)(x-\varepsilon y)\ldots(x-\varepsilon^{si}y),$$

где $\varepsilon=e^{\frac{2\pi i}{si+1}}$, к двучлену $\omega^{si+1}-p^{ri+\nu}\cdot c_n^{si}\cdot\omega^{si+1}-$

$$-p^{ri+\nu}\cdot c_n^{si}=\left(\omega-p^{\frac{ri+s\nu}{si+1}}\cdot c_n^{\frac{si}{si+1}}\right)\times$$
$$\times\left(\omega-\varepsilon\cdot p^{\frac{ri+\nu}{si+1}}c_n^{\frac{si}{si+1}}\right)\ldots\left(\omega-\varepsilon^{si}p^{s\varepsilon+1}c^{\frac{si}{si+1}}\right),$$

откуда

$$N(\omega^{si+1}-p^{ri+\nu}\cdot c_n^{si})=\prod_{j=0}^{si}N\left(\omega-\varepsilon^j\cdot p^{\frac{ri+\nu}{si+1}}\cdot c_n^{\frac{si}{si+1}}\right),$$

где в выражениях норм в правой части с величинами $\varepsilon^j\cdot p^{\frac{ri+\nu}{si+1}}\cdot c_n^{\frac{si}{si+1}}$ надо поступать, как с рациональными числами

В силу этого к каждой из этих норм применима формула (1.8), т. е.

$$N\left(\omega - \varepsilon^j p^{\frac{ri+\nu}{si+1}} c_n^{\frac{si}{si+1}}\right) = f\left(\varepsilon^j \cdot p^{\frac{ri+\nu}{si+1}} \cdot c_n^{\frac{si}{si+1}}\right) = \left.\begin{aligned} &= \varepsilon^{jn} p^{n\frac{ri+\nu}{si+1}} c_n^{n\frac{si}{si+1}} + p^{\lambda_{n-1}+(n-1)\frac{ri+\nu}{si+1}} \cdot \varepsilon^{j(n-1)} \times \\ &\times c\, c_n^{(n-1)\frac{si}{si+1}} + \ldots + p^{\lambda_1+\frac{ri+\nu}{si+1}} \cdot \varepsilon^j \cdot c_{n-1} c_n^{\frac{si}{si+1}} + p^{\lambda} c_n. \end{aligned}\right\} \quad (3.4)$$

Так как в силу нашего предположения $\mu \neq \nu$, то можно подобрать i так, чтобы все показатели

$$n\frac{ri+\nu}{si+1},\ \lambda_{n-1}+(n-1)\frac{ri+\nu}{si+1},\ \ldots,\ \lambda_1+\frac{ri+\nu}{si+1},\ \lambda \quad (3.5)$$

степеней p, на которые *точно* делятся члены выражения (3.4), были все различны между собой. В самом деле, каждое из равенств

$$\lambda_u + u\frac{ri+\nu}{si+1} = \lambda_v + v\frac{ri+\nu}{si+1} \qquad (u, v = 0, 1, 2, \ldots, n)$$

или удовлетворяется тождественно относительно i, что влечет за собой равенства

$$\lambda_u s + ur = \lambda_v \cdot s + vr, \quad \lambda_u + u\nu = \lambda_v + v\nu,$$

откуда

$$(u-v)\left(\frac{r}{s} - \nu\right) = 0,$$

что в силу $u \neq v$ и $\mu = \frac{r}{s} \neq \nu$ невозможно, или удовлетворяется только одним значением i. Исключив такие значения i, соответствующие всевозможным комбинациям u и v, выберем i в остальном произвольно. Из того, что все показатели (3.5) различны, следует, что все члены выражения (3.4) делятся на различные степени p. Поэтому выражение (3.4) делится на p в степени, показатель которой равен наименьшему из чисел (3.5).

Из нашего допущения $\mu = \frac{r}{s} > \nu$ следует $r > s\nu$, откуда, прибавляя к обеим частям неравенства по rsi, будем иметь:

$$r(si+1) > s(ri+\nu) \quad \text{или} \quad \mu = \frac{r}{s} > \frac{ri+\nu}{si+1}. \quad (3.6)$$

С другой стороны, в силу определения μ существует такой значок f, для которого имеет место

$$\mu = \frac{\lambda - \lambda_f}{f},$$

или

$$\lambda = \lambda_f + \mu f,$$

откуда в силу (3.6)

$$\lambda > \lambda_f + f \cdot \frac{ri+\nu}{si+1}.$$

Правая часть этого неравенства равна одному из показателей (3.5), и таким образом это неравенство говорит нам, что выражение (3.4) для каждого значения j делится на p в меньшей, чем λ-ая, степени. Их произведение поэтому делится на p в меньшей, чем $\lambda(si+1)$-ая, степени. Но, с другой стороны, мы имели, что это произведение, равное $N(\omega^{si+1} - p^{ri+\nu} \cdot c_n^{si})$, делится на p по меньшей мере в $\lambda(si+1)$-ой степени. Полученное противоречие доказывает, что $\mu \leqslant \nu$, ч. и т. д.

7. Возьмем два произвольных целых алгебраических числа рассматриваемого поля: ω_1 и ω_2, и подберем такое целое число поля ω', чтобы порядок числа $\omega_3 = \omega_1 + \omega' \cdot \omega_2$ был возможно меньшим. Докажем, что ω_2 (а потому и ω_1) p-делится на ω_3. Пусть порядок числа ω_2 есть p^ν. Умножим ω_3 на целое число $\omega_4 = \frac{cp^\nu}{\omega_2}$ (c — взаимно просто с p):

$$\omega_4 \cdot \omega_3 = \omega_4\omega_1 + \omega' \cdot cp^\nu.$$

Тогда очевидно, что $\omega_4 \cdot \omega_3$ будет иметь среди всех чисел типа $\omega_4\omega_1 + \omega' cp^\nu$ наименьший порядок. Вместе с тем из хода доказательства теоремы 7 видно, что ничего не изменится, если мы вместо произвольных целых чисел ω' будем брать числа типа $c \cdot \omega'$, где c — определенное взаимно простое целое рациональное число. Поэтому мы можем в силу теоремы 7 утверждать, что p^ν p-делится на $\omega_4\omega_3$, т. е. что при некотором взаимно простом с p числе c'

$$\frac{c'p^\nu}{\omega_3\omega_4} = \frac{c' \cdot p^\nu \omega_2}{\omega_3 \cdot cp^\nu} = \frac{c'\omega_2}{c\omega_3}$$

есть целое число. Отсюда следует, что ω_2 p-делится на ω_3, ч. и т. д.

Итак, ω_3 есть p-делитель чисел ω_1 и ω_2. С другой стороны, всякий общий p-делитель чисел ω_1 и ω_2 есть также p-делитель числа $\omega_3 = \omega_1 + \omega'\omega_2$. Поэтому число ω_3 является *общим наибольшим p-делителем* чисел ω_1 и ω_2, и мы приходим к

Теореме 8. Всякие два (или также более) целых числа алгебраического поля имеют общий наибольший p-делитель.

В частности, если для ω_1 и ω_2 можно подобрать ω' так, чтобы число $\omega_1 + \omega'\omega_2$ имело нулевой порядок (т. е. чтобы его

норма не делилась на p), то числа ω_1 и ω_2 будем называть *p-взаимно-простыми*.

8. Из факта существования для любой пары целых чисел поля общего наибольшего p-делителя вытекает справедливость следующих теорем:

Теорема 9. Если произведение $\alpha\beta$ p-делится на γ, а α p-взаимно-просто с γ, то β p-делится на γ.

Доказательство. Из p-взаимной простоты α и γ следует, что существует такое ω', что $\varepsilon=\alpha'+\gamma\omega'$ имеет взаимно простую с p норму $N(\varepsilon)=c$. Умножая равенство на целое алгебраическое число $\varepsilon'=\frac{c}{\varepsilon}$, получим:

$$c=\alpha\varepsilon'+\gamma\omega'\varepsilon'.$$

Умножая на β, мы видим, что правая часть равенства $c\beta=\alpha\beta\varepsilon'+\gamma\omega'\varepsilon'$ p-делится на γ. Поэтому и $c\beta$ p-делится на γ, т. е. существует такое взаимно простое с p число c', что $\frac{c'c\beta}{\gamma}$ есть целое число. Это показывает, что β p-делится на γ, ч. и т. д.

Теорема 10. Если α и β p-взаимно-просты с γ, то и их произведение $\alpha\beta$ p-взаимно-просто с γ.

Доказательство. В силу определения можно найти такие ω' и ω'', что $\varepsilon'=\alpha+\gamma\omega'$ и $\varepsilon''=\beta+\gamma\omega''$, где нормы ε' и ε'' взаимно просты с p. Перемножив, получим:

$$\varepsilon'\varepsilon''=\alpha\beta+\gamma(\alpha\omega''+\beta\omega'+\gamma\omega'\omega''),$$

где $N(\varepsilon'\varepsilon'')$ взаимно проста с p. Это равенство доказывает теорему

Теорема 11. Если α p-делится на два взаимно простых числа β и γ, то оно p-делится и на их произведение $\beta\gamma$.

Доказательство. Из условия вытекает, что при некотором взаимно простом с p числе c число $\frac{c\alpha}{\beta}$ — целое. Произведение $c\alpha=\frac{c\alpha}{\beta}\beta$ p-делится на γ. Но так как β p-взаимно-просто $c\gamma$, то в силу теоремы 9 $\frac{c\alpha}{\beta}$ p-делится на γ, откуда α p-делится на $\beta\gamma$, ч. и т. д.

9. Дадим два различных определения *p-простых чисел* и покажем, что эти определения равносильны.

I. Число π называется p-простым, если всякий раз, когда произведение $\alpha\beta$ p-делится на π, должен p-делиться на π один из множителей.

II. Число π называется *p-простым*, если всякое целое число поля или p-делится на π или p-взаимно-просто с π.

Пусть для π имеет место свойство I. Докажем, что для него имеет место свойство II, т. е. что всякое число α, не p-взаимно-простое с π, p-делится на π. Пусть α не p-взаимно-просто с π и пусть их общим наибольшим делителем будет δ. Тогда порядок чисел $\frac{\pi}{\delta}$ должен быть ниже порядка числа π, а потому $\frac{\pi}{\delta}$ не может p-делиться на π. Но так как $\frac{\alpha}{\delta}\cdot\pi=\alpha\cdot\frac{\pi}{\delta}$ p-делится на π, то в силу свойства I α должно p-делиться на π, ч. и т. д.

Предположим теперь, что для π имеет место свойство II. Пусть произведение $\alpha\beta$ p-делится на π. Докажем, что или α или β p-делится на π. Если α не p-делится на π, то в силу свойства II оно p-взаимно-просто с π. Тогда в силу теоремы 9 β p-делится на π, что доказывает для π справедливость свойства II.

10. Зададимся целью разложить p на p-простые множители. Рассмотрим совокупность чисел

$$c_0\omega_0+c_1\omega_1+\ldots+c_{n-1}\omega_{n-1},$$

где $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ — фундаментальный базис поля, а каждое из c_i пробегает по одному разу представителей классов сравнений по модулю p. Этих представителей мы каждый раз будем выбирать так, чтобы число $\alpha=c_0\omega_0+c_1\omega_1+\ldots+c_{n-1}\omega_{n-1}$ имело наименьший p-порядок по сравнению со всевозможными числами вида $\alpha+p\cdot\omega'$. Обозначим получаемые таким образом числа через

$$\alpha_1, \alpha_2, \ldots, \alpha_{\sigma-1}, \tag{3.7}$$

где $\sigma=p^n$ (комбинацию $c_0=c_1=\ldots=c_{n-1}=0$ мы исключаем). Из теоремы 7 следует, что все числа (3 · 7) суть p-делители числа p. Кроме того, все p-простые числа содержатся среди чисел (3.7). В самом деле, всякое целое число поля можно представить в формуле $\alpha=\alpha_i+p\omega'$, где α_i — одно из чисел (3.7). Но p, а потому и α, p-делится на α_i. Вместе с тем $N(\alpha)\equiv N(\alpha_i) \pmod p$, в силу чего, если α_i, то и α имеет нулевой p-порядок. Если теперь α есть p-простое число, то α_i, будучи p-делителем α и имея отличный от нулевого p-порядок, тоже должно быть p-простым числом, p-делящимся на α. Такие p-простые числа мы не будем считать различными.

Если все нормы чисел (3.7) взаимно просты с p, то само p является простым числом внутри поля. В самом деле, всякое целое число поля может быть представлено в виде $\alpha_i+p\omega'$ или $0+p\omega'$. В первом случае оно p-взаимно-просто с p, во втором делится на p, так что число p удовлетворяет свойству II.

Если же некоторые из чисел (3.7) имеют отличный от нулевого p-порядок, то выберем среди них число π_1 с наименьшим

p-порядком f_1. Нетрудно видеть, что π_1 является p-простым числом. В самом деле, возьмем произвольное целое число ω нашего поля и рассмотрим всевозможные числа вида $\pi_1 + \omega\omega'$. Каждое из них можно представить или в виде $0 + p\omega'$ или в виде $\alpha_i + p\omega'$, и в обоих случаях оно в силу определения f_1 будет иметь или нулевой, или не меньший, чем f_1, p-порядок. В последнем случае в силу теоремы 7 ω p-делится на π_1, так что для π_1 имеет место свойство II.

Пусть $\pi_1^{e_1}$ будет наибольшая степень, на которую p-делится p. Целое число $\frac{cp}{\pi_1^{e_1}}$, где $(c,p)=1$, не p-делится на π_1 и потому p-взаимно просто с π_1.

Выберем среди всех чисел (3.7), p-взаимно простых с π_1, число π_2, имеющее наименьший отличный от нуля p-порядок f_2. Чтобы доказать, что π_2 есть p-простое число, возьмем любое целое число поля ω и рассмотрим всевозможные числа $\pi_2 + \pi_1\omega\omega'$. Если среди них нет чисел нулевого p-порядка, то в силу определения π_2 и f_2 их порядок не может быть меньше, чем f_2, так как каждое такое число можно представить в виде $\alpha_i + p\omega''$, где α_i p-взаимно просто с π_1. Отсюда следует, что $\pi_1\omega$ p-делится на π_2. В силу же того, что π_1 и π_2 p-взаимно просты и теоремы 9, ω p-делится на π_2. Опять для π_2 соблюдается свойство II.

Пусть $\pi_2^{e_2}$ будет наибольшая степень, на которую p-делится p. В силу теоремы 10 $\pi_1^{e_1}$ и $\pi_2^{e_2}$ p-взаимно-просты, и в силу теоремы 11 p p-делится на $\pi_1^{e_1}\pi_2^{e_2}$. Их частное $\frac{cp}{\pi_1^{e_1}\pi_2^{e_2}}$ p-взаимно-просто и с π_1 и с π_2.

Далее берем среди чисел (3.7), взаимно простых с π_1 и π_2, число π_3, имеющее наименьший p-порядок f_3. Беря произвольное целое число поля ω и рассматривая числа $\pi_3 + \pi_1\cdot\pi_2\omega\cdot\omega'$, мы опять докажем, что π_3 есть p-простое число. Продолжаем процесс выбора π_i. Он не может продолжаться неограниченно, так как число чисел (3.7), p-взаимно-простых с $\pi_1, \pi_2, \pi_3 \ldots$ и имеющих не нулевой p-порядок, все время убывает. В конце концов мы дойдем до числа π_k такого рода, что все числа (3.7), p-взаимно-простые с $\pi_1, \pi_2, \ldots, \pi_k$, будут иметь нулевой p-порядок. Тогда, если p p-делится точно на $\pi_1^{e_1}\pi_2^{e_2}\ldots\pi_k^{e_k}$, то число $\varepsilon = \frac{cp}{\pi_1^{e_1}\pi_2^{e_2}\ldots\pi_k^{e_k}}$, p-взаимно-простое с $\pi_1, \pi_2, \ldots, \pi_k$, должно иметь нулевой p-порядок. Таким образом мы получаем следующее разложение числа p на p-простые множители:

$$cp = \varepsilon\pi_1^{e_1}\pi_2^{e_2}\ldots\pi_k^{e_k}. \tag{3.8}$$

Докажем, что такое разложение единственно. Пусть имеет место такое другое разложение:

$$\bar{c}p = \bar{\varepsilon}\bar{\pi}_1^{\bar{e}_1}\bar{\pi}_2^{\bar{e}_2}\ldots\bar{\pi}_k^{\bar{e}_k}.$$

Приравнивая оба разложения:

$$\bar{c}\varepsilon\pi_1^{e_1}\pi_2^{e_2}\ldots\pi_k^{e_k} = c\bar{\varepsilon}\bar{\pi}_1^{\bar{e}_1}\bar{\pi}_2^{\bar{e}_2}\ldots\bar{\pi}_k^{\bar{e}_k}, \tag{3.9}$$

мы из свойства I p-простого числа—π_1 убеждаемся, что один из множителей $\pi_1, \pi_2, \ldots, \pi_k$, например π_1, должен p-делиться на $\bar{\pi}_1$. В силу же свойства II π_1 тоже должно p-делиться на $\bar{\pi}_1$, т. е. числа π_1 и $\bar{\pi}_1$ мы не должны считать различными. Сокращая равенство (3.9) и продолжая рассуждение, мы убедимся, что $e_1 = \bar{e}_1$. Продолжая рассуждение относительно других множителей, мы убедимся в однозначности разложения.

11. Докажем, что $\pi_1, \pi_2, \ldots, \pi_k$ являются единственными p-простыми числами, и одновременно докажем однозначность разложения на их степени любого целого числа ω нашего поля. Прибавляя к ω соответственно подобранную кратность p, мы получим одно из чисел ряда (3.7): $\omega = \alpha_i + p\omega'$. Если α_i имеет нулевой p-порядок, то, в силу

$$N(\alpha_i + p\omega') \equiv N(\alpha_i) \pmod{p},$$

это же имеет место для числа ω. Если же p-порядок α_i отличен от нуля, то в процессе выбора $\pi_1, \pi_2, \ldots, \pi_k$ и связанного с ним отбрасывания из системы (3.7) не p-взаимно-простых с $\pi_1, \pi_2, \ldots, \pi_k$ чисел, мы должны отбросить и α_i. Это показывает, что α_i (а потому и ω) не p-взаимно-просто с одним из $\pi_1, \pi_2, \ldots, \pi_k$, например с π_i, и в силу свойства II p-делится на π_i. Рассматривая таким же образом целое число $\frac{c\omega}{\pi_i}$, мы видим, что его p-порядок ниже, чем у ω. Продолжая процесс, мы в конце концов придем к целому числу $\frac{c\omega}{\pi_1^{m_1}\pi_2^{m_2}\ldots\pi_k^{m_k}}$ нулевого p-порядка. Это показывает, что ω разлагается в произведение p-простых чисел так:

$$\pi_1^{m_1}\pi_2^{m_2}\ldots\pi_k^{m_k}.$$

Однозначность разложения доказывается в точности так же, как в п. **10** для числа p.

12. Как с помощью конечного числа действий найти среди чисел $\alpha + p^\nu\omega'$ такое, p-порядок которого был бы возможно меньший? Это—вопрос, без разрешения которого весь излагаемый метод нельзя считать эффективным.

Для его решения обратим внимание на то, что

$$N(\alpha + p^m\omega') \equiv N(\alpha) \pmod{p^m}.$$

Справедливость этого сравнения видна из того, что

$$N(\alpha + p^m\omega') = \prod_{i=0}^{n-1}(\alpha^{(i)} + p^m\omega'^{(i)}),$$

где $\alpha^{(i)}$, $\omega'^{(i)}$ — сопряженные с α, ω' числа, которые тоже являются целыми. Если p-порядок числа α равен p^{λ}, то числа типа $\alpha+p^{\lambda+1}\omega'$ будут иметь тот же p-порядок, а потому мы всегда обнаружим наименьший p-порядок чисел $\alpha+p^{\nu}\omega'$, если рассмотрим всевозможные числа $\omega'=c_0\omega_0+c_1\omega_1+\ldots+c_{n-1}\omega_{n-1}$, где каждое из чисел $c_0, c_1, \ldots, c_{n-1}$ пробегает значения 0, 1, 2, $\ldots$, $p^{\lambda+1-\nu}-1$.

13. В частном случае, когда p не входит в индекс поля, задача разложения p на p-простые множители значительно упрощается. В этом случае можно выбрать такое целое число поля ω, что всякое целое число поля может быть представлено в виде $c_0+c_1\omega+c_2\omega^2+\ldots+c_{n-1}\omega^{n-1}$, где $c_0, c_1, \ldots, c_{n-1}$ — целые рациональные числа и c взаимно просто с p. При этом, если полином $\varphi(x)$ взаимно прост по модулю p с неприводимым полиномом $f(x)$, корнем которого является ω, то $\varphi(\omega)$ имеет нулевой p-порядок. Действительно, в этом случае можно найти такие полиномы $U(x)$, $V(x)$, чтобы имело место

$$U(x)f(x)+V(x)\varphi(x)=c,$$

где $(c,p)=1$. Подставляя $x=\omega$, получим:

$$V(\omega)\cdot\varphi(\omega)=c_1,$$

откуда

$$N[V(\omega)]\cdot N[\varphi(\omega)]=c^n,$$

и $N[\varphi(\omega)]$, будучи делителем c^n, не делится на p.

Если $\varphi(x)$ разлагается по модулю p на множители:

$$\varphi(x)=\psi(x)\chi(x)+p\cdot\varepsilon(x),$$

то, подставляя $x=\omega$, мы получим:

$$\varphi(\omega)=\psi(\omega)\chi(\omega)+p\cdot\varepsilon(\omega).$$

Поэтому, если $\varphi(\omega)$ p-делится на p-простое число π, то или $\psi(\omega)$ или $\chi(\omega)$ p-делится на π. Поэтому мы можем взять в качестве p-простых чисел $f_i(\omega)$, где $f_i(x)$ — неприводимые по модулю p полиномы, которые в силу предыдущего должны быть делителями $f(x)$ по модулю p. Таким образом, если $f(x)$ разлагается на неприводимые по модулю p множители так:

$$f(x)+p\cdot\psi(x)=[f_1(x)]^{e_1}\cdot[f_2(x)]^{e_2}\ldots[f_k(x)]^{e_k}, \qquad (3.10)$$

то единственными p-простыми числами являются

$$\pi_1=f_1(\omega),\ \pi_2=f_2(\omega),\ \ldots,\ \pi_k=f_k(\omega).$$

Подставляя в тождество (3.10) $x=\omega$, получим:

$$p\cdot\psi(\omega)=\pi_1^{e_1}\cdot\pi_2^{e_2}\ldots\pi_k^{e_k},$$

В этом случае p-порядок f_i каждого p-простого числа $f_i(\omega)$ равен p^{n_i}, где n_i — степень полинома $f_i(x)$. В самом деле, обозначая через $\alpha_1, \alpha_2, \ldots, \alpha_i$ корни полинома $f_i(x)$, а через $\omega_1, \omega_2, \ldots, \omega_n$ — корни полинома $f(x)$, будем иметь:

$$N[f_i(\omega)]=\prod_{i=1}^{n}f_i(\omega_i)=\prod_{i=1}^{n}(\omega_i-\alpha_1)(\omega_i-\alpha_2)\ldots(\omega_i-\alpha_n)=\pm\prod_{j=1}^{n_i}f(\alpha_j).$$

Подставляя в (3.10) $\chi=\alpha_i$:

$$f(\alpha_i)+p\cdot\psi(\alpha_i)=0 \qquad (i=1, 2, \ldots, n_1,)$$

и перемножая получаемые равенства, будем иметь:

$$N[f_1(\omega)]=\pm p^{n_1}\cdot\prod_{i=1}^{n_1}\psi(\alpha_i).$$

Так как множитель $\prod_{i=1}^{n_1}\psi(\alpha_i)$ есть целое число, то

$$f_1\geqq n_1,$$

и аналогично

$$f_i\geqq n_i \qquad (i=1, 2, \ldots, k). \qquad (3.11)$$

Но, сравнивая степени обеих частей тождества (3.10), имеем:

$$e_1n_1+e_2n_2+\ldots+e_kn_k=n. \qquad (3.12)$$

С другой стороны, сравнивая p-порядки обеих частей равенства (3.8), получим

$$e_1f_1+e_2f_2+\ldots+e_kf_k=n. \qquad (3.13)$$

Сопоставляя (3.11), (3.12) и (3.13), мы приходим к равенствам

$$f_i=n_i \qquad (i=1, 2, \ldots, k). \qquad (3.14)$$

Вместе с тем получается, что число $\psi(\omega)$ имеет нулевой p-порядок, откуда следует, что полином $\psi(x)$ взаимно-прост с $f(x)$ по модулю p.

14. В рассматриваемом простейшем случае нетрудно также определить, в какой степени число p входит в дискриминант уравнения (и в силу наших предположений в дискриминант поля). Для этого продифференцируем тождество (3.10):

$$f'(x)=\sum_{i=1}^{k}e_i[f_1(x)]^{e_1}\ldots[f_{i-1}(x)]^{e_{i-1}}[f_i(x)]^{e_i-1}\cdot f_i'(x)\cdot$$

$$\cdot[f_{i+1}(x)]^{e_{i+1}}\ldots[f_k(x)]^{e_k}-p\cdot\psi'(x),$$

и подставим $x=\omega$:

$$f'(\omega)=\sum_{i=1}^{k}e_i\pi_1^{e_1}\ldots\pi_{i-1}^{e_{i-1}}\cdot\pi_i^{e_i-1}f_i'(\omega)\,\pi_{i+1}^{e_{i+1}}\ldots\pi_k^{e_k}-p\cdot\psi'(\omega).$$

Из всех слагаемых правой части член

$$e_i \pi_1^{e_1} \dots \pi_{i-1}^{e_{i-1}} \cdot \pi_i^{e_i-1} f_i'(\omega\pi)_{i+1}^{e_{i+1}} \dots \pi_k^{e_k}$$

p-делится *точно* на $e_i \pi_i^{e_i-1}$, ($f_i'(\omega)$ p-взаимно с $\pi_i = f_i(\omega)$, так как полиномы $f_i(x)$ и $f_i'(x)$ в силу неприводимости $f_i(x)$ взаимно просты по модулю p). Все же другие слагаемые правой части p-делятся по крайней мере на $\pi_i^{e_i}$ (последний член в силу p-делимости p на $\pi_i^{e_i}$). Поэтому в случае $(e_i, p) = 1$ число $f'(\omega)$ p-делится точно на $\pi_i^{e_i-1}$, в случае же $(e_i, p) > 1$ (этот случай носит название *иррегулярного*) оно p-делится по крайней мере на $\pi_i^{e_i}$.

Будем называть *критическими* (относительно данного поля) те простые числа p, которые делятся хотя бы на одно p-простое число выше чем в первой степени. Тогда для рассматриваемого случая имеет место важная

Теорема 12. В дискриминант поля входят делителями критические и только критические простые числа.

В дальнейшем мы докажем эту теорему в полном объеме.

15. Станем рассматривать разложения всех чисел поля одновременно по всем простым модулям. Возьмем целое число α поля и найдем его разложения по простым модулям, входящим в $N(\alpha)$ (относительно остальных модулей α будет играть роль единицы).

Сопоставим с каждым p-простым числом π символ $\mathfrak{P}$ *(простой дивизор)*, говоря, что число α делится на дивизор $\mathfrak{P}^k$ в том случае, если оно p-делится на π^k. *Нормой дивизора* $\mathfrak{P}$ будем называть p-порядок числа π. Два p-простых числа будем считать соответствующими одному и тому же дивизору тогда и только тогда, если они p-ассоциированы, т. е. одно p-делится на другое и обратно. Произведение нескольких простых дивизоров будем называть (не простым) дивизором.

Если теперь мы представим α как произведение своих простых дивизоров, то легко видеть, что $|N(\alpha)|$ равна произведению норм простых дивизоров числа α.

Чтобы вполне обосновать возможность представления чисел поля в виде произведения простых дивизоров, докажем следующие теоремы:

Теорема 13. Если α p-делится на β по всем простым делителям p нормы $N(\beta)$, то α делится на β алгебраически.

Доказательство. Пусть

$$N(\beta) = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}.$$

Тогда существуют целые числа поля

$$\lambda_1 = \frac{c_1 \alpha}{\beta}, \quad \lambda_2 = \frac{c_2 \alpha}{\beta}, \dots, \lambda_k = \frac{c_k \alpha}{\beta},$$

где $(c_i, p_i) = 1$ $(i = 1, 2, \dots, k)$. Кроме того, $\frac{N(\beta)\cdot\alpha}{\beta}$ есть также целое число. Вместе с тем числа $c_1, c_2, \dots, c_k, N(\beta)$ не имеют общих делителей, а потому неопределенное уравнение

$$c_1 x_1 + c_2 x_2 + \dots + c_k x_k + N(\beta) y = 1$$

имеет решение в целых рациональных числах. Поэтому

$$\frac{\alpha}{\beta} = \frac{\alpha}{\beta}[c_1 x_1 + c_2 x_2 + \dots + c_k x_k + N(\beta) y] =$$

$$= \lambda_1 x_1 + \lambda_2 x_2 + \dots + \lambda_k x_k + \frac{N(\beta)\alpha}{\beta} y$$

есть целое число, ч. и т. д.

Теорема 14. Если α и β p-взамно просты по всем p, входящим делителями одновременно в $N(\alpha)$ и $N(\beta)$, то они взаимно просты алгебраически, т. е. можно подобрать такие целые числа поля λ и μ, чтобы имело место

$$\alpha\lambda + \beta\mu = 1.$$

Доказательство. Пусть общий наибольший делитель чисел $N(\alpha)$ и $N(\beta)$ есть $d = p_1^{m_1} \cdot p_2^{m_2} \dots p_k^{m_k}$. В силу условия теоремы существуют такие числа ω_i, что

$$\alpha + \beta\omega_i = \varepsilon_i, \qquad (i = 1, 2, \dots, k),$$

где $N(\varepsilon_i)$ взаимно просты с p_i. Умножая эти равенства на целые числа $\frac{N(\varepsilon_i)}{\varepsilon_i}$ и меняя обозначения, получим:

$$\left.\begin{aligned} \alpha\rho_1 + \beta\sigma_1 &= N(\varepsilon_1) \\ \alpha\rho_2 + \beta\sigma_2 &= N(\varepsilon_2) \\ \dots\dots\dots\dots & \\ \alpha\rho_k + \beta\sigma_k &= N(\varepsilon_k), \end{aligned}\right\} \tag{3.15}$$

где ρ_i и σ_i $(i = 1, 2, \dots, k)$ — целые числа поля. Присоединим еще равенства

$$\left.\begin{aligned} \alpha \cdot \alpha' &= N(\alpha) \\ \beta \cdot \beta' &= N(\beta), \end{aligned}\right\} \tag{3.16}$$

где α', β' — тоже целые числа поля. Числа $N(\varepsilon_1), N(\varepsilon_2), \dots, N(\varepsilon_k)$, $N(\alpha)$, $N(\beta)$ не имеют общих делителей, а потому неопределенное уравнение

$$N(\varepsilon_1) \cdot x_1 + N(\varepsilon_2) x_2 + \dots + N(\varepsilon_k) x_k + N(\alpha) \cdot y_1 + N(\beta) \cdot y_2 = 1$$

имеет решение в целых рациональных числах. Умножая равенства (3.15) соответственно на $x_1, x_2, \ldots, x_k$, равенства (3.16) на y_1, y_2 и складывая, получим:

$$\alpha(\rho_1 x_1 + \rho_2 x_2 + \ldots + \rho_k x_k + \alpha' y_1) + \beta(\sigma_1 x_1 + \sigma_2 x_2 + \ldots + \sigma_k x_k + \beta' y_2) = 1,$$

что доказывает теорему.

Теорема 15. Число α определяется своим дивизором с точностью до алгебраической единицы.

Доказательство. Если два числа α и α' соответствуют одному и тому же дивизору, то они должны делиться друг на друга при всех p, входящих в $N(\alpha) = N(\alpha')$, а потому, в силу теоремы 13, они делятся друг на друга алгебраически. Таким образом и число ε и обратное к нему число $\frac{1}{\varepsilon}$ суть целые алгебраические числа. Такого рода числа ε называются *алгебраическими единицами*. Их можно охарактеризовать тем, что их норма (свободный член уравнения, которому они удовлетворяют) равна ± 1.

В дальнейшем для нас будет важна следующая теорема, показывающая, что дивизоры могут входить в числа поля независимо:

Теорема 16. Если даны дивизор $\mathfrak{a}$ и целое рациональное число M, то существуют также целые числа поля α, которые делятся на $\mathfrak{a}$, а их частные $\frac{\alpha}{\mathfrak{a}}$ являются взаимно простыми с M дивизорами.

Примечание. То обстоятельство, что в качестве M мы взяли целое рациональное число, нисколько не ограничивает теоремы. В самом деле, если бы нам вместо M было дано число поля или даже дивизор $\mathfrak{m}$, то, беря в роли M число $N(\mu)$ и соответственно $N(\mathfrak{m})$, мы только усилим эту теорему.

Доказательство. Сначала докажем эту теорему для входящего в $\mathfrak{a}$ простого дивизора $\mathfrak{P}$. Пусть π есть p-простое число, соответствующее дивизору $\mathfrak{P}$, и пусть $N(\mathfrak{P}) = p^k$, $N(\pi) = c \cdot p^k$, $(c, p) = 1$. Далее, пусть $M = M' \cdot p^m$, где M' — взаимно просто с p. Тогда число $\pi' = M' \cdot \pi + p^{k+1}$ будет удовлетворять условию теоремы. Действительно, мы имеем сравнения

$$N(\pi') \equiv N(p^{k+1}) \equiv p^{n(k+1)} (\mathrm{mod}\, M'), \quad N(\pi') \equiv M'^n \cdot c p^k (\mathrm{mod}\, p^{k+1}),$$

так что дивизор $\frac{\pi'}{\mathfrak{P}}$ будет иметь норму

$$\frac{N(\pi')}{N(\mathfrak{P})} \equiv p^{n(k+1)-k} (\mathrm{mod}\, M'), \quad \frac{N(\pi')}{N(\mathfrak{P})} \equiv M'^n \cdot c (\mathrm{mod}\, p),$$

которая взаимно проста с $M = M' \cdot p^n$.

Чтобы найти такого рода число для составного дивизора $\mathfrak{a}$, достаточно составить такие числа для каждого из его делителей, а затем перемножить их.

16. Данное нами понятие дивизора в общем совпадает с понятием *идеального числа*, предложенного Куммером (G. Kummer) и употреблявшегося в изложенном виде Е. И. Золотаревым. Слабая сторона этого понятия состоит в том, что дивизор определяется при помощи абстракции, и потому действия над дивизорами носят символический характер. Недостает предмета, которому соответствовал бы дивизор.

Этот недостаток был восполнен Дедекиндом (R. Dedekind), который ввел понятие *идеала*, как некоторой совокупности целых чисел поля, обладающей следующими двумя свойствами:

I. Сумма и разность двух чисел совокупности тоже лежит в этой совокупности.

II. Произведение числа совокупности на любое целое число поля опять дает число этой совокупности.

В поле целых рациональных чисел идеалом является совокупность чисел, делящихся на какое-нибудь число a. В этом поле не может быть идеалов других типов. В самом деле, возьмем в каком-нибудь идеале $\mathfrak{a}$ наименьшее число a, отличное от нуля. Тогда всякое другое число b идеала $\mathfrak{a}$ должно делиться на a, так как в противном случае остаток r от деления b на a был бы меньше a и в то же время, имея вид $r = b - aq$, входил бы в силу I и II в идеал $\mathfrak{a}$. С другой стороны, всякое делящееся на a число в силу II должно входить в $\mathfrak{a}$, и таким образом идеал $\mathfrak{a}$ состоит из всех целых рациональных чисел, делящихся на a.

В поле алгебраических чисел не всякий идеал можно представить как совокупность чисел, делящихся на одно число. В самом деле, в § 3, 2 мы видели пример чисел $\alpha = 3$, $\beta = 4 + \sqrt{-5}$, не имеющих общего делителя, но не взаимно простых (т. е. таких, что уравнение $\alpha\xi + \beta\eta = 1$ не может быть решено в целых числах ξ, η нашего поля). Совокупность чисел вида $\alpha\xi + \beta\eta$, где ξ, η пробегают все целые числа поля, очевидно составляет идеал. Однако все эти числа не могут быть представлены, как кратности одного числа. Те идеалы, для которых такое представление возможно, носят название *главных идеалов*.

Дедекинд определил понятия *общего наибольшего делителя и произведения идеалов*. *Делителем* идеала он называет идеал, содержащий, как часть, все числа данного идеала. Это понятие, в случае главных идеалов, приводит к обыкновенному понятию делимости чисел. Общим наибольшим же делителем двух идеалов называется наименьшая совокупность, являющаяся идеалом и содержащая оба данных идеала. Если оба идеала заданы базисами $[\alpha_1, \alpha_2, \ldots, \alpha_r]$ и $[\beta_1, \beta_2, \ldots, \beta_s]$, т. е. являются совокупностями $\alpha_1\xi_1 + \ldots + \alpha_r\xi_r$ и соответственно $\beta_1\eta_1 + \ldots +$

$+\beta_s\eta_s$, где $\xi_1, \xi_2, \ldots, \xi_r$; $\eta_1, \eta_2, \ldots, \eta_s$ пробегают все целые числа поля, то общий наибольший делитель этих идеалов имеет базисом $[\alpha_1, \alpha_2, \ldots, \alpha_r; \beta_1, \beta_2 \ldots, \beta_s]$.

Произведением двух идеалов $\mathfrak{a}$ и $\mathfrak{b}$ Дедекинд называет совокупность конечных сумм вида $\sum_i \alpha_i\beta_i$, где α_i пробегают всевозможные числа идеала $\mathfrak{a}$, а β_i — идеала $\mathfrak{b}$. Если же оба идеала заданы базисами $[\alpha_1, \alpha_2, \ldots, \alpha_r]$ и $[\beta_1, \beta_i, \ldots, \beta_s]$, то их произведение может быть задано базисом

$$[\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_1\beta_s; \alpha_2\beta_1, \alpha_2\beta_2, \ldots, \alpha_2\beta_s; \ldots; \alpha_r\beta_1, \alpha_r\beta_2, \ldots, \alpha_r\beta_s].$$

17. Нетрудно проверить, что совокупность целых чисел поля, делящихся на заданный дивизор $\mathfrak{a}$, является идеалом. Докажем обратное, т. е. что всякий идеал является совокупностью целых чисел поля, делящихся на некоторый дивизор. Пусть задан идеал $\mathfrak{a}$ и пусть $\bar{\mathfrak{a}} = p^{m_1}, p^{m_2}, p^{m_3}, \ldots p^{m_\kappa}$ есть дивизор, на который делятся все числа идеала $\mathfrak{a}$, причем пусть этот дивизор будет наибольший, в том смысле, что нет другого дивизора, делящегося на $\bar{\mathfrak{a}}$, на который бы делились все числа идеала $\mathfrak{a}$. Докажем, что всякое число, делящееся на дивизор $\bar{\mathfrak{a}}$, входит в идеал $\mathfrak{a}$. Для этого построим для идеала $\mathfrak{a}$ *базис*. Пусть $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ есть фундаментальный базис поля. Пусть $\mu_0 = a_{00}\omega_0$ будет входящее в $\mathfrak{a}$ число, имеющее возможно меньший целый рациональный коэфициент a_{00}. Идеал $\mathfrak{a}$ всегда содержит числа такого вида, так как, если в $\mathfrak{a}$ входит какое-нибудь число α, то в него в силу II входит $N(\alpha) = \alpha \cdot \alpha'$, а также $N(\alpha)\cdot\omega_0$. Если число вида $b\cdot\omega_0$ входит в $\mathfrak{a}$, то b должно делиться на a_{00}.

Далее найдем в идеале $\mathfrak{a}$ число вида $\mu_1 = a_{01}\omega_0 + a_{11}\omega_1$, в котором число a_{11} было бы возможно меньшим. Число a_{11} меньше $N(a)$, а число a_{01} — меньше a_{00}. Затем число вида $\mu_2 = a_{02}\omega_0 + a_{12}\omega_1 + a_{22}\omega_2$, в котором число a_{22} было бы возможно меньшим. Числа a_{02}, a_{12}, a_{22} опять следует выбирать среди конечного числа. Продолжая процесс, получим систему

$$\begin{aligned} \mu_0 &= a_{00}\omega_0 \\ \mu_1 &= a_{01}\omega_0 + a_{11}\omega_1 \\ &\cdots\cdots\cdots \\ \mu_{n-1} &= a_{0,n-1}\omega_0 + a_{1,n-1}\omega_1 + \ldots + a_{n-1,n-1}\omega_{n-1}. \end{aligned} \tag{3.17}$$

Докажем, что числа (3.17) образуют *базис идеала* $\mathfrak{a}$, т. е. что всякое число $\alpha = a_0\omega_0 + a_1\omega_1 + \ldots + a_{n-1}\omega_{n-1}$, входящее в идеал $\mathfrak{a}$, может быть представлено в виде $b_0\mu_0 + b_1\mu_1 + \ldots + b_{n-1}\mu_{n-1}$, где $b_0, b_1, \ldots, b_{n-1}$ — целые рациональные числа. В самом деле, a_{n-1} должно делиться на $a_{n-1,n-1}$, так как в противном случае, деля a_{n-1} на $a_{n-1,n-1}$ с остатком: $a_{n-1} = a_{n-1,n-1}\,a_{n-1} + r_{n-1}$ где $0 \leqq r_{n-1} < q$, мы получим число идеала $\alpha - q_{n-1}\mu_{n-1} = (a_0 - a_{0,n-1}q_{n-1})\omega_0 + \ldots + r_{n-1}\omega_{n-1}$, у которого коэфициент при ω_{n-1} меньше $a_{n-1,n-1}$, что противоречит определению μ_{n-1}. Положив $r_{n-1} = 0$, мы точно таким же образом убедимся, что у числа $\alpha - q_{n-1}\mu_{n-1}$ коэфициент при ω_{n-2} делится на $a_{n-2,n-2}$. Продолжая процесс, мы в конце концов получим:

$$\alpha - q_{n-1}\mu_{n-1} - q_{n-2}\mu_{n-2} - \ldots - q_0\omega_0 = 0,$$

где $q_{n-1}, q_{n-2}, \ldots, q_0$ — целые рациональные числа, ч. и т. д.

Пусть в нормы чисел базиса $\mu_0, \mu_1, \ldots, \mu_{n-1}$ входят множителями следующие простые числа: $p_1, p_2, \ldots, p_k$. Числа базиса $\mu_0, \mu_1, \ldots, \mu_{n-1}$ делятся по модулям этих чисел на общий дивизор $\bar{\mathfrak{a}}$, но не больший дивизор, так как в противном случае все числа идеала $\mathfrak{a}$, имея общим делителем дивизор $\bar{\mathfrak{a}}$, не могли бы выражаться через базис.

Пусть теперь α — произвольное целое число поля, делящееся на дивизор $\bar{\mathfrak{a}}$. Докажем, что оно входит в идеал $\mathfrak{a}$. Рассмотрим числа $\alpha, \mu_0, \mu_1, \ldots, \mu_{n-1}$ по одному из простых модулей p_i. Числа $\mu_0, \mu_1, \ldots, \mu_{n-1}$ имеют общий наибольший p_i делитель, соответствующий тому дивизору делителя дивизора $\bar{\mathfrak{a}}$, простые множители которого являются делителями числа p_i. На этот дивизор делится и α, и потому имеет место

$$c_i\alpha = \xi_{0i}\mu_0 + \xi_{1i}\mu_1 + \ldots + \xi_{n-1,i}\mu_{n-1}, \quad (i = 1, 2, \ldots, k) \tag{3.18}$$

где ξ_{jl} — целые числа поля и $(c_i, p_i) = 1$. Кроме того, $N(\mu_0)$ и потому $N(\mu_0)\cdot\alpha$ является числом идеала $\bar{\mathfrak{a}}$, причем $N(\mu_0)$ содержит только $p_1, p_2, \ldots, p_k$ в качестве простых делителей. Поэтому

$$N(\mu_0)\alpha = a_0\mu_0 + a_1\mu_1 + \ldots + a_{n-1}\mu_{n-1}, \tag{3.19}$$

где $a_0, a_1, \ldots, a_{n-1}$ — целые рациональные числа. Вместе с тем $c_1, c_2, \ldots, c_k$, $N(\mu_0)$ имеют общим множителем единицу, а поэтому неопределенное уравнение

$$c_1x_1 + c_2x_2 + \ldots + c_kx_k + N(\mu_0)y = 1$$

имеет решение в целых рациональных числах. Умножая (3.18) на x_i, суммируя и складывая с (3.19), умноженным на y, получим:

$$\alpha = \eta_0\mu_0 + \eta_1\mu_1 + \ldots + \eta_{n-1}\mu_{n-1},$$

где $\eta_0, \eta_1, \ldots, \eta_{n-1}$ — некоторые числа поля. Это равенство показывает, что α входит в идеал $\mathfrak{a}$, ч. и т. д.

Таким образом мы видим, что понятие идеала по существу не отличается от понятия дивизора, так что, говоря об идеалах, мы можем применять к ним все результаты, полученные нами относительно дивизоров. Докажем еще одну теорему:

Теорема 17. Всякий идеал можно представить в *двучленной* форме $[\lambda, \mu]$, т. е. можно найти числа λ и μ

такого рода, что всякое число идеала может быть представлено в форме $\lambda\xi+\mu\eta$, где ξ, η — целые числа поля.

Доказательство основано на теореме 16. В качестве λ можно взять произвольное число идеала, а в качестве μ—такое число, делящееся на дивизор $\bar{a}$, соответствующий заданному идеалу, чтобы частное $\mu:\bar{a}$ было взаимно просто с λ [или даже с $N(\lambda)$]. Тогда общим наибольшим делителем чисел λ, μ будет точно дивизор $\bar{a}$, откуда, повторяя предыдущие рассуждения, нетрудно доказать, что всякое целое число поля, делящееся на дивизор $\bar{a}$, может быть представлено в форме $\lambda\xi+\mu\eta$, где ξ, η — целые числа поля.

§ 4. Сравнения по идеальным модулям

1. Два целых числа α, β поля называются *сравнимыми* по модулю идеала $\mathfrak{a}$:

$$\alpha\equiv\beta \pmod{\mathfrak{a}}, \tag{4.1}$$

если их разность $\alpha-\beta$ есть число идеала $\mathfrak{a}$ (или, что то же, делится на дивизор, соответствующий идеалу $\mathfrak{a}$).

2. Докажем, что над сравнениями можно производить те же операции, что и над обыкновенными равенствами (см. часть I, Прибавление).

I. Из

$$\alpha\equiv\beta,\ \gamma\equiv\delta \pmod{\mathfrak{a}}$$

следует

$$\alpha\pm\gamma\equiv\beta\pm\delta \pmod{\mathfrak{a}}$$

$$\alpha\gamma\equiv\beta\delta \pmod{\mathfrak{a}}.$$

Первое из этих сравнений вытекает из того, что $\alpha-\beta$ и $\gamma-\delta$ принадлежат к идеалу $\mathfrak{a}$, и в силу указанного свойства I идеала к нему принадлежат и их сумма и разность $(\alpha\pm\beta)-(\beta\pm\delta)$.

Второе сравнение вытекает из тождества

$$\alpha\gamma-\beta\delta=\alpha(\gamma-\delta)+\delta(\alpha-\beta).$$

Его правая часть принадлежит к $\mathfrak{a}$ в силу свойств I и II.

Применяя эти два равенства любое число раз, мы придем к следующему свойству сравнений:

II. Из

$$\alpha\equiv\beta \pmod{\mathfrak{a}},$$

вытекает

$$f(\alpha)\equiv f(\beta) \pmod{\mathfrak{a}},$$

где $f(x)$ — произвольный полином с целыми числами поля в качестве коэфициентов.

В случае, если $\mathfrak{a}=\mathfrak{P}$ есть простой идеал, имеют место также следующие свойства:

III. Если

$$\alpha\cdot\beta\equiv 0 \pmod{\mathfrak{P}},$$

то или $\alpha\equiv 0 \pmod{\mathfrak{P}}$ или $\beta\equiv 0 \pmod{\mathfrak{P}}$.

IV. Сравнение

$$f(\xi)\equiv 0 \pmod{\mathfrak{P}} \tag{4.2}$$

n-ой степени может иметь внутри поля не более n корней, если корни, сравнимые между собой по модулю $\mathfrak{P}$, не считать различными.

В самом деле, если α есть корень сравнения (4.2), то остаток $\mathfrak{P}$ от деления $f(\xi)$ на $\xi-\alpha$ делится на $\mathfrak{P}$ (т. е. есть число идеала $\mathfrak{P}$). Это следует из того, что $f(\xi)=Q(\xi)(\xi-\alpha)+R$ и $f(\alpha)\equiv 0 \pmod{\mathfrak{P}}$. Подставляя $\xi=\alpha$, получим:

$$R=f(\alpha)\equiv 0 \pmod{\mathfrak{P}}.$$

Предположив, что сравнение (4.2) имеет $n+1$ корней α_0, $\alpha_1,\ldots,\alpha_{n-1}$, и последовательно применяя упомянутое соображение, мы представим полином $f(\xi)$ в виде

$$f(\xi)\equiv a_0(\xi-\alpha_1)(\xi-\alpha_2)\ldots(\xi-\alpha_n) \pmod{\mathfrak{P}}.$$

Но так как α_0 является корнем сравнения (4.2), то один из множителей $\alpha_0-\alpha_i\,(i=1,2,\ldots,n)$ должен делиться на $\mathfrak{P}$, что противоречит нашему предположению.

3. Объединяя числа, сравнимые друг с другом по модулю $\mathfrak{a}$, в *классы сравнений*, поставим задачу нахождения числа классов сравнений по модулю $\mathfrak{a}$. Здесь имеет место

Теорема 18. Число классов сравнений по идеальному модулю $\mathfrak{a}$ равно абсолютной величине нормы идеала $\mathfrak{a}$.

Доказательство мы расчленим на несколько частей.

1. Если $[\mu_0,\mu_1,\ldots,\mu_{n-1}]$ есть базис идеала $\mathfrak{a}$, то число классов по модулю $\mathfrak{a}$ равно определителю подстановки

$$\begin{aligned}
\mu_0&=a_{00}\omega_0+a_{01}\omega_1+\ldots+a_{0,n-1}\omega_{n-1},\\
\mu_1&=a_{10}\omega_0+a_{11}\omega_1+\ldots+a_{1,n-1}\omega_{n-1},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
\mu_{n-1}&=a_{n-1,0}\omega_0+a_{n-1,1}\omega_1+\ldots+a_{n-1,n-1}\omega_{n-1}.
\end{aligned}$$ [1]

[1] $[\omega_0,\omega_1,\ldots,\omega_{n-1}]$ есть фундаментальный базис поля.

Мы видели в § 3.17, что этот базис можно выбрать в виде

$$\begin{aligned}
\mu_0 &= a_{00}\,\omega_0 \\
\mu_1 &= a_{10}\,\omega_0 + a_{11}\,\omega_1 \\
&\cdots\cdots\cdots \\
\mu_{n-1} &= a_{n-1,0}\,\omega_0 + a_{n-1,1}\,\omega_1 + \ldots + a_{n-1,n-1}\,\omega_{n-1}.
\end{aligned} \tag{4.3}$$

Нетрудно убедиться, что представителями классов по модулю $\mathfrak{a}$ могут служить следующие числа:

$$c_0\,\omega_0 + c_1\,\omega_1 + \ldots + c_{n-1}\,\omega_{n-1}, \tag{4.4}$$

где c_i пробегает значения $0, 1, 2, \ldots, |a_{ii}| - 1$ $(i = 0, 1, \ldots, n-1)$. Действительно, с одной стороны, всякое число поля может быть последовательным прибавлением кратностей μ_{n-1}, $\mu_{n-2}, \ldots, \mu_1$, μ_0 приведено к виду (4.4). С другой стороны, два числа вида (4.4) не могут иметь разность, входящую в идеал $\mathfrak{a}$, т. е. представляемую через базис (4.3), так как, если эта разность равна $f_0\,\omega_0 + f_1\,\omega_1 + \ldots + f_i\,\omega_i$, где $f_i \neq 0$, то $|f_i| < |a_{ii}|$, а потому она не может входить в $\mathfrak{a}$, так как, согласно данному в § 3.17 определению, $|a_{ii}|$ есть наименьшее из чисел $|f_i|$ такого рода, что $f_0\,\omega_0 + f_1\,\omega_1 + \ldots + f_i\,\omega_i$ входит в $\mathfrak{a}$. Число представителей (4.4) равно $|a_{00}\,a_{11}\ldots a_{n-1,n-1}|$, т. е. определителю подстановки (4.3).

Утверждение справедливо также для случая произвольного базиса, так два различных базиса одного и того же идеала переходят друг в друга при помощи целочисленных подстановок, произведение которых равно тождественной подстановке, в силу чего определители этих подстановок должны быть равны ± 1.

2. Теорема 18 справедлива для случая главного идеала. Действительно, если $\mathfrak{a}$ есть совокупность чисел, делящихся на числа α, то его базисом служит $[\alpha\omega_0, \alpha\omega_1, \ldots \alpha\omega_{n-1}]$. Поэтому число классов по модулю $\mathfrak{a}$ равно определителю подстановки

$$\begin{aligned}
\alpha\omega_0 &= c_{00}\,\omega_0 + c_{01}\,\omega_1 + \ldots + c_{0,n-1}\,\omega_{n-1} \\
\alpha\omega_1 &= c_{10}\,\omega_0 + c_{11}\,\omega_1 + \ldots + c_{1,n-1}\,\omega_{n-1} \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
\alpha\omega_{n-1} &= c_{n-1,0}\,\omega_0 + c_{n-1,1}\,\omega_1 + \ldots + c_{n-1,n-1}\,\omega_{n-1}.
\end{aligned}$$

Но из этих соотношений можно получить для α следующее уравнение:

$$\begin{vmatrix}
c_{00} - \alpha, & c_{01}, \ldots, & c_{0,n-1} \\
c_{10}, & c_{11} - \alpha, \ldots, & c_{1,n-1} \\
\cdots\cdots & \cdots\cdots & \cdots\cdots \\
c_{n-1,0}, & c_{n-1,1}, \ldots, & c_{n-1,n-1} - \alpha
\end{vmatrix} = 0,$$

откуда следует, что $|N(\alpha)|$ равно этому самому определителю.

3. Теорема 18 справедлива для случая простого идеала. В самом деле, пусть простой идеал $\mathfrak{P}$ есть делитель простого

числа p, и пусть соответствующее ему p-простое число есть π. Идеал $\mathfrak{P}$ состоит из чисел, p-делящихся на π. Если $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$ есть базис идеала $\mathfrak{P}$, то для каждого $\mu_i = a_{i0}\,\omega_0 + a_{i1}\,\omega_1 + \ldots + a_{ii}\,\omega_i$ число $|a_{ii}|$ есть степень p. Действительно, если бы $a_{ii} = cp^k$, где $(c, p) = 1$ и $c > 1$, то, решая уравнение $cx + py = 1$ в целых рациональных числах, мы бы пришли к числу $\mu_i x + p^{k+1}\,\omega_i y = a_{i0}\,x\,\omega_0 + a_{i1}\,x\,\omega_1 + \ldots + p^k\,\omega_i$ идеала $\mathfrak{P}$ (так как p тоже входит в $\mathfrak{P}$), у которого координата при ω_i будет меньше, чем a_{ii}, а это противоречит данному в § 3.17 определению числа μ_i. Таким образом здесь определитель подстановки (4.3) равен степени числа p.

Вместе с тем этот определитель отличается от $N(\pi)$ множителем, взаимно простым с p. Действительно, существуют такие взаимно простые с p числа $c_0, c_1, \ldots, c_{n-1}$, что числа $c_0\mu_0, c_1\mu_1, \ldots, c_{n-1}\mu_{n-1}$ делятся на π, а потому каждое из них выражается через $[\pi\omega_0, \pi\omega_1, \ldots, \pi\omega_{n-1}]$. Таким образом определитель подстановки, переводящей в $[c_0\mu_0, c_1\mu_1, \ldots, c_{n-1}\mu_{n-1}]$ базис $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$, делится на $N(\pi)$. С другой стороны, $N(\pi)$ в силу той же причины делится на определитель подстановки, переводящей $[\omega_0, \omega_1 \ldots, \omega_{n-1}]$ в $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$, на число классов по модулю $\mathfrak{P}$, которое отличается взаимно простым с p множителем $c_0 c_1 \ldots c_{n-1}$ от определителя подстановки, переводящей $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ в $[c_0\mu_0, c_1\mu_1, \ldots, c_{n-1}\mu_{n-1}]$. Поэтому число классов по модулю $\mathfrak{P}$ равно наибольшей степени p, входящей в $N(\pi)$, т. е., согласно определению нормы простого идеала, $N(\mathfrak{P})$.

4. Чтобы распространить теорему 18 на произвольные идеалы, достаточно доказать:

Число классов по модулю $\mathfrak{a}\,\mathfrak{P}$ равно произведению чисел классов по модулю $\mathfrak{a}$ и по модулю $\mathfrak{P}$.

Пусть $\alpha_1, \alpha_2, \ldots, \alpha_r$ будут представители классов по модулю $\mathfrak{a}$ и $\beta_1, \beta_2, \ldots, \beta_s$ — по модулю $\mathfrak{P}$. Докажем, что числа

$$\alpha_i + \alpha \cdot \beta_j \qquad (i = 1, 2, \ldots, r,\ j = 1, 2, \ldots, s) \tag{4.5}$$

могут служить представителями классов по модулю $\mathfrak{a}\,\mathfrak{P}$, если выбрать число α так, чтобы оно делилось на $\mathfrak{a}$ и чтобы частное $\frac{\alpha}{\mathfrak{a}}$ было взаимно просто с $N(\mathfrak{a}, \mathfrak{P})$ (см. теорему 16). Действительно, с одной стороны, всякое целое число поля ω сравнимо по модулю $\mathfrak{a}\,\mathfrak{P}$ с одним из чисел (4.5).

В самом деле, пусть ω сравнимо с представителем α_i по модулю $\mathfrak{a}$. Число $c\frac{\omega - \alpha_i}{\mathfrak{a}}$ есть целое, где c — некоторое взаимно простое с $N(\mathfrak{a}, \mathfrak{P})$ число. Если

$$c \cdot \frac{\omega - \alpha_i}{\mathfrak{a}} \equiv \beta_j \pmod{\mathfrak{P}},$$

то, решая неопределенное уравнение

$$cx = 1 + N(\mathfrak{P})y,$$

мы получаем

$$c \cdot \frac{\omega - \alpha_i}{\alpha} \equiv \beta_j \pmod{\mathfrak{P}},$$

причем β_j сравнимо с некоторым $c \cdot \beta_u$. Отсюда следует, что $c(\omega - \alpha_i - \alpha\beta_u)$ входит в идеал $\mathfrak{a}\mathfrak{P}$. Но так как c взаимно просто с $N(\mathfrak{a}\mathfrak{P})$, то

$$\omega \equiv \alpha_i + \alpha\beta_u \pmod{\mathfrak{a}\mathfrak{P}}.$$

С другой стороны, числа (4.5) несравнимы друг с другом по модулю $\mathfrak{a}\mathfrak{P}$. В самом деле, если бы, например, имело место

$$\alpha_i + \alpha\beta_j \equiv \alpha_u + \alpha\beta_\nu \pmod{\mathfrak{a}\mathfrak{P}},$$

то отсюда бы следовало

$$\alpha_i \equiv \alpha_u \pmod{\mathfrak{P}},$$

т. е. $u = i$. Далее, из

$$\alpha(\beta_j - \beta_\nu) \equiv 0 \pmod{\mathfrak{a}\mathfrak{P}}$$

следует $\beta_j - \beta_\nu \equiv 0 \pmod{\mathfrak{P}}$, т. е. $j = \nu$. Таким образом число классов по модулю $\mathfrak{a}\mathfrak{P}$ равно числу чисел (4.5), т. е. rs, ч. и т. д.

Это позволяет считать теорему 18 вполне доказанной.

4. Распространим на случай простого идеала теорему Ферма:

Теорема 19. Если для простого идеала $\mathfrak{P}$ $N(\mathfrak{P}) = p^f$, [1]) то для всякого целого числа поля ξ имеет место

$$\xi^{p^f} \equiv \xi \pmod{\mathfrak{P}}. \tag{4.6}$$

Доказательство. Пусть $0, \alpha_1, \alpha_2, \ldots, \alpha_{s-1}$ $(s = p^f)$ будут представители всех классов по модулю $\mathfrak{P}$. Так как $\mathfrak{P}$ есть простой идеал, то все представители, кроме 0, взаимно просты с $\mathfrak{P}$. Поэтому, если ξ произвольное взаимно простое с $\mathfrak{P}$ число, то числа $\xi\alpha_1, \xi\alpha_2, \ldots, \xi\alpha_{s-1}$ сравнимы по модулю $\mathfrak{P}$ с числами $\alpha_1, \alpha_2, \ldots, \alpha_{s-1}$, взятыми может быть в другом порядке:

$$\xi\alpha_1 \equiv \alpha_{k_1}, \ \xi\alpha_2 \equiv \alpha_{k_2}, \ldots, \xi\alpha_{s-1} \equiv \alpha_{k_{s-1}} \pmod{\mathfrak{P}}.$$

Перемножая эти сравнения, получим

$$\alpha_1\alpha_2, \ldots, \alpha_{s-1}(\xi^{s-1} - 1) \equiv 0 \pmod{\mathfrak{P}}.$$

Но так как $\alpha_1\alpha_2, \ldots, \alpha_{s-1}$ взаимно просто с $\mathfrak{P}$, то имеет место

$$\xi^{p^f - 1} \equiv 1 \pmod{\mathfrak{P}}. \tag{4.6}$$

[1]) p^f называется *степенью* простого идеала.

Умножая на ξ, получим сравнение (4.5), которое имеет место также для делящихся на $\mathfrak{P}$.

5. Теорема 20. Если $N(\mathfrak{P}) = p$ (идеал $\mathfrak{P}$ первой степени), то всякое целое число поля сравнимо по модулю $\mathfrak{P}$ с рациональным числом.

Действительно, в этом случае в качестве представителей классов можно выбрать числа $0, 1, \ldots, p-1$, так как разности этих чисел, будучи меньше p, взаимно просты с p, а число этих чисел в силу теоремы 18 равно числу классов по модулю $\mathfrak{P}$.

6. Рассмотрим случай *нормального* поля. Пусть $\mathfrak{P}$ есть простой идеал в нормальном поле K и пусть $N(\mathfrak{P}) = p^f$. Будем обозначать через α^S величину поля K, получаемую из величины α путем применения к ней автоморфизма S группы Галуа поля K. В силу нормальности поля K, наряду с α в поле K входят все величины α^S. Подобным же образом определяется и идеал $\mathfrak{a}^S$ из идеала $\mathfrak{a}$: если $\mathfrak{a}$ есть совокупность чисел $\alpha, \beta, \gamma, \ldots$, то идеал $\mathfrak{a}^{S-1}$ есть совокупность чисел $\alpha^{S-1}, \beta^{S-1}, \gamma^{S-1}, \ldots$

Если $\mathfrak{P}$ есть простой идеал, то и $\mathfrak{P}^{S-1}$ есть простой идеал, так как в противном случае, применяя подстановку S^{-1} к равенству $\mathfrak{P}\mathfrak{b} = \mathfrak{a} \cdot \mathfrak{b}$, мы придем к равенству $\mathfrak{P} = \mathfrak{a}^{S-1} \cdot \mathfrak{b}^{S-1}$, противоречащему простоте идеала $\mathfrak{P}$.

При применении автоморфизмов группы Галуа нормы идеалов остаются неизменными, так как системы представителей классов $\alpha_1, \alpha_2, \ldots, \alpha_s$ по модулю $\mathfrak{a}$ для модуля $\mathfrak{a}^{S-1}$ превращаются в систему $\alpha_1^{S-1}, \alpha_2^{S-1}, \ldots, \alpha_s^{S-1}$, обладающую теми же свойствами для своего модуля.

В нормальных полях норма идеала может быть определена иначе. Чтобы показать это, докажем

Теорему 21. Норма идеала в нормальном поле равна произведению идеалов, сопряженных с данным.

Доказательство. Достаточно доказать теорему для простого идеала $\mathfrak{P}$. Выберем делящееся на $\mathfrak{P}$ число π такого рода, чтобы идеал $\pi/\mathfrak{P}$ был взаимно прост с $N(\mathfrak{P}) = p^f$. Если

$$\mathfrak{G} = 1 + S_2 + \ldots + S_n$$

есть группа Галуа поля, то $\pi \cdot \pi^{s_2} \ldots \pi^{s_n} = N(\pi)$. Выделим из обеих частей все идеальные множители, являющиеся делителями числа p. В левой части это очевидно будет $\mathfrak{P} \cdot \mathfrak{P}^{s_2} \ldots \mathfrak{P}^{s_n}$; в правой же, в силу определения нормы простого идеала и того, что π есть p-простое число, мы получим $N(\mathfrak{P})$. Поэтому

$$\mathfrak{P}\mathfrak{P}^{s_2} \ldots \mathfrak{P}^{s_n} = N(\mathfrak{P}). \tag{4.7}$$

§ 5. Критические простые числа и дискриминант поля

1. Теперь мы можем доказать в общем виде

Теорему 12. Чтобы простое число p было критическим для поля K, необходимо и достаточно, чтобы оно было делителем дискриминанта поля K.

Доказательство. 1. Условие необходимо. В самом деле, пусть для поля K простое число p есть критическое, т. е. пусть простой идеал $\mathfrak{P}$ входит в p делителем выше, чем в первой степени. Тогда квадрат числа α, делящегося на $\frac{p}{\mathfrak{P}}$, но не на p, делится на p.

Если выразить α через фундаментальный базис:

$$\alpha = x_0\omega_0 + x_1\omega_1 + \ldots + x_{n-1}\omega_{n-1}, \tag{5.1}$$

то не все x_i делятся на p, так как в противном случае α делилось бы на p. Пусть $x_s \not\equiv 0 \pmod p$. С другой стороны, $\frac{\alpha^2}{p}$ и потому и $\frac{\alpha}{\sqrt{p}}$ суть целые алгебраические числа, а потому $\frac{S(\alpha)}{\sqrt{p}}$ есть целое алгебраическое число. Но так как $S(\alpha)$ рационально, то оно должно делиться на p. Сказанное имеет место также для чисел

$$\omega_0\alpha,\ \omega_1\alpha,\ \ldots,\ \omega_{n-1}\alpha,$$

в силу чего

$$\left.\begin{aligned} S(\omega_0\alpha) &= S(\omega_0^2)x_0 + S(\omega_0\omega_1)x_1 + \ldots + \\ &+ S(\omega_0\omega_{n-1})x_{n-1} \equiv 0 \pmod p, \\ S(\omega_1\alpha) &= S(\omega_1\omega_0)x_0 + S(\omega_1^2)x_1 + \ldots + \\ &+ S(\omega_1\omega_{n-1})x_{n-1} \equiv 0 \pmod p, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ S(\omega_{n-1}\alpha) &= S(\omega_{n-1}\omega_0)x_0 + S(\omega_{n-1}\omega)x_1 + \ldots + \\ &+ S(\omega^2_{n-1})x_{n-1} \equiv 0 \pmod p. \end{aligned}\right\} \tag{5.2}$$

Определитель этой системы сравнений есть дискриминант Δ поля K. Обозначим его миноры так: Σ_{ij}. Умножая сравнения (5.2) соответственно на $\Sigma_{s0},\ \Sigma_{s1},\ \ldots,\ \Sigma_{s,\,n-1}$ и складывая, получим

$$\Delta \cdot x_s \equiv 0 \pmod p, \tag{5.3}$$

откуда в силу $x_s \not\equiv 0 \pmod p$ имеем $\Delta \equiv 0 \pmod p$, ч. и т. д.

2. Теперь предположим, что $\Delta \equiv 0 \pmod p$, и докажем, что p есть критическое простое число поля K. Δ есть квадрат определителя

$$\delta = \begin{vmatrix} \omega_0, & \omega_1, & \ldots, & \omega_{n-1} \\ \omega_0', & \omega_1', & \ldots, & \omega'_{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ \omega_0^{(n-1)}, & \omega_1^{(n-1)}, & \ldots, & \omega_{n-1}^{(n-1)} \end{vmatrix}, \tag{5.4}$$

который в силу предположения делится на $\sqrt{p}$. Элементы определителя δ являются сопряженными с ω_i и потому лежат в нормальном поле K, составленном из всех сопряженных с K полей (норма поля K). Пусть $\mathfrak{P}$ есть простой идеальный множитель числа p, и пусть $\mathfrak{P}^{S_2}, \mathfrak{P}^{S_3}, \ldots, \mathfrak{P}^{S_k}$ все различные между собой идеалы, сопряженные с $\mathfrak{P}$. Произведение $\mathfrak{G} = \mathfrak{P}\cdot\mathfrak{P}^{S_2}\ldots\mathfrak{P}^{S_k}$ является идеалом, инвариантным относительно всех автоморфизмов группы Галуа $\mathfrak{G}$ поля K. δ делится на $\mathfrak{G}$. С другой стороны, из теоремы 21 вытекает, что $N(\mathfrak{P})$, а потому и p, является делителем некоторой степени $\mathfrak{G}$.

Рассмотрим систему сравнений

$$\left.\begin{aligned} \omega_0\xi_0 + \omega_1\xi_1 + \ldots + \omega_{n-1}\xi_{n-1} &\equiv 0 \pmod{\mathfrak{G}} \\ \omega_0'\xi_0 + \omega_1'\xi_1 + \ldots + \omega'_{n-1}\xi_{n-1} &\equiv 0 \pmod{\mathfrak{G}} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ \omega_0^{(n-1)}\xi_0 + \omega_1^{(n-1)}\xi_1 + \ldots + \omega_{n-1}^{(n-1)}\xi_{n-1} &\equiv 0 \pmod{\mathfrak{G}}. \end{aligned}\right\} \tag{5.5}$$

Ее можно решить в целых числах $\xi_0,\ \xi_1,\ \ldots,\ \xi_{n-1}$ поля K, не делящихся на $\mathfrak{G}$.

В самом деле, пусть все миноры $(s+1)$-го порядка определителя δ этой системы делятся на $\mathfrak{G}$, в то время как по крайней один из миноров s-го порядка, например

$$\begin{vmatrix} \omega_0, & \omega_1, \ldots, & \omega_{s-1} \\ \omega_0', & \omega_1', \ldots, & \omega'_{s-1} \\ \ldots & \ldots & \ldots \\ \omega_0^{(s-1)}, & \omega_1^{(s-1)}, \ldots, & \omega_{s-1}^{(s-1)} \end{vmatrix}, \tag{5.6}$$

пусть не делится на $\mathfrak{G}$. Тогда, вводя обозначение

$$\begin{vmatrix} \omega_0, & \omega_1, \ldots, & \omega_{s-1}, & \omega_s \\ \omega_0', & \omega_1, \ldots, & \omega'_{s-1}, & \omega_s' \\ \ldots & \ldots & \ldots & \ldots \\ \omega_0^{(s-1)}, & \omega_1^{(s-1)}, \ldots, & \omega_{(s-1)}^{(s-1)}, & \omega_s^{(s-1)} \\ u_0, & u_1, \ldots, & u_{s-1}, & u_s \end{vmatrix} = A_0u_0 + A_1u_1 + \ldots + A_su_s,$$

где $A_s \not\equiv 0 \pmod{\mathfrak{G}}$, мы увидим, что при $u_0 = \omega_0^{(i)}$, $u_1 = \omega_1^{(i)}$, ..., $u_s = \omega_s^{(i)}$ $(i = 0, 1, \ldots, n-1)$ эта форма получает значения, делящиеся на $\mathfrak{G}$.

Поэтому в качестве решения системы (5.5) достаточно взять

$$\xi_0 = A_0,\ \xi_1 = A_1,\ \ldots,\ {}_s = A_s,\ \xi_{s+1} = 0,\ \ldots,\ \xi_{n-1} = 0. \tag{5.7}$$

Из решения $[\xi_0, \xi_1, \ldots, \xi_{n-1}]$ можно получить другое, в котором ξ_s есть целое рациональное число, взаимно простое с p. Для этого мы обратим внимание на то, что, применяя к системе (5.5) любую подстановку группы Галуа, мы не изменим системы, так как левые части сравнений поменяются между собой,

а модуль $\mathfrak{G}$ останется инвариантным. Поэтому наряду с $[\xi_0, \xi_1, \ldots, \xi_{n-1}]$ решения $[\xi_0^S, \xi_1^S, \ldots, \xi_{n-1}^S]$, где S—любой автоморфизм группы Галуа, тоже удовлетворяют сравнениям (5,5). Пусть ξ_s не делится на простой идеальный делитель $\mathfrak{P}$ идеала $\mathfrak{G}$. Тогда $\xi_s^{S_2}, \ldots, \xi_s^{S_k}$ не будет делиться соответственно на $\mathfrak{P}^{S_2}, \mathfrak{P}^{S_3}, \ldots, \mathfrak{P}^{S_k}$, а потому мы можем подобрать такие множители $\lambda_1 \lambda_2, \ldots, \lambda_k$, чтобы $\sum_i \lambda_i \xi_s^{S_k}$ было взаимно простым с $\mathfrak{G}$, т. е. с p.

Таким образом решение $[\eta_0, \eta_1, \ldots, \eta_{n-1}] = \left[\sum_i \lambda_i \xi_0^{S_i}, \sum_i \lambda_i \xi_1^{S_i}, \ldots, \sum_i \lambda_i \xi_{n-1}^{S_i}\right]$ имеет η_s, взаимно простое с p. Умножая решение на $\frac{N(\eta_s)}{\eta_s}$, мы придем к решению $[\zeta_0, \zeta_1, \ldots, \zeta_{n-1}]$, в котором ζ_0 есть взаимно простое с p целое рациональное число, а $\zeta_{s+1} = \ldots = \zeta_{n-1} = 0$.

Решения этого типа единственны с точностью до взаимно простого с p рационального множителя. В самом деле, если $[\rho_0, \rho_1, \ldots, \rho_{n-1}]$ есть другое решение этого типа системы (5.5), то, подбирая рациональные множители $\lambda_1 \mu$ так, чтобы имело место $\lambda\zeta_s + \mu\rho_s = 0$, где λ и μ взаимно просты с p, и вводя обозначение $\sigma_i = \lambda\zeta_i + \mu\rho_i$, мы получим решение $[\sigma_0, \sigma_1, \ldots, \sigma_{n-1}]$, в котором $\sigma_s = \sigma_{s+1} = \ldots = \sigma_{n-1} = 0$. Это решение является также решением системы

$$\omega_0^{(i)}\xi_0 + \omega_1^{(i)}\xi_1 + \ldots + \omega_{s-1}^{(i)}\xi_{s-1} \equiv 0 \pmod{\mathfrak{G}} \quad (i = 0, 1, \ldots n-1), \tag{5.8}$$

определитель которой (5.6) не делится $\mathfrak{G}$. Эта система тоже инвариантна относительно автоморфизмов группы Галуа. Поэтому, если предположить, что в решении $[\sigma_0, \sigma_1, \ldots, \sigma_{s-1}]$ одно из чисел не делится на $\mathfrak{G}$, то мы сможем найти такое же решение, в котором одно из чисел взаимно просто с p. Но, беря из системы (5.8) первые s сравнений и рассуждая как в n° 1, мы докажем, что ни одно из чисел $\sigma_0, \sigma_1, \ldots, \sigma_{n-1}$ не может быть взаимно просто с $\mathfrak{G}$. Следовательно система (5.5) допускает единственное решение $[\zeta_0, \zeta_1, \ldots, \zeta_{n-1}]$ (с точностью до взаимно простого с p рационального множителя), в котором ζ равно взаимно простому с p целому рациональному числу, а $\zeta_{s+1} = \ldots = \zeta_{n-1} = 0$.

Возьмем произвольный автоморфизм S группы Галуа поля K. $[\zeta_0^S, \zeta_1^S, \ldots, \zeta_{n-1}^S]$ является тоже, как мы видели, решением системы (5.5). В нем тоже $\zeta_{s+1}^S = \ldots = \zeta_{n-1}^S = 0$, а $\zeta_s^S = \zeta_s$, в силу чего

$$\zeta_0^S \equiv \zeta_0, \quad \zeta_1^S \equiv \zeta_1, \ldots, \zeta_{s-1}^S \equiv \zeta_{s-1} \pmod{\mathfrak{G}}, \tag{5.9}$$

где S—любой автоморфизм группы Галуа $\mathfrak{G}$ поля K.

Докажем, что каждое из чисел $\zeta_0, \zeta_1, \ldots, \zeta_{s-1}$ сравнимо по модулю $\mathfrak{G}$ с целым рациональным числом. Для этого воспользуемся первой теоремой Силова (Sylow), которую мы докажем в этом же параграфе:

Всякая конечная группа порядка $p^m \cdot u$, где p—простое число и $(u, p) = 1$, содержит подгруппу порядка p^m.

Пусть порядок группы $\mathfrak{G}$ равен $p^m \cdot u$. Обозначим через

$$\mathfrak{H} = 1 + T_2 + \ldots + T_{p^m}$$

ее подгруппу порядка p^m. Если ζ—одно из чисел, удовлетворяющих сравнениям (5.9), то имеет место

$$\eta = \zeta \cdot \zeta^{T_2}, \ldots, \zeta^{T_{p^m}} \equiv \zeta^{p^m} \pmod{\mathfrak{G}}, \tag{5.10}$$

причем η инвариантно относительно автоморфизмов группы $\mathfrak{H}$. Но в силу обобщенной теоремы Ферма (§ 4.4) мы имеем:

$$\zeta^{p^f} \equiv \zeta \pmod{\mathfrak{P}},$$

а в силу инвариантности ζ, по модулю $\mathfrak{G}$ также

$$\zeta^{p^f} \equiv \zeta \pmod{\mathfrak{G}}. \tag{5.11}$$

Разделим m на f с *отрицательным* остатком:

$$m = fq - r, \qquad (0 \leqq r < f).$$

Тогда в силу (5.11) имеем:

$$\zeta \equiv \zeta^{p^f} \equiv \zeta^{p^{2f}} \equiv \ldots \equiv \zeta^{p^{qf}} \equiv \zeta^{p^m} p^r \pmod{\mathfrak{G}}$$

и в силу (5.10)

$$\zeta = \eta^{p^r} \pmod{\mathfrak{G}}. \tag{5.12}$$

Чтобы доказать, что η сравнимо по модулю $\mathfrak{G}$ с рациональным числом, разложим $\mathfrak{G}$ по $\mathfrak{H}$:

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H}S_2 + \ldots + \mathfrak{H}S_u, \quad (u, p) = 1.$$

Число

$$\nu = \frac{\eta + \eta^{S_2} + \ldots + \eta^{S_u}}{u} \equiv \eta \pmod{\mathfrak{G}}$$

инвариантно относительно всей группы $\mathfrak{G}$ и потому равно рациональному числу. Таким образом η, в силу (5.12) и ζ, сравнимы с рациональными числами по модулю $\mathfrak{G}$.

Пусть $[x_0, x_1, \ldots, x_{n-1}]$ есть решение системы (5.5), состоящее из рациональных чисел, из которых $x_s \equiv 0 \pmod{p}$. Первое сравнение (5.5) дает нам:

$$\alpha = x_0\omega_0 + x_1\omega_1 + \ldots + x_{n-1}\omega_{n-1} \equiv 0 \pmod{\mathfrak{G}}.$$

Поэтому достаточно высокая степень α делится на p, в то время как само α (величина поля K) не делится на p в силу $x_s \not\equiv 0 \pmod{p}$ Это доказывает, что p есть критическое простое число для поля K.

2. Докажем теперь первую теорему Силова:

Теорема 22. Всякая конечная группа $\mathfrak{G}$ порядка $p^m \cdot u$, где p — простое число и $(u, p) = 1$, содержит подгруппу порядка p^m.

Доказательство проводится методом полной индукции. Предположим, что теорема доказана для групп, порядки которых меньше $p^m \cdot u$. Разобьем все элементы группы $\mathfrak{G}$ на классы, объединяя в один класс все различные элементы типа $S^{-1}AS$, где S пробегает все элементы группы $\mathfrak{G}$. Если класс элемента A состоит только из одного элемента, то A перестановочен со всеми элементами группы $\mathfrak{G}$. Такого рода элементы группы $\mathfrak{G}$ составляют группу $\mathfrak{Z}$, являющуюся абелевым нормальным делителем группы $\mathfrak{G}$ и называемую ее центром. Пусть порядок $\mathfrak{Z}$ равен ν.

Чтобы найти число элементов класса любого элемента B, рассмотрим группу $\mathfrak{N}_B$, состоящую из всех элементов, перестановочных с B (нормализатор элемента B). Разлагая $\mathfrak{G}$ по $\mathfrak{N}_B$

$$\mathfrak{G} = \mathfrak{N}_B + \mathfrak{N}_B S_2 + \ldots + \mathfrak{N}_B S_\mu,$$

мы убедимся, что все различные элементы класса B могут быть представлены так:

$$B,\ S_2^{-1}BS_2,\ \ldots,\ S_\mu^{-1}BS_\mu$$

(см. часть I), и что потому число μ элементов в классе B равно индексу нормализатора $\mathfrak{N}_B$.

Порядок группы $\mathfrak{G}$ равен сумме чисел элементов, входящих в каждый класс:

$$p^m \cdot u = \nu + \mu + \mu' + \mu'' + \ldots \qquad (5.13)$$

1. ν взаимно просто с p. Тогда из равенства (5.12) вытекает, что какое-нибудь из чисел μ должно быть взаимно простым с p. Пусть это будет μ, число элементов класса B. Тогда нормализатор $\mathfrak{N}_B$ имеет порядок, делящийся на p^m и меньший $p^m \cdot u$ (в противном случае B принадлежала бы к центру $\mathfrak{Z}$). В силу предположения о группах низших порядков теорема доказана.

2. ν делится на p. Все элементы $\mathfrak{Z}$, порядки которых суть степени p, пусть образуют подгруппу $\mathfrak{H}$ порядка p^s (см. часть I, стр. 21), тоже являющуюся нормальным делителем группы $\mathfrak{G}$. Дополнительная группа $\mathfrak{G}/\mathfrak{H}$ порядка $p^{m-s} \cdot u$ в силу предположения имеет подгруппу порядка p^{m-s}. Тогда, если эта подгруппа образуется композицией сопряженных систем $\mathfrak{H}$, $\mathfrak{H}T_2$, ..., $\mathfrak{H}T_{p^{m-s}}$ то элементы, содержащиеся в этих сопряженных системах, образуют искомую подгруппу порядка p^m группы $\mathfrak{G}$.

Таким образом в обоих случаях теорема доказана.

§ 6. Лемма из теории линейных форм

1. Докажем следующую лемму из теории линейных форм, которая в дальнейшем будет иметь важные применения:

Теорема 23. Дана система n линейных форм

$$\left.\begin{aligned} y_1 &= a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\ y_2 &= a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \\ &\cdots\cdots\cdots\cdots \\ y_n &= a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n \end{aligned}\right\} \qquad (6.1)$$

от n переменных $x_1, x_2, \ldots, x_n$ с определителем D. Существуют целые рациональные значения $x_1, x_2, \ldots, x_n$, соответствующие которым значения $y_1, y_2, \ldots, y_n$ удовлетворяют неравенствам

$$|y_i| \leqq \sqrt[n]{|D|}. \qquad (i = 1, 2, \ldots, n) \qquad (6.2)$$

Доказательство. Сначала предположим, что коэфициенты a_i суть целые рациональные числа. Решая систему (6.1) относительно $x_1, x_2, \ldots, x_n$, получим линейные выражения от $y_1, y_2, \ldots, y_n$ с дробными коэфициентами, в знаменателях которых стоит D. Придавая $y_1, y_2, \ldots, y_n$ целочисленные значения, мы будем получать, вообще говоря, дробные значения переменных $x_1, x_2, \ldots, x_n$. Если значениям $(y_1', y_2', \ldots, y_n')$ и $(y_1'', y_2'', \ldots, y_n'')$ соответствуют значения (x_i') и (x_i''), имеющие одинаковые дробные части (т. е. такие, что $x_i' - x_i''$ суть целые числа), то будем говорить, что системы (y_i') и (y_i'') лежат в одном и том же классе.

Определим число различных классов такого рода. Для этого обратим внимание на то, что целым значениям форм $y_1, y_2, \ldots, y_n$ соответствуют целые значения форм $z_1 = y_1$, $z_2 = y_2 \pm k_2 y_1$, ..., $z_n = y_n \pm k_n y_1$, где $k_2, k_3, \ldots, k_n$ — любые целые числа, и обратно, а потому формы $(y_1, y_2, \ldots, y_n)$ и $(z_1, z_2, \ldots, z_n)$ будут иметь одно и то же число классов.

Воспользуемся этим преобразованием следующим образом. Найдем среди чисел $a_{11}, a_{21}, \ldots, a_{n1}$ первой колонны системы (6.1) наименьшее отличное от нуля и, меняя нумерацию строк, поставим его на первом месте, так что это будет a_{11}. Заменим формы $(y_1, y_2, \ldots, y_n)$ формами $(y_1, y_2 - k_2 y_1, \ldots, y_n - k_n y_1)$, где $k_2, k_3, \ldots, k_n$ подберем так, чтобы имело место $0 \leqq a_i - k_i a_k < a_{11}$ $(i = 2, 3, \ldots, n)$. Полученные формы имеют то же число классов и ту же величину определителя, так как последний получается из D вычитанием первой строки из остальных строк. В полученной системе форм производим тот же процесс. Каждый из производимых процессов уменьшает абсолютную величину наименьшего элемента первой колонны. Поэтому после конечного

числа действий мы придем к системе форм, у которой в первой колонне только один элемент не равен нулю, т. е. к системе вида

$$\begin{aligned} z_1 &= b_{11}x_1 + b_{12}x_2 + \ldots + b_{1n}x_n \\ z_2 &= \quad b_{22}x_2 + \ldots + b_{2n}x_n \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ z_n &= \quad b_{n2}x_2 + \ldots + b_{nn}x_n . \end{aligned}$$

Продолжая подобное преобразование для второй колонны форм $z_2, z_3, \ldots, z_n$, затем для третьей и т. д., наконец для $(n-1)$-ой, мы придем к следующим формам:

$$\left.\begin{aligned} u_1 &= R_{11}x_1 + R_{12}x_2 + R_{13}x_3 + \ldots + R_{1n}x_n \\ u_2 &= \quad R_{22}x_2 + R_{23}x_3 + \ldots + R_{2n}x_n \\ u_3 &= \quad R_{33}x_3 + \ldots + R_{3n}x_n \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ u_n &= \quad R_{nn}x_n \end{aligned}\right\} \qquad (6.3)$$

Все проделанные преобразования не меняют ни числа классов системы форм, ни абсолютной величины ее определителя, так что мы имеем:

$$|R_{11}\cdot R_{22}\cdot R_{33}\ldots R_{nn}| = |D|. \qquad (6.4)$$

Определим теперь число классов системы форм (6.3). Для этого, придавая каждой из форм одно из значений 0, 1, 2, $|D|-1$, определим, сколько из полученных $|D|^n$ комбинаций значений $(u_1, u_2, \ldots, u_n)$ соответствует целым значениям переменных $x_1, x_2, \ldots, x_n$ или, как мы будем говорить, лежит в *нулевом классе*. Чтобы x_n было целым, необходимо и достаточно, чтобы $u_n = R_{nn}x_n$ делилось на R_{nn}, т. е. мы R_{nn} имеем право придать u_n $\left|\frac{D}{R_{nn}}\right|$ значений: $0, |R_{nn}|, 2|R_{nn}|, \ldots, \left(\left|\frac{D}{R_{nn}}\right|-1\right)|R_{nn}|$.

Каждому такому значению u_n соответствует столько различных по модулю D значений $u_{n-1} = R_{n-1,n-1}x_{n-1} + R_{n-1,n}x_n$, дающих для x_{n-1} целые значения, сколько существует различных по модулю D классов значений $u_{n-1} - R_{n-1,n}x_n$, делящихся на $R_{n-1,n-1}$, т. е. $\left|\frac{D}{R_{n-1,n-1}}\right|$. Подобным же образом докажем, что каждой такой системе значений u_{n-1}, u_n соответствует $\left|\frac{D}{R_{n-2,n-2}}\right|$ различных по модулю D значений u_{n-2}, дающих целые значения для x_{n-2}. Продолжая рассуждение, мы убедимся, что из $|D|^n$ различных по модулю D значений $u_1, u_2, \ldots, u_n$ целые значения для $x_1, x_2, \ldots, x_n$ дают

$$\left|\frac{D}{R_{11}}\right|\cdot\left|\frac{D}{R_{22}}\right|\cdots\left|\frac{D}{R_{n-1,n-1}}\right|\cdot\left|\frac{D}{R_{nn}}\right| = \left|\frac{D^n}{D}\right| = |D^n| \qquad (6.5)$$

значений. (Отметим, что не важно, какой из представителей класса по модулю D будет взят в роли u_i, так как если в двух системах значений соответственные числа u_i отличаются на кратность D, то получаемые значения x_i отличаются на целые значения.)

Прибавляя к какой-нибудь системе целых значений $(u_1, u_2, \ldots, u_n)$ все по очереди $|D|^{n-1}$ систем значений нулевого класса, мы будем получать $|D|^{n-1}$ систем значений одного и того же класса. Других систем значений входить в этот класс не может, так как если системы $(u_1', u_2', \ldots, u_n')$ и $(u_1'', u_2'', \ldots, u_n'')$ лежат в одном и том же классе, то системе $(u_1' - u_1'', u_2' - u_2'', \ldots, u_n' - u_n'')$ соответствуют целые значения x_i, т. е. она лежит в нулевом классе. Таким образом всего будет

$$|D|\cdot|D|^{n-1} = |D|$$

различных классов. Столько же классов имеет система форм (6.1).

Определим теперь целое положительное число k, удовлетворяющее неравенствам

$$k^n \leqq |D| < (k+1)^n, \qquad (6.6)$$

и станем придавать каждой переменной значения $0, 1, 2, \ldots, k$. В результате мы получим $(k+1)^n$ различных систем значений $y_1, y_2, \ldots, y_n$. Так как в силу (6.6) число различных систем меньше чем $(k+1)^n$, то среди этих систем найдутся по крайней мере две лежащие в одном классе. Пусть это будут $(y_1', y_2', \ldots, y_n')$ и $(y_1'', y_2'', \ldots, y_n'')$. Тогда их разность $(y_1' - y_1'', y_2' - y_2'', \ldots, y_n' - y_n'')$ лежит в нулевом классе, т. е. соответствует целым значениям $x_1, x_2, \ldots, x_n$. Вместе с тем в силу $0 \leqq y_i' \leqq k$, $0 \leqq y_i'' \leqq k$ имеет место

$$|y_i' - y_i''| \leqq k \leqq \sqrt[n]{|D|}, \qquad (6.7)$$

т. е. система значений $(y_1' - y_1'', y_2' - y_2'', \ldots, y_n' - y_n'')$ удовлетворяет условиям теоремы.

2. Теперь предположим, что коэфициенты a_{ik} системы (6.1) являются дробными рациональными числами, и пусть a будет их общий знаменатель. Рассмотрим систему следующих форм:

$$\left.\begin{aligned} z_1 &= ay_1 = aa_{11}x_1 + aa_{12}x_2 + \ldots + aa_{1n}x_n \\ z_2 &= ay_2 = aa_{21}x_1 + aa_{22}x_2 + \ldots + aa_{2n}x_n \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ z_n &= ay_n = aa_{n1}x_1 + aa_{n2}x_2 + \ldots + aa_{nn}x_n. \end{aligned}\right\} \qquad (6.8)$$

Определитель этой системы равен a^nD. Ее коэфициенты являются целыми рациональными числами, а потому к формам $(z_1, z_2, \ldots, z_n)$ можно применить теорему 23, т. е. найти такие целые значения $x_1, x_2, \ldots, x_n$, чтобы каждое из значений $z_1, z_2, \ldots, z_n$ было по абсолютной величине

$$\leqq \sqrt[n]{a^n|D|} = a\sqrt[n]{|D|}.$$

Тогда в силу $y_i = \frac{z_i}{a}$ для $y_1, y_2, \ldots, y_n$ будет иметь место

$$|y_i| \leqq \sqrt[n]{|D|},$$

что доказывает теорему для случая дробных рациональных a_{ij}.

3. Чтобы доказать теорему для случая иррациональных вещественных a_{ik}, укажем верхний предел для значений $x_1, x_2, \ldots, x_n$, удовлетворяющих условию теоремы. Решая систему (6.1) относительно $x_1, x_2, x_3, \ldots, x_n$:

$$\left.\begin{aligned} x_1 &= \frac{D_{11}}{D}y_1 + \frac{D_{21}}{D}y_2 + \ldots + \frac{D_{n1}}{D}y_n \\ x_2 &= \frac{D_{12}}{D}y_1 + \frac{D_{22}}{D}y_2 + \ldots + \frac{D_{n2}}{D}y_n \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n &= \frac{D_{1n}}{D}y_1 + \frac{D_{2n}}{D}y_2 + \ldots + \frac{D_{nn}}{D}y_n, \end{aligned}\right\} \qquad (6.9)$$

где D_{ij} — миноры определителя D, и обозначая через D_1 наибольшее абсолютное значение этих миноров, мы в силу неравенств

$$|y_i| \leqq \sqrt[n]{|D|} \qquad (i = 1, 2, \ldots, n)$$

будем иметь

$$|x_i| \leqq \frac{nD_1}{|D|^{\frac{n-1}{n}}} \qquad (i = 1, 2, \ldots, n). \qquad (6.10)$$

Если поэтому мы будем менять значения a_{ij}, не позволяя им выходить из известных пределов, а $|D|$ — спускаться ниже известного предела, то величины $|x_i|$, удовлетворяющие условию теоремы, не смогут беспредельно возрастать.

Пусть элементы a_{ij} иррациональны и вещественны. Представим каждый из них как предел последовательности рациональных чисел $a_{ij}^{(1)}, a_{ij}^{(2)}, a_{ij}^{(3)}, \ldots$ Тогда определители $D^{(\lambda)}$, составленные из $a_{ij}^{(\lambda)}$, а также миноры $D_{ij}^{(\lambda)}$, стремятся при неограниченном возрастании значка λ соответственно к пределам D и D_{ij}. При этом для каждого λ можно найти систему значений $(x_1, x_2, \ldots, x_n)$, удовлетворяющую неравенствам

$$\left| a_{i1}^{(\lambda)} x_1 + a_{i2}^{(\lambda)} x_2 + \ldots + a_{in}^{(\lambda)} x_n \right| \leqq \sqrt[n]{D^{(\lambda)}} \quad (i = 1, 2, \ldots, n), \qquad (6.11)$$

откуда в силу (6.10) (т. е. в силу ограниченности $|x_i|$) мы получим

$$|a_{i1} x_1 + a_{i2} x_2 + \ldots + a_{in}|x_n| \leqq \sqrt[n]{|D|} + \varepsilon_{i\lambda} \quad (i = 1, 2, \ldots, n), \qquad (6.12)$$

где все $\varepsilon_{i\lambda}$ стремятся при возрастании λ к нулю. В силу (6.10) существует лишь конечное число значений $x_1, x_2, \ldots, x_n$, удовлетворяющих неравенствам (6.12) при каких бы то ни было значениях λ. Докажем, что хоть одно из этих значений удовлетворяет неравенствам

$$|a_{i1} x_1 + a_{i2} x_2 + \ldots + a_{in} x_n| \leqq \sqrt[n]{|D|} \qquad (i = 1, 2, \ldots, n).$$

Допустим противное, т. е. пусть для каждого из этих значений существует такая форма $a_{i1} x_1 + a_{i2} x_2 + \ldots + a_{in} x_n$, что

$$|a_{i1} x_1 + a_{i2} x_2 + \ldots + a_{in} x_n| \geqq \sqrt[n]{|D|} + \alpha, \qquad (6.13)$$

где $\alpha > 0$. Возьмем λ настолько большим, чтобы все соответствующие $|\varepsilon_{i\lambda}|$ были меньше наименьшего из α. Тогда формулы (6.12) и (6.13) находятся в противоречии. Это доказывает теорему.

4. Рассмотрим случай, когда элементы a_{ij} могут быть комплексными, но так, что каждой i-ой строке соответствует другая j-ая строка, в которой $a_{jk} = \overline{a_{ik}}$ $(k = 1, 2, \ldots, n)$. Тогда значения y_i и y_j должны быть сопряженно-комплексными. Строки же с вещественными элементами не требуют соответствующих строк.

Заменим в системе форм все сопряженно-комплексные формы y_i и y_j следующими их комбинациями:

$$z_i = \frac{1}{\sqrt{2}}(y_i + y_j), \quad z_j = \frac{1}{i\sqrt{2}}(y_i - y_j), \qquad (6.14)$$

которые являются вещественным формами. Из (6.14) вытекает:

$$y_i = \frac{1}{\sqrt{2}}(z_i + iz_j), \quad y_j = \frac{1}{\sqrt{2}}(z_i - iz_j), \qquad (6.15)$$

откуда следует, что неравенство $|y_i| \leqq \sqrt[n]{|D|}$ равносильно следующему:

$$\sqrt{\frac{z_i^2}{2} + \frac{z_j^2}{2}} \leqq \sqrt[n]{|D|}, \qquad (6.16)$$

которое во всяком случае будет удовлетворено, если

$$|z_i| \leqq \sqrt[n]{|D|}, \quad |z_j| \leqq \sqrt[n]{|D|}. \qquad (6.17)$$

После замены форм y_i формами z_i определитель системы сохранит свою величину, так как эта замена соответствует следующей последовательности операций над определителем D: 1) прибавлению к j-ой строке i-ой, 2) умножению i-ой строки на 2, 3) отнятию от i-ой строки j-ой, 4) перемене местами i-ой и j-ой строк, 5) делению i-ой строки на $\sqrt{2}$, а j-ой на $i\sqrt{2}$. Первая и третья операции не изменяют величины определителя, четвертая меняет его знак, вторая увеличивает его в 2 раза, а пятая делит его на $2i$. Таким образом в результате абсолютная величина определителя остается той же.

Переходя подобным образом от каждой пары сопряженно-комплексных форм к вещественным формам и применяя результат 3 к вещественным формам $(z_1, z_2, \ldots, z_n)$, мы докажем теорему и для этого случая.

5. Можно доказать теорему 23 в более сильной формулировке. Именно можно доказать, что целые значения $x_1, x_2, \ldots, x_n$ можно выбрать так, чтобы для всех форм, кроме может быть одной, имело место не только $|y_i| \leqq \sqrt[n]{|D|}$, но и $|y_i| < \sqrt[n]{|D|}$.

Для доказательства выберем произвольную величину $\varepsilon\,(0<\varepsilon<1)$ и определим по ней другую, ε', связанную с ε равенством

$$(1-\varepsilon)^{n-1}(1+\varepsilon')=1. \tag{6.18}$$

Очевидно, что $\varepsilon'>0$ и что при стремлении ε к нулю и ε' стремится к нулю.

Разделим первую из форм (6.1) (будем предполагать ее вещественной) на $1+\varepsilon'$, а остальные на $1-\varepsilon$. Применяя теорему 23 к формам $\left(\frac{y_1}{1+\varepsilon'}, \frac{y_2}{1-\varepsilon}, \ldots, \frac{y_n}{1-\varepsilon}\right)$ (их определитель в силу (6.18) тоже равен D), мы найдем такую систему значений $(x_1, x_2, \ldots, x_n)$, для которых имеет место

$$|y_1| \leqq (1+\varepsilon')\sqrt[n]{|D|},\ |y_2| \leqq (1-\varepsilon)\sqrt[n]{|D|},\ \ldots,\ |y_n| \leqq (1-\varepsilon)\sqrt[n]{|D|}. \tag{6.19}$$

Будем придавать ε последовательность значений $\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots$, стремящуюся к нулю. Для каждого из них существует лишь конечное число систем значений $(x_1, x_2, \ldots, x_n)$, удовлетворяющих неравенствам (6.19). Докажем, что можно найти такой значок λ, при котором наряду с (6.19) выполнялось бы неравенство $|y_1| \leqq \sqrt[n]{|D|}$. Допустим противное, т. е. что при всех λ имеет место $|y_1| = \sqrt[n]{|D|}\,(1+\alpha)$, где $\alpha>0$. Так как для всех λ таких систем $(x_1, x_2, \ldots, x_n)$ конечное число, то мы можем выбрать ту систему, для которой α имеет наименьшее значение. Тогда для всех систем, удовлетворяющих неравенствам (6.19) при значениях $\varepsilon = \varepsilon_\lambda, \varepsilon_{\lambda+1}, \varepsilon_{\lambda+2}, \ldots$, имеет место неравенство $|y_1| \geqq (1+\alpha)\sqrt[n]{|D|}$. Но так как значения $\varepsilon_1', \varepsilon_2', \ldots$, определяемые из равенства (6.18), тоже стремятся к нулю, то при некотором λ будет иметь место $\varepsilon'^{(\lambda)} < \alpha$, и тогда первое из неравенств (6.19) не будет удовлетворяться, вопреки теореме 23. Таким образом для некоторого λ мы получим неравенства:

$$|y_1| \leqq \sqrt[n]{|D|},\ |y_2| \leqq (1-\varepsilon_\lambda)\sqrt[n]{|D|},\ \ldots,\ |y_n| \leqq (1-\varepsilon_\lambda)\sqrt[n]{|D|},$$

т. е.

$$|y_1| \leqq \sqrt[n]{|D|},\ |y_2| < \sqrt[n]{|D|},\ \ldots,\ |y_n| < \sqrt[n]{|D|}. \tag{6.20}$$

В случае комплексных форм $y_1, y_2, \ldots, y_n$ мы перейдем, как в п. 4, к вещественным формам $z_1, z_2, \ldots, z_n$, и в роли y_1 [см. (6.19)] возьмем форму z_1, дающую начало вещественной части формы y_1. Тогда мы сможем определить такие системы значений $(x_1, x_2, \ldots, x_n)$, при которых имеет место

$$|z_1| \leqq \sqrt[n]{|D|} \text{ и } |z_i| < \sqrt[n]{|D|} \qquad (i=2, 3, \ldots, n).$$

В силу (6.16) для всех форм $(y_1, y_2, \ldots, y_n)$ имеет место

$$|y_i| < \sqrt[n]{|D|} \qquad (i=1, 2, \ldots, n) \tag{6.21}$$

Г. Минковский, пользуясь методами геометрии чисел, получил для случая комплексных форм более низкую оценку, чем (6.21).

§ 7. Теорема Минковского

1. Теорема 24. (Минковского). Дискриминант всякого поля алгебраических чисел отличен от ± 1.

Доказательство. Пусть $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$—фундаментальный базис поля k. Рассмотрим систему форм

$$\left.\begin{aligned} y^{(0)} &= \omega_0 x_0 + \omega_1 x_1 + \ldots + \omega_{n-1} x_{n-1} \\ y^{(1)} &= \omega_0^{(1)} x_0 + \omega_1^{(1)} x_1 + \ldots + \omega_{n-1}^{(1)} x_{n-1} \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ y^{(n-1)} &= \omega_0^{(n-1)} x_0 + \omega_1^{(n-1)} x_1 + \ldots + \omega_{n-1}^{(n-1)} x_{n-1} \end{aligned}\right\} \tag{7.1}$$

Допустим, что дискриминант поля k равен ± 1. Тогда для системы форм (7.1) можно найти такую систему значений $(x_0, x_1, \ldots, x_n)$, из которых не все равны нулю, для которой будет иметь место

$$|y^{(0)}| \leqq 1,\ |y^{(1)}| \leqq 1,\ \ldots,\ |y^{(n-1)}| < 1.$$

Отсюда следует

$$|N(y^{(0)})| = |y^{(0)} \cdot y^{(1)} \ldots y^{(n-1)}| < 1. \tag{7.2}$$

Но $y^{(0)}$ является целым алгебраическим числом, а потому его норма должна быть равна целому рациональному числу. При этом она отлична от нуля, так как в противном случае мы бы имели по крайней мере для одного значения i:

$$y^{(i)} = \omega_0^{(i)} x_0 + \omega_1^{(i)} x_1 + \ldots + \omega_{n-1}^{(i)} x_{n-1} = 0.$$

Но это противоречит тому, что $[\omega_0^{(i)}, \omega_1^{(i)}, \ldots, \omega_{n-1}^{(i)}]$ является базисом сопряженного поля $k^{(i)}$. Таким образом $|N(y^{(0)})| \geqq 1$, что противоречит неравенству (7,2), ч. и т. д.

2. Из теоремы Минковского следует, что дискриминант поля k, будучи целым рациональным числом, непременно содержит простые множители. Сопоставляя это с теоремой 12, согласно

которой простые делители дискриминанта поля k, и только они, являются критическими простыми числами внутри k, мы можем формулировать теорему Минковского так:

Теорема 24а. Всякое поле алгебраических чисел непременно обладает критическими простыми числами.

3. Аналогичные соображения позволяют доказать следующую теорему:

Теорема 25. Существует только конечное число полей, имеющих заданное значение дискриминанта.

Доказательство. Мы ограничимся рассмотрением полей заданной степени n с дискриминантом D. Рассматривая для каждого такого поля систему форм

$$\sqrt[2n]{|D|}\cdot y^{(0)},\ \sqrt[2n]{|D|}\cdot y^{(1)},\ \ldots,\ \sqrt[2n]{|D|}\cdot y^{(n-1)} \tag{7.3}$$

[см. 7.1)], мы убедимся, что внутри каждого из таких полей содержится целое алгебраическое число, удовлетворяющее вместе со своими сопряженными числами следующим неравенствам:

$$|y^{(0)}|\leqq\sqrt{|D|},\ |y^{(1)}|<1|,\ \ldots,\ |y^{(n-1)}|<1. \tag{7.4}$$

Это число определяет собой поле. В самом деле, если бы $y^{(0)}$ не было примитивным числом поля, то оно должно было бы частично совпадать со своими сопряженными числами. Но это невозможно, так как из неравенства (7.4) и

$$|N(y^{(0)})|=|y^{(0)}\cdot y^{(1)}\ldots y^{(n-1)}|\geqq 1$$

следует $|y^{(0)}|>1$, в то время как его сопряженные числа подчиняются неравенствам $|y^{(i)}|<1\quad(i=1,2,\ldots,n-1)$.

Далее, из (7.4) мы убеждаемся, что элементарно симметрические функции от $y^{(0)}, y^{(1)}, \ldots, y^{(n-1)}$, т. е. коэфициенты уравнения, которому удовлетворяет $y^{(0)}$, не превышают некоторых пределов, зависящих только от D. Но так как они являются целыми рациональными числами, то число значений этих элементарно-симметрических функций ограничено. Поэтому можно построить некоторое (конечное) число уравнений n-ой степени такого рода, что всякое поле n-ой степени с дискриминантами D может быть порождено корнем одного из этих уравнений. Отсюда следует конечность такого рода полей, ч. и т. д.

Этот факт дает средство для классификации полей n-ой степени. Можно построить таблицу полей n-ой степени в порядке возрастания дискриминантов.

4. Минковский показал, что при заданном дискриминанте конечно также число возможных степеней n. Именно, он получил формулу

$$|D|>\left(\frac{\pi}{4}\right)^{2(n-\nu)}\cdot\frac{e}{2\pi n}^{2n-\frac{1}{6n}}, \tag{7.5}$$

где ν — сумма числа вещественных и числа пар комплексных полей, сопряженных с k.

§ 8. Группа инерции. Теорема монодромии

1. С критическими простыми идеалами в нормальном поле связаны особые подгруппы группы Галуа поля, называемые *группами инерции*. Группа инерции простого идеала $\mathfrak{P}$ определяется как совокупность автоморфизмов S поля K, для которых имеет место

$$\alpha^S\equiv\alpha\pmod{\mathfrak{P}} \tag{8.1}$$

для всякого целого числа поля K. Чтобы обнаружить связь групп инерции с критическими простыми идеалами, докажем

Теорему 26. Если простой идеал $\mathfrak{P}$ нормального поля K входит в простое число p в m-ой степени, то порядок группы инерции $\mathfrak{T}$ идеала $\mathfrak{P}$ равен m.

Доказательство. Обозначим через ν число различных простых идеалов, сопряженных с $\mathfrak{P}$. Если теперь $\mathfrak{Z}$ есть совокупность автоморфизмов, оставляющих $\mathfrak{P}$ неизменным (называемая *группой разложения* идеала $\mathfrak{P}$), то легко убедиться, что ν равно индексу $(\mathfrak{G}:\mathfrak{Z})$.

Пусть p^f — степень идеала $\mathfrak{P}$. Тогда существует p^f классов сравнений по модулю $\mathfrak{P}$, и все его представители удовлетворяют сравнению

$$\alpha^{p^f}\equiv\alpha\pmod{\mathfrak{P}}. \tag{8.2}$$

Группы этих классов относительно сложения и умножения изоморфны с конечным полем порядка p^f (см. часть I), а потому существуют представители этих классов, удовлетворяющие неприводимому по модулю p сравнению $f(x)\equiv 0$ f-ой степени. Если α—такой представитель, то все степени $\alpha,\ \alpha^p,\ \alpha^{p^2},\ \ldots,\ \alpha^{p^{f-1}}$ несравнимы между собой и составляют полную систему корней сравнения $f(x)\equiv 0\pmod p$. Поэтому каждый автоморфизм группы $\mathfrak{Z}$ переводит α в величину, сравнимую по модулю $\mathfrak{P}$ с одной из степеней $\alpha,\ \alpha^p,\ \ldots,\ \alpha^{p^{f-1}}$. С другой стороны, должен существовать автоморфизм, переводящий α в величину, сравнимую с α^p. В самом деле, если бы все автоморфизмы группы $\mathfrak{Z}$ переводили α только в некоторые из этих степеней, например в $\alpha,\ \alpha^{(1)},\ \ldots,\ \alpha^{(s-1)}\ (s<f)$, то элементарно-симметрические функции от $\alpha,\ \alpha'',\ \ldots,\ \alpha^{(s-1)}$ оставались бы от автоморфизмов группы $\mathfrak{Z}$ неизменными, а потому, рассуждая как при доказательстве теоремы 12, мы убедимся, что эти величины сравнимы по модулю $\mathfrak{P}$ с числами, инвариантными относительно группы $\mathfrak{Z}$. Если мы вдобавок выберем α так, чтобы оно делилось на все

идеалы, сопряженные с $\mathfrak{P}$, то все числа, сопряженные с α, будут делиться на $\mathfrak{P}$. Если поэтому ξ — число, инвариантное относительно $\mathfrak{Z}$, и $\xi^{(1)}, \xi', \ldots, \xi^{(t-1)}$—все различные сопряженные с ξ числа, то $\xi \equiv \xi + \xi^{(1)} + \ldots + \xi^{(t-1)} \pmod{\mathfrak{P}}$, то ξ сравнимо по модулю $\mathfrak{P}$ с рациональным числом. Таким образом величины $\alpha, \alpha'', \ldots, \alpha^{(t-1)}$ будут корнями сравнения s-ой степени с рациональными коэфициентами, что противоречит неприводимости $f(x) \equiv 0 \pmod{p}$:

Если таким образом автоморфизмы $Z_1, Z_2, \ldots, Z_f$ переводят α в величины, сравнимые соответственно с $\alpha, \alpha^p, \ldots, \alpha^{p^{f-1}}$, то совокупность сопряженных систем $\mathfrak{T} + \mathfrak{T}Z_2 + \ldots + \mathfrak{T}Z_f$ составляет всю группу $\mathfrak{Z}$. Поэтому индекс $(\mathfrak{Z}:\mathfrak{T}) = f$, откуда индекс $(\mathfrak{G}:\mathfrak{T}) = (\mathfrak{G}:\mathfrak{Z}) \cdot (\mathfrak{Z}:\mathfrak{T}) = \nu \cdot f$ и порядок группы $\mathfrak{T}$ равен $\frac{n}{\nu f}$.

Теперь примем во внимание, что в нормальных полях степени сопряженных простых идеалов равны, а также равны кратности, с которой они входят в простое число p. Пусть $\mathfrak{P}$ входит в p с кратностью m. Беря норму от обеих частей равенства

$$p = \mathfrak{P}_1^m \mathfrak{P}_2^m \ldots \mathfrak{P}_\nu^m,$$

получим:

$$p^n = p^{fm\nu},$$

откуда

$$n = fm\nu.$$

Таким образом и кратность m и порядок групп $\mathfrak{T}$ равны одному и тому же числу $\frac{n}{f\nu}$, ч. и т. д.

2. Отсюда, как следствие, вытекает, что для простого идеала группа инерции отлична от единичной группы тогда и только тогда, если он является критическим. Так как по теореме 12 критические простые идеалы являются делителями дискриминанта поля, т. е. их число конечно, то в каждом поле существует лишь конечное число отличных от единичной группы групп инерции. С другой стороны, по теореме Минковского каждое поле непременно содержит критические простые идеалы, а потому в каждом нормальном поле всегда имеются группы инерции, отличные от единичной группы.

3. Группы инерции имеют замечательную структуру. Если m не делится на p (мы будем называть *регулярным* соответствующее этому случаю простое число), группа инерции циклическая. Если же $m = p^n \cdot m'$, где m' не делится на p, группа инерции имеет нормальный делитель $\mathfrak{V}$ (называемый *группой разветвления*), и тогда группа $\mathfrak{T}/\mathfrak{V}$ циклическая.

Чтобы доказать это, возьмем p=простое число π, делящееся точно на первую степень $\mathfrak{P}$, и применим к нему какую-нибудь подстановку T группы инерции. Число π^T в силу свойства

группы инерции будет делиться на $\mathfrak{P}$, в силу чего существует такое неделящееся на p число c, что $\frac{c \cdot \pi^T}{\pi}$ будет целым алгебраическим. Оно взаимно просто с $\mathfrak{P}$ и потому лежит в одном из взаимно простых с $\mathfrak{P}$ классов сравнений по модулю $\mathfrak{P}$. Но эти классы образуют циклическую группу относительно умножения (см. часть I, стр. 162), в силу чего все классы сравнений по модулю $\mathfrak{P}$ сравнимы со степенями одного некоторого представителя α. Таким образом $c\pi^T \equiv \pi\alpha^s \pmod{\mathfrak{P}^2}$, откуда, умножая на представителя обратного к c класса и вводя новое обозначение для s, получим:

$$\pi^T \equiv \alpha^s \cdot \pi \pmod{\mathfrak{P}^2}.$$

Составляя подобные сравнения для всех подстановок T группы инерции $\mathfrak{T}$, обратим внимание на показатели s. Некоторые из них могут быть равны нулю, и тогда

$$\pi^v \equiv \pi \pmod{\mathfrak{P}^2}.$$

Нетрудно убедиться, что совокупность подстановок типа v составляет группу. Эту группу обозначают через $\mathfrak{V}$ и называют группой разветвления. Покажем, что ее порядок равен степени p. Для этого обратим внимание, что разность $\pi^\nu - \pi$ делится на $\mathfrak{P}^2$. Обозначив через $\mathfrak{P}^i$ степень, на которую эта разность делится точно, мы, рассуждая подобно прежнему, получим:

$$\pi^v \equiv \pi + \beta \cdot \pi^i \pmod{\mathfrak{P}^{i+1}}. \tag{8.5}$$

Отсюда в силу $\beta^v \equiv \beta \pmod{\mathfrak{P}}$ будет следовать:

$$\pi^{v^2} \equiv \pi + \beta^\nu \cdot (\pi^\nu)^i \equiv \pi + 2\beta\pi^i \pmod{\mathfrak{P}^{i+1}},$$
$$\pi^{v^3} \equiv \pi + 3\beta\pi^i \pmod{\mathfrak{P}^{i+1}},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\pi^{v^p} \equiv \pi + p \cdot \pi^i \equiv \pi \pmod{\mathfrak{P}^{i+1}}.$$

Таким образом разность $\pi^{v^p} - \pi$ делится по крайней мере на $\mathfrak{P}^{i+1}$. Продолжая рассуждение, получим:

$$\pi^{v^{p^2}} \equiv \pi \pmod{\mathfrak{P}^{i+2}}$$
$$\pi^{v^{p^3}} \equiv \pi \pmod{\mathfrak{P}^{i+3}}.$$
$$\ldots\ldots\ldots\ldots$$

Но так как дискриминант числа π, будучи равен произведению разностей $\pi^s - \pi$, делится на конечную степень $\mathfrak{P}$, то при достаточно высоком s из $\pi^{v^{p^s}} \equiv \pi \pmod{\mathfrak{P}^{i+s}}$ следует $v^{p^s} = 1$. Таким образом порядок всякой подстановки группы $\mathfrak{V}$ есть степень p. Если бы порядок группы $\mathfrak{V}$ содержал отличный от p простой множитель, например q^t, то по первой теореме

Силова $\mathfrak{V}$ содержала бы подгруппу порядка q^t, все подстановки которой суть степени q. Это противоречит нашему результату. Таким образом порядок $\mathfrak{V}$ есть степень p.

Обратимся теперь к (8.3). Пусть a будет наименьший отличный от нуля из показателей s, соответствующих различным подстановкам T группы $\mathfrak{T}$. Тогда все остальные показатели должны делиться на a. В самом деле, если

$$\pi^{T_1} \equiv \alpha^a \cdot \pi \pmod{\mathfrak{P}^2}, \tag{8.6}$$

$$\pi^{T} \equiv \alpha^s \cdot \pi \pmod{\mathfrak{P}^2}, \tag{8.7}$$

то, деля s с остатком на a: $s = aq + r$, где $0 \leqq r < a$, мы получим:

$$\pi^{T_1^{-1}} \equiv \alpha^b \cdot \pi \pmod{\mathfrak{P}^2}.$$

Применяя к этому сравнению подстановку T_1 и принимая во внимание, что $\alpha^{T_1} \equiv \pmod{\mathfrak{P}}$, будем иметь:

$$\pi \equiv \alpha^b \cdot \pi^{T_1} \equiv \alpha^{b+a} \pi \pmod{\mathfrak{P}},$$

откуда $\alpha^{b+a} \equiv 1 \pmod{\mathfrak{P}}$, так что можно положить $b = -a$.

Принимая во внимание, что

$$\pi^{T_1^{-1}} \equiv \alpha^{-a} \cdot \pi \pmod{\mathfrak{P}^2}, \tag{8.8}$$

применим к сравнению (8.7) подстановку T_1^{-q}:

$$\pi^{TT_1^{-q}} \equiv \alpha^{s-aq} \cdot \pi \pmod{\mathfrak{P}^2}.$$

В силу $0 \leqq s - aq < a$ и определения a должно иметь место $s - aq = 0$, т. е.

$$\pi^{TT_1^{-q}} \equiv \pi \pmod{\mathfrak{P}^2},$$

откуда следует, что TT_1^{-q} входит в группу $\mathfrak{V}$. Таким образом каждая подстановка группы $\mathfrak{T}$ входит в одну их сопряженных систем $\mathfrak{V}$, $\mathfrak{V}T_1$, $\mathfrak{V}T_1^2$,... Степень T_1^u входит в $\mathfrak{V}$ тогда и только тогда, если $\alpha^{ua} \equiv 1 \pmod{\mathfrak{P}}$, т. е. если $u.a$ делится на $p^f - 1$ [в силу того, что наименьшая степень s, дающая $\alpha^s \equiv 1 \pmod{\mathfrak{P}}$, есть (p^f-1)-ая]. Итак, u есть делитель $p^f - 1$ и потому взаимно просто с p. Кроме того, имеем:

$$\mathfrak{T} = \mathfrak{V} + \mathfrak{V}T_1 + \mathfrak{V}T_1^2 + \ldots + \mathfrak{V}T_1^{u-1}. \tag{8.9}$$

Остается доказать, что $\mathfrak{V}$ есть нормальный делитель группы $\mathfrak{T}$. Для этого возьмем произвольную подстановку v из $\mathfrak{V}$ и преобразуем его произвольной подстановкой T из $\mathfrak{T}$. Покажем, что $T^{-1}vT$ тоже входит в $\mathfrak{V}$. Для этого из сравнений

$$\pi^T \equiv \alpha^s \pi \pmod{\mathfrak{P}^2}\, v\, \pi^{T^{-1}} \equiv \alpha^{-s}\pi \pmod{\mathfrak{P}^2},\ \pi^v \equiv \pi \pmod{\mathfrak{P}^2}$$

получим:

$$\pi^{T^{-1}vT} = (\alpha^{-s}\pi)^{vT} = (\alpha^{-s}\pi)^T \equiv \alpha^{-s} \cdot \alpha^s \pi \equiv \pi \pmod{\mathfrak{P}^2},$$

что доказывает наше утверждение.

Из разложения (8.9) следует, что дополнительная группа $\mathfrak{T}/\mathfrak{V}$ есть циклическая группа, порядок которой u есть делитель $p^f - 1$ и потому взаимно прост с p.

Формулируем полученные результаты:

Теорема 27. Если порядок группы инерции $\mathfrak{T}$ простого идеала $\mathfrak{P}$ равен $p^s \cdot u$, где $(u, p) = 1$, то $\mathfrak{T}$ имеет нормальный делитель $\mathfrak{V}$ порядка p^s, представляющий совокупность подстановок, сохраняющих класс сравнений чисел поля по модулю $\mathfrak{P}^2$. Дополнительная группа $\mathfrak{T}/\mathfrak{V}$ циклическая, и ее порядок u есть делитель числа $p^f - 1$, где f — степень $\mathfrak{P}$.

3. Для доказательства теоремы монодромии необходима

Теорема 28. Если k есть делитель нормального поля K, принадлежащий к подгруппе $\mathfrak{H}$ его группы Галуа $\mathfrak{G}$, то, чтобы простое число p поля K, делящееся на простой идеал $\mathfrak{P}$ поля K, не было критическим, необходимо и достаточно, чтобы группа $\mathfrak{H}$ содержала, как делитель, группу инерции идеала $\mathfrak{P}$.

Доказательство. 1. Пусть $\mathfrak{T}$ не входит в $\mathfrak{H}$. Тогда существует подстановка T из $\mathfrak{T}$, не входящая в $\mathfrak{H}$, т. е. переводящая фундаментальный базис $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ поля K в систему других величин, например в $[\omega_0', \omega_1', \ldots, \omega'_{n-1}]$. Дискриминант поля K есть квадрат определителя

$$\begin{vmatrix} \omega_0, & \omega_1, & \ldots, & \omega_{n-1} \\ \omega_0', & \omega_1', & \ldots, & \omega'_{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ \omega_0^{(n-1)}, & \omega_1^{(n-1)}, & \ldots, & \omega_{n-1}^{(n-1)} \end{vmatrix},$$

т. е.

$$\begin{vmatrix} \omega_0 - \omega_0', & \omega_1 - \omega_1', & \ldots, & \omega_{n-1} - \omega'_{n-1} \\ \omega_0', & \omega_1', & \ldots, & \omega'_{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ \omega_0^{(n-1)}, & \omega_1^{(n-1)}, & \ldots & \omega_{n-1}^{(n-1)} \end{vmatrix}$$

Верхняя строка этого определителя в силу свойства группы инерции делится на $\mathfrak{P}$. Поэтому квадрат этого определителя должен делиться на p, и простое число p является критическим.

Применяя этот результат к каждому из простых идеалов, сопряженных с $\mathfrak{P}$, мы убедимся, что простое число будет критическим внутри k, если хоть одна из групп инерции, соответствующих этим простым идеалам, не входит в $\mathfrak{H}$.

2. Предположим теперь, что $\mathfrak{H}$ содержит $\mathfrak{T}$. Чтобы доказать, что простой идеал $\mathfrak{P}$, делящийся на $\mathfrak{P}$, входит в p в первой степени, достаточно показать, это для поля k_t, принадлежащего к группе $\mathfrak{T}$ (называемого *полем инерции* идеала $\mathfrak{P}$). В самом деле, простой идеал $\mathfrak{P}$ внутри k останется идеалом

и в более обширном поле k_t, и если он входит в p выше, чем в первой степени, то это будет иметь место и для k_t.

Заметим прежде всего, что всякое число поля K сравнимо по модулю $\mathfrak{P}$ с числом из k_t. Прием доказательства тот же, что в доказательстве теоремы 12. Именно, в силу

$$\alpha^T \equiv \alpha \pmod{\mathfrak{P}}$$

для каждой подстановки T из $\mathfrak{T}$ мы покажем, что произведение $\alpha \cdot \alpha^v \cdot \alpha^{v^2} \dots$, распространенное на подстановки из $\mathfrak{V}$, сравнимо с p^s-ой степенью α, и применим обобщенную теорему Ферма. Получив число, инвариантное относительно $\mathfrak{V}$, возьмем среднее арифметическое из сопряженных с ним относительно $\mathfrak{T}$ чисел.

Из этого факта мы заключаем, что внутри k_t находится столько же (p^f) различных классов сравнений по модулю $\mathfrak{P}$, сколько и в K. Эти классы внутри k_t несравнимы также по модулю простого идеала $\mathfrak{P}_t$ поля k_t. Других классов k_t иметь не может. Поэтому

$$N_K(\mathfrak{P}) = N_{k_t}(\mathfrak{P}_t),$$

где индексы K, k_t показывают, внутри какого поля берется норма.

Пусть π будет p-простое число из K, делящееся на $\mathfrak{P}$. Вводя обозначения

$$\mathfrak{T} = 1 + T_2 + \dots + T_m$$
$$\mathfrak{G} = \mathfrak{T} + \mathfrak{T}S_2 + \dots + \mathfrak{T}S_{\frac{n}{m}},$$

получим для нормы $N(\pi)$ следующее выражение:

$$N(\pi) = (\pi \cdot \pi^{T_2} \dots \pi^{T_m} \cdot \pi^{S_2} \cdot \pi^{T_2 S_2} \dots \pi^{T_m S_2} \dots \times$$
$$\times \pi^{S_{\frac{n}{m}}} \cdot \pi^{T_2 S_{\frac{n}{m}}} \dots \pi^{T_m S_{\frac{n}{m}}} = cp^f, \quad (c,p) = 1.$$

Вводя для числа из k_t $\pi \cdot \pi^{T_2} \dots \pi^{T_m}$ обозначение π_t перепишем формулу так:

$$N(\pi) = \pi_t \cdot \pi_t^{S_2} \dots \pi_t^{S_{\frac{n}{m}}} = cp^f, (c,p) = 1.$$

Это показывает, что норма π_t из k_t делится на ту же степень p, что и норма простого идеала $\mathfrak{P}_t$, на который делится π_t. Поэтому π_t должно быть p-простым числом, соответствующим $\mathfrak{P}_t$. Но, рассматривая $\pi_t = \pi \cdot \pi^{T_2} \dots \pi^{T_m}$ как число из K, мы видим, что в силу $\mathfrak{P}^{T_i} = \mathfrak{P}$ оно делится на $\mathfrak{P}^m$ и больше ни на какие простые идеалы, сопряженные с $\mathfrak{P}$. Поэтому

$$\mathfrak{P}_t = \mathfrak{P}^m.$$

Но так как K входит в p в m-ой степени, то $\mathfrak{P}_t$ может входить в p только в первой степени, ч. и т. д.

4. Полученные результаты можно формулировать так:

> Чтобы для делителя k нормального поля K простое число p не было критическим, необходимо и достаточно, чтобы группа $\mathfrak{H}$, к которой принадлежит k, содержала группы инерции всех простых идеальных множителей числа p.

Заметим, что если $\mathfrak{T}$ есть группа инерции простого идеала $\mathfrak{P}$, то группой инерции сопряженного простого идеала $\mathfrak{P}^S$ является $S^{-1}\mathfrak{T}S$. В самом деле, если T входит в $\mathfrak{T}$, то для произвольного целого числа α поля K имеет место

$$\alpha^T \equiv \alpha \pmod{\mathfrak{P}}.$$

Написав это свойство для $\alpha^{S^{-1}}$, получим:

$$\alpha^{S^{-1}T} \equiv \alpha^{S^{-1}} \pmod{\mathfrak{P}}.$$

Применяя к этому сравнению подстановку S, будем иметь:

$$\alpha^{S^{-1}TS} \equiv \alpha \pmod{\mathfrak{P}^S},$$

что показывает, что подстановки группы $S^{-1}\mathfrak{T}S$ входят в группу инерции $\mathfrak{T}_1$, идеала $\mathfrak{P}^S$. Обратно, если T_1 есть подстановка из $\mathfrak{T}_1$, то ST_1S^{-1} должна входить в $\mathfrak{T}$. Поэтому

$$\mathfrak{T}_1 = S^{-1}\mathfrak{T}S.$$

Так как в p входят только сопряженные с $\mathfrak{P}$ простые идеалы, то p соответствуют только сопряженные с $\mathfrak{T}$ группы инерции. Это замечание важно, например, для случая абелевых полей, когда группы инерции, соответствующие сопряженным простым идеалам, должны совпадать.

5. Пусть K — нормальное поле, $\mathfrak{G}$ — его группа Галуа. Построим группы инерции, соответствующие всем критическим простым идеалам поля K, и образуем их композит (т. е. наименьшую содержащую их группу). Из теоремы 28 следует, что ни одно из критических простых чисел поля K не может быть критическим для поля, принадлежащего к нашему композиту. Другие простые числа тоже не могут быть критическими, так как простой идеал поля K, входящий в соответствующее простое число в первой степени, не может сделаться составным идеалом внутри делителя поля K. Таким образом поле, принадлежащее к нашему композиту, не имеет критических простых чисел и по теореме Минковского совпадает с полем рациональных чисел. Поэтому наш композит совпадает с $\mathfrak{G}$, и мы приходим к *арифметической теореме монодромии*:

> **Теорема 29.** Наименьшая группа, содержащая все группы инерции нормального поля, совпадает с группой Галуа этого поля.

§ 9. Абелевы поля и поля деления круга

1. В деле изучения арифметической структуры полей, имеющих заданную группу, первым этапом является следующая теорема, высказанная Кронекером (L. Kronecker) и впервые доказанная Вебером (H. Weber):

Теорема 30. Все абелевы поля с полем рациональных чисел в качестве области рациональности суть поля деления круга.

При доказательстве этой теоремы мы можем ограничиться рассмотрением циклических полей, так как в части I мы видели, что всякая абелева группа есть прямое произведение циклических групп (стр. 42, теорема 30) и что в связи с этим абелево поле является композитом циклических полей (стр. 98—99, „Прямое произведение полей"). При этом степень поля можно считать степенью простого числа.

2. Рассмотрим циклическое уравнение

$$f(x)=0 \tag{9.1}$$

степени $n=l^h$, где l — простое число. Пусть его корень (или, что то же, его корни) образует нормальное поле K. Рассмотрим группы инерции, соответствующие всем критическим простым числам этого поля (каждому критическому простому числу абелева поля соответствует только одна группа инерции, так как в абелевых группах сопряженные подгруппы совпадают). Тогда одна из этих групп инерции должна совпадать с группой Галуа $\mathfrak{G}$ поля K. В самом деле, если бы ни одна из групп инерции не совпадала с $\mathfrak{G}$, то все они имели бы порядок не выше l^{h-1}, т. е. были бы делителями группы $\mathfrak{G}_1$, составленной из l-ых степеней элементов группы $\mathfrak{G}$. Тогда композит всех групп инерции тоже были бы делителями $\mathfrak{G}_1$, что противоречит теореме 29.

Будем называть *вполне критическими* простые числа, имеющие группой инерции $\mathfrak{G}$. Мы видели, что они всегда существуют.

3. Сначала мы разберем случай, когда K имеет вполне критические простые числа, отличные от l (регулярный случай). Пусть p — такое простое число. Для него $m=l^h=n$. Из формулы $n=fm\nu$ (§ 8.1) следует $f=\nu=1$, т. е p равно l^h-ой степени простого идеала первой степени. В силу теоремы 27 l^h есть делитель $p-1$.

Рассмотрим поле K_1, образованное p-ыми корнями из единицы. Его группа циклическая порядка $p-1$ (часть I, стр. 113, § 2.4). Полагая $p-1=l^h\cdot s$ и образуя поле K_2, принадлежащее к группе порядка s, образованной l^h-ыми степенями подстановок группы поля K_1, мы убедимся, что группа поля K_2 есть

циклическая группа порядка l^h. Из того, что дискриминант уравнения $x^p-1=0$ равен

$$N[f'(x)]=N(p\cdot x^{p-1})=\pm p^p,$$

мы видим, что единственным критическим простым числом поля K_1 (и тем более K_2) является p. Поэтому для этих полей p (в силу теоремы 29) p является вполне критическим простым числом.

Рассмотрим композит KK_2 полей K и K_2. Степень его есть делитель произведения l^{2h} степеней полей K и K_2. Его группа есть прямое произведение циклической и абелевой групп порядков l^h и $l^{h'}$ ($h'\leqq h$). Действительно, каждую величину γ поля KK_2 можно представить в виде полинома $\varphi(\alpha,\beta)$, где α — число из K и β — из K_2. Применяя к γ любую подстановку S группы поля KK_2 и обозначая через $\alpha=S_1S_2$ автоморфизмы, которые она производит внутри K и соответственно K_2, мы получим:

$$\gamma^S=\varphi(\alpha^{S_1},\beta^{S_2}).$$

Точно так же для другой подстановки $\overline{S}$:

$$\gamma^{\overline{S}}=\varphi(\alpha^{\overline{S}_1},\beta^{\overline{S}_2}).$$

Но автоморфизмы полей K и K_2 перестановочны, в силу чего

$$\gamma^{S\overline{S}}=\varphi(\alpha^{S_1\overline{S}_1},\beta^{S_2\overline{S}_2})=\varphi(\alpha^{\overline{S}_1S_1},\beta^{\overline{S}_1S_1})=\gamma^{\overline{S}S},$$

что показывает, что группа поля KK_2 абелева. Порядки ее подстановок не могут быть выше $m=l^h$, так как

$$\gamma^{S^m}=\varphi(\alpha^{S_1{}^m},\beta^{S_2{}^m})=\varphi(\alpha,\beta)=\gamma,$$

откуда $S^m=1$. С другой стороны, подстановка, производящая внутри K автоморфизм порядка m, не может иметь порядок ниже m. Поэтому группа поля KK_2 распадается на прямое произведение циклической группы $\mathfrak{A}$ и другой абелевой группы порядка $l^{h'}$ ($h'\leqq h$), структуру которой мы не станем изучать.

Группа инерции $\mathfrak{T}$ критического числа p в поле KK_2 не может быть порядка ниже l^h, так как таков порядок группы инерции его делителей K и K_2. С другой стороны, она не может быть и более высокого порядка, так как p — регулярное простое число, и в силу теоремы 27 его группа инерции циклическая, а группа поля не содержит циклических подгрупп выше l^h-ой степени. Принадлежащее к этой группе поле инерции K_t степени l^h уже не будет иметь p критическим простым числом.

Поля K_t и K_2 не имеют общего иррационального поля, так как для делителей K_t p не критическое простое число, в то время как для всякого делителя K_2 p, будучи единственным критическим простым числом, должно быть вполне критическим. Поэтому группа их композита есть прямое произведение полей

компонентов; его порядок равен $l^{h+h'}$, так что этот композит совпадает с KK_2.

Это показывает, что величины поля K рационально выражаются через корни из единицы и через величины поля K_t, имеющего меньше вполне критических простых чисел. Применяя этот процесс к полю K_t и т. д., мы придем к полю, у которого единственным вполне критическим простым числом будет l.

4. Пусть K — циклическое поле степени $n=l^h$ с единственным вполне критическим простым числом l. Его делитель k l-ой степени принадлежит к подгруппе $\mathfrak{H}$ группы Галуа $\mathfrak{G}$ поля K l^{h-1}-го порядка, состоящей из l-ых степеней элементов группы $\mathfrak{G}$. Так как все числа, кроме l, мы предположим не вполне критическими, то их группы инерции являются делителями группы $\mathfrak{H}$, в силу чего по теореме 28 единственным критическим простым числом поля K является l.

Докажем, что в случае нечетного l существует только одно циклическое поле l-ой степени с единственным критическим числом l. Этим полем, как мы докажем, является делитель l-ой степени поля корней l^2-ой степени из единицы. Это поле имеет дискриминантом делитель числа

$$Nf'(e^{\frac{2\pi i}{l^2}})=\pm l^{2l},$$

где $f(x)=x^{l^2}-1$, а потому l является единственным критическим простым числом. Пусть, кроме этого поля (обозначим его через K_1), существует другое поле K_2 степени l с единственным критическим простым числом l. Образуем его композит K_1K_2. В силу взаимной простоты полей K_1 и K_2 (они различны, и их степень есть простое число), группа поля K_1K_2 есть прямое произведение двух циклических групп порядка l. Так как l есть единственное критическое простое число поля K_1K_2, то в силу теоремы 29 оно должно быть вполне критическим, т. е. его группа инерции должна совпадать с группой Галуа. Так как вместе с тем порядок этой группы есть l^2, то группа инерции совпадает с группой разветвления. Число l должно быть степенью одного простого идеала первой степени:

$$l=\mathfrak{l}^p.$$

Пусть λ есть l-простое число, соответствующее простому идеалу $\mathfrak{l}$. Тогда, как мы видели в § 8.2, для каждой подстановки S группы Галуа имеет место:

$$\lambda^S\equiv\lambda+a\lambda^r \pmod{\mathfrak{l}^{r+1}}, \tag{9.2}$$

где в качестве a может быть взято число из поля инерции, т. е. целое рациональное число, которое можно выбором r сделать взаимно простым с l, т. е. числом ряда $1, 2, \ldots, l-1$. Каждой подстановке S соответствует определенное значение r и a. Так как группа содержит l^2-1 подстановок l-го порядка,

то, предположив, что всем подстановкам соответствует одно и то же значение r, мы получим две подстановки с одним и тем же значением a:

$$\lambda^S\equiv\lambda+a\lambda^r,\ \lambda^{S_1}\equiv\lambda+a\lambda^r \pmod{\mathfrak{l}^{r+1}},$$

откуда

$$\lambda^{SS_1^{-1}}\equiv\lambda \pmod{\mathfrak{l}^{r+1}}.$$

Это показывает, что подстановке SS_1^{-1}, тоже l-го порядка, соответствует более высокое значение r, что противоречит нашему предположению.

Докажем, что это при $l\neq 2$ невозможно, откуда будет следовать невозможность существования двух различных циклических полей с указанными выше свойствами. Для этого сначала рассмотрим произведение $\Lambda=\lambda\cdot\lambda^S\ldots\lambda^{S^{l-1}}$, где

$$\mathfrak{a}=1+S+\ldots+S^{l-1}$$

какая-нибудь подгруппа группы $\mathfrak{G}$. Величина Λ принадлежит к подгруппе $\mathfrak{a}$ и потому входит в некоторое поле l-ой степени. Если $\mathfrak{L}$ простой идеал в этом поле, делящийся на $\mathfrak{l}$, то Λ точно делится на первую степень $\mathfrak{L}$, а $l=\mathfrak{L}^l$. Пусть Λ удовлетворяет уравнению

$$f(\Lambda)=\Lambda^l+a_1\Lambda^{l-1}+\ldots+a_{l-1}\Lambda+a_l=0.$$

Его критическое число l иррегулярно. Если σ подстановка его группы, то

$$\Lambda^\sigma\equiv\Lambda+a\Lambda^\rho \pmod{\Lambda^{\rho+1}},$$

где $\rho\geqq 2$, а a число из ряда $1, 2, \ldots, l-1$. Отсюда получим:

$$\Lambda^{\sigma^i}\equiv\Lambda+ia\Lambda^\rho \pmod{\Lambda^{\rho+1}} \qquad (i=1,2,\ldots,l-1).$$

Поэтому произведение

$$(\Lambda-\Lambda^\sigma)\cdot(\Lambda-\Lambda^{\sigma^2})\ldots(\Lambda-\Lambda^{\sigma^{l-1}})$$

делится точно на $\rho(l-1)$-ую степень $\mathfrak{L}$. Диференцируя тождество

$$f(x)=(x-\Lambda)(x-\Lambda^\sigma)\ldots(x-\Lambda^{\sigma^{l-1}}),$$

получим:

$$(\Lambda-\Lambda^\sigma)(\Lambda-\Lambda^{\sigma^2})\ldots(\Lambda-\Lambda^{\sigma^{l-1}})=$$
$$=l\Lambda^{l-1}+(l-1)a_1\Lambda^{l-2}+\ldots+a_{l-1}.$$

Обозначив через l^{v_i} степень l, на которую точно делится a_i, мы видим, что каждый член правой части делится соответственно на $\mathfrak{L}$ в степени $l+l-1$, $lv_1+l-2, \ldots, lv_{l-1}$. Так как все эти числа различны (различны их остатки от деления на l),

то каждый член правой части должен делиться на $\mathfrak{L}^{\rho(l-1)}$, на который делится левая часть. В частности мы имеем:

$$l+l-1 \geqq \rho(l-1), \quad \rho \leqq 2+\frac{1}{l-1}, \tag{9.2'}$$

откуда при $l>2$ следует

$$\rho=2.$$

Вернемся к числу λ. Оно является корнем полинома

$$(x-\lambda)(x-\lambda^S)\dots(x-\lambda^{S^{l-1}}) = x^l+a_1x^{l-1}+ \\ +\dots+a_{l-1}x+a_l, \tag{9.3}$$

коэфициенты которого не изменяются от подстановок группы a и потому лежат в только-что упомиавшемся поле l-ой степени. В частности, $a_l=\Delta$. Диференцируя (9.3) и подставляя $x=\lambda$, получим:

$$(\lambda-\lambda^S)\dots(\lambda-\lambda^{S^{l-1}}) = l\lambda^{l-1}+(l-1)a_1\lambda^{l-2}+\dots+a_{l-1}. \tag{9.4}$$

Если $\lambda-\lambda^S$ точно делится на $\mathfrak{l}^r$, то левая часть точно делится на $\mathfrak{l}^{r(l-1)}$. Если a_l делится точно на $\mathfrak{l}^{u_i}$ (простой идеал поля коэфициентов $\mathfrak{L}=\mathfrak{l}^l$), то члены правой части делятся на $\mathfrak{l}$ соответственно в степенях

$$l^2+l-1, \quad lu_1+l-2, \dots, lu_{l-1},$$

которые, будучи различны, должны все быть больше чем $r(l-1)$. Отсюда мы заключаем, что все члены равенства

$$\lambda^l+a_1\lambda^{l-1}+\dots+a_{l-1}\lambda+a_l=0, \tag{9.5}$$

кроме первого и последнего, делятся на $\mathfrak{l}^{r(l-1)+1}$.

Возьмем теперь внутри поля подстановку σ такого рода, что $\lambda-\lambda^\sigma$ точно делится на $\mathfrak{l}^{r_1}$, где $r_1>r$.

Заметим, что если α делится на $\mathfrak{l}^k$, то $\alpha-\alpha^\sigma$ делится по крайней мере на $\mathfrak{l}^{k+r_1-1}$. В самом деле, сравнение

$$\lambda^\sigma-\lambda \equiv 0 \pmod{\mathfrak{l}^{r_1-1}}$$

можно переписать так:

$$\frac{\lambda^\sigma}{\lambda}-1 \equiv 0 \pmod{\mathfrak{l}^{r_1-1}},$$

$\frac{\lambda^\sigma}{\lambda}$ является целым по модулю l числом (т. е. после умножения на взаимно простое с l число становится целым). Отсюда

$$\frac{(\lambda^\sigma)^k}{\lambda^k}-1 \equiv 0 \pmod{\mathfrak{l}^{r_1-1}},$$

α можно представить в виде $a_k\lambda_k+a_{k+1}\lambda^{k+1}+\dots+\beta\lambda^u$, где u — сколько угодно высокий показатель, $a_k,\dots,a_{u-1}$—целые рациональные числа, β — целое по модулю l число. Отсюда

$$\alpha^\sigma-\alpha = a_k\lambda^k\left[\frac{(\lambda^\sigma)^k}{\lambda^k}-1\right]+a_{k+1}\lambda^{k+1}\left[\frac{(\lambda^\sigma)^{+k1}}{\lambda^{k+1}}-1\right]+\dots \\ \dots+\lambda^u\left[\beta^\sigma\frac{(\lambda^\sigma)^u}{\lambda^u}-\beta\right] \equiv 0 \pmod{\mathfrak{l}^{k+r_1-1}}.$$

Кроме того,

$$(\lambda^\sigma)^l-\lambda^l = \lambda^l[(1+\gamma\lambda^{r_1-1})^l-1] = \\ = \lambda^l\left[l\gamma\lambda^{r_1-1}+\frac{l(l-1)}{2}\gamma^2\lambda^{2r_1-2}+\dots+\gamma^l\lambda^{l(r_1-1)}\right],$$

откуда в силу $l=\mathfrak{l}^{l2}$ видно, что $(\lambda^\sigma)^l-\lambda^l$ делится на $\mathfrak{l}^v$, где v — меньшее из чисел l^2+l+r_1-1 и lr_1. Применим к равенству (9.5) подстановку σ:

$$(\lambda^\sigma)^l+\alpha_1{}^\sigma(\lambda^\sigma)^{l-1}+\dots+\alpha^\sigma{}_{l-1}\lambda^\sigma+\alpha^\sigma{}_l=0 \tag{9.6}$$

и вычтем (9.6) из (9.5) почленно. Последний член даст: $\alpha_l-\alpha^\sigma{}_l = \Lambda-\Lambda^\sigma=\gamma\cdot\Delta^\rho$, откуда в силу $\rho-2$ следует, что $\alpha_l-\alpha^\sigma{}_l$ точно делится на $\mathfrak{L}^2=\mathfrak{l}^{2l}$. Первая разность разделится на $\mathfrak{l}^v$. Остальные разности, представляя разность $\alpha-\alpha^\sigma$ для числа α, делящегося на $\mathfrak{l}^{r(l-1)+1}$, разделятся по крайней мере на $\mathfrak{l}^{r(l-1)+r_1}$. Отсюда следует, что по крайней мере один из показателей l^2+l+r_1-1, lr_1, $r(l-1)+r_1$ должен не превышать $2l$, т. е. что должно иметь место одно из равенств

$$l^2+l+r_1-1 \leqq 2l$$
$$lr_1 \leqq 2l$$
$$r(l-1)+r_1 \leqq 2l.$$

Первое неравенство дает $l(l-1)+(r_1-1)\leqq 0$ и потому невозможно.

Остальные равенства в силу $r\geqq 2$ приводят к $r_1\leqq 2$, что в силу $r_1>r\geqq 2$ невозможно. Таким образом существует только одно циклическое поле l-ой степени с единственным критическим числом l.

5. В случае $l=2$ формула (9.2') дает нам $\rho_0\leqq 3$, в чем нет ничего недопустимого. Для этого случая проще всего решить вопрос элементарным путем. Найдем все квадратичные поля $K(\sqrt{d})$, у которых только 2 является критическим простым числом. Можно предположить, что каждый простой множитель входит в d в первой степени. Если бы в d входил нечетный

простой множитель p, то p было бы для $K(\sqrt{d})$ критическим простым числом, так как число $\sqrt{d}$ не делится на p, а его квадрат делится. Поэтому в d может входить множителем только 2, и мы приходим к трем следующим возможным типам квадратичных полей с единственным критическим числом 2:

$$K(\sqrt{-1}),\ K(\sqrt{-2}),\ K(\sqrt{2}). \tag{9.7}$$

Из этих полей только третье вещественно.

6. Пусть K—циклическое поле l^h-ой степени с единственным вполне критическим числом l. Построим другое поле K_2 того же типа, взяв делитель поля l^{h+1}-ых корней из единицы, принадлежащей к её подгруппе порядка $l-1$. В случае $l=2$ возьмем поле 2^{h+2}-ых корней из единицы. Оно имеет степень 2^{h+1}. Его группа есть прямое произведение циклических групп порядков 2^h и 2. К последней принадлежит вещественное циклическое поле 2^h-ой степени (см. часть I, стр. 111—112, § 2.5). Так как существует только одно (в случае $l=2$ притом вещественное) поле l-ой степени с единственным критическим простым числом l, то поля K и K_2 содержат общее поле kl-ой степени (ведь группы инерции, соответствующие другим, не вполне критическим простым числам поля K, являются делителями подгруппы порядка l^{h-1} его группы Галуа, в силу чего эти простые числа не являются критическими для K). Поэтому композит KK_2 имеет степень $l^{h+h'}$, где $h' \leqq h-1$. Обозначая через A тот автоморфизм поля KK_2, который, будучи применен к полю K_2, воспроизводит его примитивный (т. е. порядка l^h) автоморфизм, мы убедимся, что порядок A равен l^h (так как l^h-ая степень всякого автоморфизма поля KK_2 воспроизведет среди величин K и K_2 тождественный автоморфизм, а потому она не будет менять и величин поля KK_2). Разлагая группу $\mathfrak{G}$ поля KK_2 на сопряженные системы по подгруппе

$$\mathfrak{A} = 1 + A + A^2 + \ldots + A^{l^h-1};$$
$$\mathfrak{G} = \mathfrak{A} + \mathfrak{A}B_2 + \ldots + \mathfrak{A}B_{l^{h'}}$$

и нормируя элементы B_i так, чтобы они составили группу (см. часть I, стр. 43—44, теорема 30,2), мы разложим группу $\mathfrak{G}$ на прямое произведение:

$$\mathfrak{G} = \mathfrak{A} \times \mathfrak{B}.$$

Элемент A группы $\mathfrak{G}$ воспроизводит также автоморфизм поля k, в силу чего поле K_3, принадлежащее внутри KK_2 к $\mathfrak{A}$, не содержит поля k. Поэтому поля K_2 и K_3 взаимно просты (их общее иррациональное поле содержало бы поле степени l, а таковым у K_2 является только k) и, будучи степеней l^h и $l^{h'}$, воспроизводят все поле KK_2. Таким образом величины поля K рационально выражаются через величины поля K_2, т. е. через

корни из единицы, и величины поля K_3, имеющего более низкую степень.

Применяя тот же процесс к полю K_1 и т. д., мы окончательно выразим величины поля K через корни из единицы. Это доказывает теорему 30.

§ 10. Группы разложения

1. *Группой разложения* простого идеала $\mathfrak{P}$ в нормальном поле K называется совокупность автоморфизмов, не меняющих идеала $\mathfrak{P}$. Группа разложения содержит группу инерции. При доказательстве теоремы 26 мы видели, что среди автоморфизмов группы разложения $\mathfrak{Z}$ содержится такой Z, для которого имеет место при всяком целом числе α из K:

$$\alpha^Z \equiv \alpha^p \pmod{\mathfrak{P}}. \tag{10.1}$$

Его степени $Z^2, Z^3, \ldots, Z^{f-1}$, где f—степень простого идеала $\mathfrak{P}$, переводят α в величины, сравнимые соответственно с $\alpha^{p^2}, \alpha^{p^3}, \ldots, \alpha^{p^{f-1}}$. Z^f переводит α в α^{p^f}, и в силу обобщенной теоремы Ферма

$$\alpha^{Z^f} \equiv \alpha^{p^f} \equiv \alpha \pmod{\mathfrak{P}}, \tag{10.2}$$

откуда следует, что Z^f лежит в группе инерции $\mathfrak{T}$.

Совокупность автоморфизмов

$$\mathfrak{T} + \mathfrak{T}Z + \mathfrak{T}Z^2 + \ldots + \mathfrak{T}Z^{f-1} \tag{10.3}$$

дает mf различных автоморфизмов группы $\mathfrak{Z}$, а так как мы видели при доказательстве теоремы 26, что порядок группы $\mathfrak{Z}$ равен $m \cdot f$, то отсюда следует, что автоморфизмы (10.3) исчерпывают собой всю группу $\mathfrak{Z}$.

Докажем, что группа $\mathfrak{T}$ есть нормальный делитель группы $\mathfrak{Z}$. Пусть T — произвольная подстановка из $\mathfrak{T}$. Тогда

$$\alpha^T \equiv \alpha,\ \alpha^Z \equiv \alpha^p,\ Z^{-1} \equiv \alpha^{p^{f-1}} \pmod{\mathfrak{P}}.$$

Отсюда

$$\alpha Z^{-1} TZ \equiv (\alpha^{Z^{-1}} T)^p \equiv (\alpha^{Z^{-1}})^p \equiv \alpha^{p^{f-1}p} \equiv \alpha^{p^f} \equiv \alpha \pmod{\mathfrak{P}},$$

что доказывает, что $Z^{-1}TZ$ совпадает с T, т. е, что $\mathfrak{T}$ есть нормальный делитель группы $\mathfrak{Z}$. Итак мы имеем:

Теорема 31. Группа разложения $\mathfrak{Z}$ простого идеала $\mathfrak{P}$ в нормальном поле K имеет группу инерции $\mathfrak{T}$ нормальным делителем. Дополнительная группа $\mathfrak{Z}/\mathfrak{T}$ циклическая, и ее порядок равен степени f простого идеала $\mathfrak{P}$.

2. В том случае, когда идеал $\mathfrak{P}$ не критический, т. е. когда $\mathfrak{T}=1$, идеалу $\mathfrak{P}$ соответствует одна и только одна подстановка Z, для которой имеет место

$$\alpha^Z \equiv \alpha^p \pmod{\mathfrak{P}}. \tag{10.4}$$

В самом деле, если наряду с (10.4) имеет также место

$$\alpha^Z \equiv \alpha^p \pmod{\mathfrak{P}}, \tag{10.5}$$

то

$$\alpha^{ZZ_1^{-1}} \equiv (\alpha^p)^{Z_1^{-1}} \equiv \alpha \pmod{\mathfrak{P}},$$

откуда следует, что ZZ_1^{-1} лежит в $\mathfrak{T}$, т. е. в силу нашего предположения $ZZ_1^{-1} = 1$. Будем говорить, что простой идеал $\mathfrak{P}$ *принадлежит* к автоморфизму Z.

Если $\mathfrak{P}$ принадлежит к Z, то $\mathfrak{P}^s$ принадлежит к автоморфизму $S^{-1}ZS$. В самом деле, применим (9.4) к $\alpha^{S^{-1}}$:

$$\alpha^{S^{-1}ZS} \equiv (\alpha^{S^{-1}})^p \pmod{\mathfrak{P}},$$

и произведем над этим сравнением автоморфизм S:

$$\alpha^{S^{-1}ZS} \equiv \alpha^p \pmod{\mathfrak{P}},$$

что доказывает наше утверждение.

Таким образом, если

$$\mathfrak{G} = \mathfrak{Z} + \mathfrak{Z}S_2 + \ldots + \mathfrak{Z}S_\nu$$

то всем различным сопряженным с $\mathfrak{P}$ простым идеалам $\mathfrak{P}$, $\mathfrak{P}^{S_2}, \ldots \mathfrak{P}^{S^\nu}$ соответствуют все сопряженные с Z автоморфизмы

$$Z,\ S_2^{-1}ZS_2, \ldots,\ S_\nu^{-1}ZS_\nu,$$

образующие, как мы будем говорить, *класс* автоморфизма Z. Будем говорить, что простое число, p которое является произведением простых идеалов, сопряженных с $\mathfrak{P}$, *принадлежит к классу* автоморфизма Z.

Гассе (H. Hasse) ввел для обозначения автоморфизма, к которому принадлежит простой идеал $\mathfrak{P}$, символ $\left[\frac{K}{\mathfrak{P}}\right]$, а для класса автоморфизмов, к которому принадлежит простое число p, символ $\left(\frac{K}{p}\right)$. Таким образом мы имеем:

$$\alpha^{\left[\frac{K}{\mathfrak{P}}\right]} \equiv \alpha^p \pmod{\mathfrak{P}}. \tag{10.6}$$

3. Рассмотрим наряду с нормальным полем K его делитель k, принадлежащий к подгруппе $\mathfrak{H}$ его группы $\mathfrak{G}$. Исследуем, на какие неприводимые по модулю p множители распадается полином, корнем которого является примитивная величина α поля k. Чтобы α удовлетворяло неприводимому по модулю $\mathfrak{P}$ сравнению степени f с рациональными коэфициентами, необходимо и достаточно, чтобы $\equiv$ оно удовлетворяло сравнению

$$\alpha^{p^f} \equiv \alpha \pmod{\mathfrak{P}} \tag{10.7}$$

и не удовлетворяло подобным сравнениям при меньших значениях f. Но в силу $\alpha^p \equiv \alpha^Z \pmod{\mathfrak{P}}$ сравнение (10.7) равносильно следующему сравнению:

$$\alpha^{Z^f} \equiv \alpha \pmod{\mathfrak{P}}. \tag{10.8}$$

Если мы предположим, что α выбрано в k так, чтобы его дискриминант не делился на p (это всегда можно сделать, если p не входит ни в дискриминант, ни в индекс поля k), то сравнение (10.8) возможно только в том случае, если Z^f не меняет величины α т. е. входит в $\mathfrak{H}$. Можно также охарактеризовать число f как число сопряженных систем $\mathfrak{H}S$, содержащихся в комплексе $\mathfrak{H}\mathfrak{Z}$ (см. часть I, стр. 137—138). Разлагая $\mathfrak{G}$ на комплексы по двум подгруппам $\mathfrak{E}$ и $\mathfrak{Z}$:

$$\mathfrak{G} = \mathfrak{H}\mathfrak{Z} + \mathfrak{H}S_2\mathfrak{Z} + \ldots + \mathfrak{H}S_k\mathfrak{Z}, \tag{10.9}$$

мы видим, что число сопряженных систем $\mathfrak{H}S$ в каждом комплексе

$$\mathfrak{H}S_i\mathfrak{Z} = \mathfrak{H} \cdot S_i\mathfrak{Z} \cdot S_i^{-1} \cdot S_i$$

равно показателю наименьшей степени $S_iZS_i^{-1}$, входящей в $\mathfrak{H}$ (или, что то же, показателю наименьшей степени Z, входящей в $S_i^{-1}\mathfrak{H}S_i$, т. е. степени неприводимого сравнения, которому удовлетворяет α по модулю $\mathfrak{P}^{S_i}$ (или $\alpha^{S_i^{-1}}$ по модулю $\mathfrak{P}$).

Если $f(\alpha) = 0$ и $f(x) \equiv f_1(x) \cdot f_2(x) \ldots f_k(x) \pmod{p}$, то $f_1(\alpha) \times \times f_2(\alpha) \ldots f_k(\alpha) = p \cdot \psi(\alpha)$. Если мы предположим, что p не входит в индекс поля, то $\psi(\alpha)$ взаимно просто с p. С другой стороны, $f_i(x)$ не взаимно просты с $f(x)$ по модулю p, в силу чего каждое число $f_i(\alpha)$ должно делиться на какой-нибудь простой идеальный множитель $\mathfrak{p}_i$ поля k. Из того, что

$$f_i(\alpha) \equiv 0 \pmod{\mathfrak{P}^{S_i}}$$

есть сравнение наименьшей степени, которому удовлетворяет α, мы заключаем, что все классы сравнений по модулю $\mathfrak{P}^{S_i}$ (и значит по модулю простого идеала $\mathfrak{p}$ из k, делящегося на $\mathfrak{P}^{S_i}$) внутри k исчерпываются представителями

$$c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{f_i-1}\alpha^{f_i-1} \qquad (c_i = 0, 1, \ldots, p-1),$$

и их число, т. е. $N\mathfrak{p}_i$, равно p^{f_i}. Беря норму от обеих частей:

$$f_1(\alpha) \cdot f_2(\alpha) \ldots f_\kappa(\alpha) = p\,\psi(\alpha),$$

мы в левой части получим по *крайней мере* $p^{f_1} + f^2 + \ldots + f_k = p^n$ в виде множителя, а в правой части *точно* p^n. Из этого вытекает, что $f_i(\alpha)$ не делится, кроме $\mathfrak{p}_i$, ни на какой другой идеальный множитель числа p, так что $N(\mathfrak{p}_i) = p^{f_i}$.

Рассмотрим разложение $\mathfrak{G}$ по двойному модулю $\mathfrak{Z}$ и $\mathfrak{H}$:

$$\mathfrak{G} = \mathfrak{Z}\mathfrak{H} + \mathfrak{Z}S_2\mathfrak{H} + \ldots + \mathfrak{Z}S_\kappa\mathfrak{H}.$$

Если

$$\mathfrak{Z}S_i\mathfrak{H}=\mathfrak{Z}S_{i1}+\mathfrak{Z}S_{i2}+\ldots+\mathfrak{Z}S_{ir_i},$$

где

$$r_i=\frac{f_i h}{f},$$

h — порядок группы $\mathfrak{H}$ и f — порядок группы $\mathfrak{Z}$, то идеал

$$\mathfrak{P}^{s_{i1}}\mathfrak{P}^{s_{i2}}\ldots,\mathfrak{P}^{s_{ir_i}} \tag{10.10}$$

инвариантен относительно k, а потому, не будучи критическим, он является идеалом поля k. Вместе с тем норма этого идеала внутри K равна $p^{fr_i}=p^{f_i h}$, а внутри k равна p^{f_i}, так как степень поля k в h раз меньше, чем степень поля K. Поэтому идеал (10.10) должен совпасть с простым идеалом $\mathfrak{p}_i$, поля k. Этот факт дает нам рецепт для получения простых идеалов внутри делителей нормального поля.

§ 11. Теорема Штикельбергера—Вороного

1. Для формулировки нижеследующей теоремы, открытой Штикельбергером (Stickelberger) и независимо от него Вороным, необходимо ввести понятие *квадратичного вычета*. Целое рациональное число a называется *квадратичным вычетом* относительно простого числа p, взаимно простого с a, если сравнение

$$z^2-a\equiv 0 \pmod p \tag{11.1}$$

имеет рациональные корни. В противном случае, т. е. если полином z^2-a неприводим по модулю p, говорят, что a есть *невычет* относительно p.

Для обозначения этого свойства числа a Лежандр (A. M. Legendre) ввел символ $\left(\frac{a}{p}\right)$, полагая $\left(\frac{a}{p}\right)=+1$, если a вычет, и $\left(\frac{a}{p}\right)=-1$, если невычет относительно p.

2. Если a есть вычет относительно p, т. е. если существует целое рациональное число b такого рода, что

$$a\equiv b^2 \pmod p,$$

то, возводя это сравнение в степень $\frac{p-1}{2}$ и применяя теорему Ферма, получим:

$$a^{\frac{p-1}{2}}\equiv 1 \pmod p. \tag{11.2}$$

Обратно, если a удовлетворяет сравнению (11.2), то оно есть вычет.

В самом деле, a всегда сравнимо с некоторой степенью первообразного корня g:

$$a\equiv g^k \pmod p.$$

Подставляя в (11.2), получим:

$$g^{k\frac{p-1}{2}}\equiv 1 \pmod p. \tag{11.3}$$

Но в силу того, что g есть первообразный корень, сравнение (11.3) может иметь место только в том случае, если показатель $k\frac{p-1}{2}$ делится на $p-1$, т. е. если k делится на 2 (см. часть I, стр. 206—208). Пусть $k=2k_1$. Тогда число g^k является корнем сравнения (11.1).

Теорему Ферма можно формулировать так: все числа 1, 2, ..., $p-1$ являются корнями сравнения

$$x^{p-1}-1\equiv\left(x^{\frac{p-1}{2}}-1\right)\left(x^{\frac{p-1}{2}}+1\right)\equiv 0 \pmod p. \tag{11.4}$$

Из них те, которые являются вычетами относительно p, обращают в нуль первый множитель, $x^{\frac{p-1}{2}}-1$ (их таким образом всего $\frac{p-1}{2}$). Остальные $\frac{p-1}{2}$ должны быть корнями $x^{\frac{p-1}{2}}+1\equiv 0 \pmod p$ и являются невычетами. Таким образом число невычетов тоже равно $\frac{p-1}{2}$, и все они удовлетворяют условию

$$a^{\frac{p-1}{2}}\equiv -1 \pmod p.$$

Сопоставляя (11.2) и (11.5) с определением символа $\left(\frac{a}{p}\right)$, получаем:

$$a^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right) \pmod p. \tag{11.6}$$

3. Теорема 32 (Штикельбергера—Вороного). Если неприводимое уравнение n-ой степени

$$f(x)=0 \tag{11.7}$$

разлагается по модулю p на k неприводимых по модулю p множителей:

$$f(x)\equiv f_1(x)\cdot f_2(x)\ldots f_k(x) \pmod p \tag{11.8}$$

и дискриминант D уравнения (11.7) не делится на p, то имеет место

$$\left(\frac{D}{p}\right)=(-1)^{n-k}. \tag{11.9}$$

Доказательство. 1. Сначала рассмотрим случай, когда $k=1$, т. е. когда сравнение

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

неприводимо по модулю p. В части I, стр. 165, доказано, что группа этого сравнения циклическая. Она является делителем знакопеременной группы в том и только в том случае, если n есть нечетное число (см. часть I, стр. 22). В силу этого дискриминант D сравним по модулю p с точным квадратом в том и только в том случае, если n нечетно. Это можно записать так:

$$\left(\frac{D}{p}\right)=(-1)^{n-1}. \tag{11.10}$$

2. Рассмотрим общий случай, когда неприводимые по модулю p множители $f_i(x)$ полинома $f(x)$ имеют степень n_i, так что

$$n_1+n_2+\ldots+n_k=n. \tag{11.11}$$

Пусть $D_1, D_2, \ldots, D_k$ будут дискриминанты этих множителей. Формула (1.15) части I, стр. 65, дает для дискриминанта D полинома $f(x)$ следующее выражение:

$$D=D_1\cdot D_2\ldots D_k\cdot R^2, \tag{11.12}$$

где R — некоторое целое рациональное число.

Из формулы (11.6) вытекает:

$$\left(\frac{a\cdot b}{p}\right)\equiv (ab)^{\frac{p-1}{2}}\equiv a^{\frac{p-1}{2}}b^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\pmod p,$$

откуда

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right). \tag{11.13}$$

Применяя этот результат к формуле (11.12) и имея в виду, что

$$\left(\frac{R}{p}\right)^2=\left(\frac{R}{p}\right)\cdot\left(\frac{R}{p}\right)=+1,$$

получим:

$$\left(\frac{D}{p}\right)=\left(\frac{D_1}{p}\right)\cdot\left(\frac{D_2}{p}\right)\ldots\left(\frac{D_k}{p}\right). \tag{11.14}$$

Применяя к каждому из полиномов $f_i(x)$ формулу (11.10), получим:

$$\left(\frac{D}{p}\right)=(-1)^{n_1-1}(-1)^{n_2-1}\ldots(-1)^{n_k-1}=(-1)^{n-k}, \tag{11.15}$$

ч. и т. д.

§ 12. Группы разложения в полях деления круга. Закон взаимности

1. В полях деления круга вопрос, какова группа разложения данного простого числа, решается весьма просто. Сначала рассмотрим поле $K\left(e^{\frac{2\pi i}{n}}\right)$ n-ых корней из единицы. Пусть $k_1=1, k_2, \ldots, k_s$ будут все взаимно простые с n и не превышающие n числа $[s=\varphi(n)]$. Тогда сопряженными с $e^{\frac{2\pi i}{n}}$ величинами поля являются

$$e^{\frac{2\pi i}{n}},\ e^{\frac{2k_2\pi i}{n}},\ \ldots,e^{\frac{2k_s\pi i}{2}}. \tag{12.1}$$

Переход от $e^{\frac{2\pi i}{n}}$ к какой-нибудь из этих величин соответствует одному и только одному автоморфизму поля, так как в нормальном поле переход одной примитивной величины вполне определяет автоморфизм. Возьмем некритическое простое число p и зададимся вопросом, к какому автоморфизму оно принадлежит. Наименьшим положительным вычетом числа p (будучи некритическим, оно взаимно просто с p) по модулю n должно быть одно из чисел $k_1, k_2, \ldots, k_s$. Пусть

$$p\equiv k_u \pmod n. \tag{12.2}$$

Тогда

$$e^{\frac{2\pi ip}{n}}=e^{\frac{2k_u\pi i}{n}}.$$

Применяя теорему Шенемана (см. часть I, стр. 110), получим для любой величины $\varphi\left(e^{\frac{2\pi i}{n}}\right)$ нашего поля:

$$\left[\varphi\left(e^{\frac{2\pi i}{n}}\right)\right]^p\equiv\varphi\left(e^{\frac{2k_u\pi i}{n}}\right)\pmod p, \tag{12.3}$$

откуда следует, что p принадлежит к тому автоморфизму поля, который переводит $e^{\frac{2\pi i}{n}}$ в $e^{\frac{2k_u\pi i}{n}}$, если p лежит в арифметической прогрессии $nx+k_u$.

Чтобы узнать, каков порядок группы разложения простого числа p, нужно определить наименьший показатель f, который дает

$$p^f\equiv 1 \pmod n, \tag{12.4}$$

или, что то же,

$$kf_u\equiv 1 \pmod n. \tag{12.5}$$

В частности, p принадлежит к единичному автоморфизму в том и только в том случае, если

$$p \equiv 1 \pmod{p}. \tag{12.6}$$

2. Рассмотрим общий случай, когда поле k есть делитель поля $K\left(e^{\frac{2\pi i}{n}}\right)$. Пусть k принадлежит внутри $K\left(e^{\frac{2\pi i}{n}}\right)$ к группе $\mathfrak{H}$, автоморфизмы которой переводят $\varepsilon = e^{\frac{2\pi i}{n}}$ в

$$\varepsilon, \varepsilon^{k_2}, \ldots, \varepsilon^{k_m}.$$

Если $\varphi(\varepsilon)$ есть примитивная величина поля k, то

$$\varphi(\varepsilon) = \varphi(\varepsilon^{k_2}) = \ldots = \varphi(\varepsilon^{k_m}), \tag{12.7}$$

в то время как $\varphi(\varepsilon) \neq \varphi(\varepsilon^k)$, если k не входит в систему $1, k_2, \ldots, k_m$. Порядок группы разложения некритического простого числа p равен наименьшему показателю f, дающему

$$[\varphi(\varepsilon)]^{p^f} \equiv \varphi(\varepsilon) \pmod{p}. \tag{12.8}$$

Но в силу теоремы Шенемана

$$[\varphi(\varepsilon)]^{p^f} \equiv \varphi(\varepsilon^{p^f}) \pmod{p},$$

а потому в силу (12.7) для того, чтобы имело место (12.8), необходимо и достаточно, чтобы ε^{p^f} равнялось одному из чисел $\varepsilon, \varepsilon^{k_2}, \ldots, \varepsilon^{k_m}$ (в силу некритичности p сравнение $\varepsilon^{p^f} \equiv \varepsilon^{k_u} \pmod{p}$) может иметь место только в случае равенства $\varepsilon^{p^f} = \varepsilon^{k_u}$, а для этого необходимо и достаточно, чтобы p^f было сравнимо по модулю n с одним из чисел $1, k_2, \ldots, k_m$, т. е. чтобы p^f лежало в одной из прогрессий

$$nx+1,\ nx+k_2, \ldots, nx+k_m. \tag{12.9}$$

В частности, p принадлежит внутри k к единичному автоморфизму тогда и только тогда, если оно лежит в одной из прогрессий (12.9).

3. Применим последние соображения, а также теорему 32, к выводу *закона взаимности* для квадратичных вычетов, т. е. формулы

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right), \tag{12.10}$$

имеющей место для любых двух нечетных простых чисел p и q. Закон взаимности был впервые строго доказан Гауссом (C. F. Gauss). Настоящий же вывод принадлежит Мириманову.

Рассмотрим поле q-ых корней из единицы, т. е. поле рациональных функций от корня ε неприводимого уравнения

$$f(x) = x^{q-1} + x^{q-2} + \ldots + x + 1 = 0. \tag{12.11}$$

Его дискриминант [будем называть здесь дискриминантом произведение квадратов разностей корней уравнения (12.11)] равен

$$D = (-1)^{\frac{q(q-1)}{2}} \cdot f'(\varepsilon) \cdot f'(\varepsilon^2) \ldots f'(\varepsilon^{q-1}). \tag{12.12}$$

Но

$$f(x) = \frac{x^q - 1}{x - 1},$$

откуда

$$f'(x) = -\frac{x^q - 1}{(x-1)^2} + \frac{q \cdot x^{q-1}}{x-1},$$

$$f'(\varepsilon^k) = \frac{q\,\varepsilon^{k(q-1)}}{\varepsilon^k - 1},$$

$$D = (-1)^{\frac{q(q-1)}{2}} \cdot \frac{q \cdot \varepsilon^{q-1} \cdot q \cdot \varepsilon^{2(q-1)} \ldots q \cdot \varepsilon^{(q-1)^2}}{(\varepsilon-1)(\varepsilon^2-1)\ldots(\varepsilon^{q-1}-1)} =$$

$$= (-1)^{\frac{q(q-1)}{2}} \cdot \frac{q^{q-1} \cdot \varepsilon^{\frac{q(q-1)^2}{2}}}{(-1)^{q-1}(1-\varepsilon)(1-\varepsilon^2)\ldots(1-\varepsilon^{q-1})} =$$

$$= (-1)^{\frac{q(q-1)}{2}} \cdot \frac{q^{q-1}}{f(1)} = (-1)^{\frac{q(q-1)}{2}} \cdot q^{q-2} = (-1)^{\frac{q-1}{2}} \cdot q^{q-2}. \tag{12.13}$$

Поэтому, принимая во внимание, что $q-2$ нечетное число и что в силу (11.6) имеет место

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \tag{12.14}$$

получим:

$$\left(\frac{D}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right). \tag{12.15}$$

Пусть f есть порядок группы разложения числа p. Это означает, что f есть наименьший показатель, дающий

$$p^f \equiv 1 \pmod{q}. \tag{12.16}$$

$\left(\frac{p}{q}\right) = +1$ в том и только в том случае, если $p^{\frac{q-1}{2}} \equiv 1 \pmod{q}$ т. е. если $\frac{q-1}{2}$ делится на f, иначе говоря, если $\frac{q-1}{f}$ есть четное число. Поэтому

$$\left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{f}}. \tag{12.17}$$

Но f есть степень неприводимых по модулю p делителей полинома $f(x)$, а потому их число равно $\frac{q-1}{f}$, откуда в силу теоремы 32

$$\left(\frac{D}{p}\right)=(-1)^{q-1-\frac{q-1}{f}}=(-1)^{\frac{q-1}{f}}. \tag{12.18}$$

Сопоставляя (12.17) с (12.18), имеем:

$$\left(\frac{D}{p}\right)=\left(\frac{p}{q}\right),$$

а подставляя в (12.15), получим:

$$\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot\left(\frac{q}{p}\right), \tag{12.19}$$

ч. и т. д,

4. Чтобы вычислить $\left(\frac{2}{p}\right)$, рассмотрим уравнение (12.20)

$$x^2-2=0. \tag{12.20}$$

Его корень можно выразить так: $\sqrt{2}=\varepsilon+\varepsilon^{-1}$, где $\varepsilon=e^{\frac{\pi i}{4}}$. Применим результаты § 12.2. Группа $k(\varepsilon)$ состоит из единицы и автоморфизма, переводящего ε в ε^{-1}, а потому корни сравнения $x^2-2\equiv 0 \pmod p$ рациональны тогда и только тогда, если p лежит в одной из прогрессий

$$8x+1, \qquad 8x-1.$$

Замечая, что в этом случае $\frac{p^2-1}{8}$ четное, в то время как в других случаях, т. е. когда $p=8x+3$ или $p=8x-3$, оно нечетно, имеем:

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}. \tag{12.21}$$

Формулы (12.14) и (12.21) называются дополнительными формулами к закону взаимности. Они позволяют приводить символы $\left(\frac{p}{q}\right)$ к символам с меньшими значениями p, q во всех случаях.

Пример. $\left(\frac{41}{59}\right)$ в силу (12.19) равен $\left(\frac{59}{41}\right)$. Вычитая из числителя кратность 41, получим

$$\left(\frac{18}{41}\right)=\left(\frac{2}{41}\right)\cdot\left(\frac{9}{41}\right).$$

Но $\left(\frac{2}{41}\right)=(-1)^{\frac{41^2-1}{8}}=+1$ в силу формул (12.21), а $\left(\frac{9}{41}\right)=+1$ в силу того, что 9 есть точный квадрат. Отсюда

$$\left(\frac{41}{59}\right)=+1.$$

На практике символы Лежандра вычисляют при помощи обобщенного символа Якоби, применимого и к составным числам и потому избавляющего от необходимости разлагать числители на простые множители.

Глава II

АНАЛИТИЧЕСКАЯ ТЕОРИЯ ИДЕАЛОВ

§ 1. Идеальные классы. Конечность их числа

1. Будем называть два идеала $\mathfrak{a}$ и $\mathfrak{b}$ какого-нибудь алгебраического поля k ***эквивалентными***, если существуют два таких целых числа α, β поля k, что имеет место

$$\beta\mathfrak{a} = \alpha\mathfrak{b}. \tag{1.1}$$

Вводя понятие дробных идеалов, мы можем также выразиться об эквивалентных идеалах так: их частное равно числу поля. Из этого вытекают следующие очевидные предложения:

I. Идеал эквивалентен самому себе *(рефлексивность* понятия).

II. Два идеала, эквивалентные одному и тому же третьему идеалу, эквивалентны друг другу (транзитивность понятия).

III. Если идеал $\mathfrak{a}$ эквивалентен $\mathfrak{b}$, а $\mathfrak{c}$—эквивалентен $\mathfrak{d}$, то и произведения $\mathfrak{ac}$ и $\mathfrak{bd}$ эквивалентны.

IV. Все главные идеалы эквивалентны друг другу.

2. Объединим все эквивалентные друг другу идеалы в один *идеальный класс*, говоря, что эквивалентные идеалы лежат в одном классе. Главные идеалы образуют *главный класс*. Имеет место важная

Теорема 33. В каждом поле k существует лишь конечное число идеальных классов.

Доказательство. Докажем, что в каждом классе можно выбрать идеал, норма которого не превышает некоторого конечного числа. Мы видели в § 3.17, что для каждого идеала можно найти базис $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$, так что все числа идеала будут выражаться в форме

$$\mu_0 x_0 + \mu_1 x_1 + \ldots + \mu_{n-1} x_{n-1},$$

где $x_0, x_1, \ldots, x_{n-1}$ пробегают все целые рациональные значения. Дискриминант этого базиса равен дискриминанту поля k, умноженному на квадрат определителя линейной подстановки, переводящей в $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$ фундаментальный базис $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ поля (см. § 2.4). Вместе с тем при доказательстве теоремы 18 мы убедились, что этот определитель равен норме рассматриваемого идеала.

Рассмотрим идеал $\mathfrak{a}$. Возьмем другой идеал $\mathfrak{b}$ такого рода, что произведение $\mathfrak{a}\cdot\mathfrak{b}$ есть главный идеал. Идеалы $\mathfrak{c}$, дающие при умножении на $\mathfrak{b}$ главные идеалы, эквивалентны идеалам $\mathfrak{a}$, так как из

$$\mathfrak{ab} = \alpha, \qquad \mathfrak{bc} = \gamma$$

следует:

$$\alpha\mathfrak{c} = \gamma\mathfrak{a}.$$

Найдем внутри идеала $\mathfrak{a}$ число γ, норма которого не превышает конечного числа. Для этого применим теорему 23 к системе форм

$$\left.\begin{aligned} y_0 &= \mu_0 x_0 + \mu_1 x_1 + \ldots + \mu_{n-1} x_{n-1} \\ y_1 &= \mu_0' x_0 + \mu_1' x_1 + \ldots + \mu'_{n-1} x_{n-1} \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ y_{n-1} &= \mu_0^{(n-1)} x_0 + \mu_1^{(n-1)} x_1 + \ldots + \mu_{n-1}^{(n-1)} x_{n-1}, \end{aligned}\right\} \tag{1.2}$$

где $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$ — базис идеала $\mathfrak{a}$ и $\mu_i\ \mu_i', \ldots, \mu_i^{n-1}$—сопряженные с μ_i числа. Определитель δ системы (1.2) по абсолютной величине равен квадратному корню из дискриминанта базиса, т. е.

$$|\delta| = |N(\mathfrak{a})| \cdot \sqrt{|D|}, \tag{1.3}$$

где D—дискриминант поля k. В силу теоремы 23 можно выбрать для $x_0, x_1, \ldots, x_{n-1}$ такие целые рациональные значения, чтобы имело место

$$|y_i| \leqq \sqrt[n]{|\delta|} \qquad (i = 0, 1, 2, \ldots, n-1). \tag{1.4}$$

Вводя обозначение $y_0 = \gamma$, мы в силу (1.4) будем иметь:

$$|N(\gamma)| = |\gamma\cdot\gamma'\ldots\gamma^{(n-1)}| = |y_0 y_1 \ldots y_{n-1}| \leqq |\delta|. \tag{1.5}$$

Но γ может быть представлено через базис $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$, т. е. делится на идеал $\mathfrak{a}$. Полагая $\gamma = \mathfrak{ab}$, будем в силу (1.3) иметь

$$|N(\gamma)| = |N(\mathfrak{a})| \cdot |N(\mathfrak{b})| \leqq |N(\mathfrak{a})| \sqrt{|D|}.$$

откуда

$$|N(\mathfrak{b})| \leqq \sqrt{D}. \tag{1.6}$$

Вместе с тем идеал $\mathfrak{b}$ эквивалентен идеалу $\mathfrak{a}^{-1}$. Поэтому внутри каждого идеального класса мы можем найти по представителю, норма которого подчинена неравенству (1.6). Но число идеалов, нормы которых не превышают определенного числа, конечно. Поэтому и число идеальных классов поля k конечно, ч. и т. д.

Число идеальных классов является весьма важным числом, связанным с полем, и его вычислению посвящено много усилий. Доказательство „великой теоремы Ферма" связано с определением числа классов для некоторых полей деления круга.

3. Из свойства III следует, что произведения $\mathfrak{a} \cdot \mathfrak{b}$, где идеалы $\mathfrak{a}$, $\mathfrak{b}$ пробегают всевозможные идеалы определенных классов A, B, лежат в одном и том же классе, который мы будем называть *произведением* $A \cdot B$ классов A и B. Установленный таким образом способ умножения классов определяет группу классов относительно умножения. Из теоремы 33 следует, что эта группа конечна. Эта группа абелева, так как произведение идеалов не зависит от порядка множителей.

4. Число идеальных классов имеет значение в другом вопросе — проблеме эквивалентности матриц. Чтобы показать это, обратим внимание на то, что каждому базису идеала соответствует представление целых чисел поля в виде определенных матриц. В самом деле, пусть $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$ будет базис какого-нибудь идеала и θ — какое-нибудь целое число поля. В силу свойств идеалов числа $\mu_0\theta, \mu_1\theta, \ldots, \mu_{n-1}\theta$ тоже входят в идеал, а потому выражаются с целыми координатами через базис. Пусть

$$\left.\begin{aligned} \mu_0\theta &= a_{00}\mu_0 + a_{01}\mu + \ldots + a_{0,n-1}\mu_{n-1}, \\ \mu_1\theta &= a_{10}\mu_0 + a_{11}\mu_1 + \ldots + a_{1,n-1}\mu_{n-1}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \mu_{n-1}\theta &= a_{n-1,0}\mu_0 + a_{n-1,1}\mu_1 + \ldots + a_{n-1,n-1}\mu_{n-1}. \end{aligned}\right\} \quad (1.7)$$

Число θ является корнем уравнения

$$\begin{vmatrix} a_{00}-\theta, a_{01}, & \ldots, a_{0,n-1} \\ a_{00}, & a_{11}-\theta, \ldots, a_{1,n-1} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n-1,0}, a_{n-1,1}, & \ldots, a_{n-1,n-1}-\theta \end{vmatrix} = 0. \quad (1.8)$$

Будем сопоставлять с числом θ матрицу

$$\Theta = \begin{Vmatrix} a_{00}, \ldots, a_{0,n-1} \\ \cdots\cdots\cdots \\ a_{n-1,0}, \ldots, a_{n-1,n-1} \end{Vmatrix}.$$

5. Определим понятие суммы и произведения матриц. Под суммой матриц $A = \|a_{ik}\|$ и $B = \|b_{ik}\|$ будем разуметь матрицу

$$A + B = \|a_{ik} + b_{ik}\|, \quad (1.9)$$

под произведением $A \cdot B$

$$A \cdot B = \left\| \sum_j a_{ij} b_{jk} \right\|. \quad (1.10)$$

Тогда имеет место

Теорема 34. Сумме двух чисел поля соответствует сумма их матриц, произведению — произведение их матриц.

Доказательство. Если числу α соответствует матрица $A = \|a_{ik}\|$, то это означает, что $\mu_i\alpha = \sum_j a_{ij}\mu_j$. Точно так же пусть числу β соответствует матрица $B = \|b_{ik}\|$, т. е. $\mu_j\beta = \sum_j b_{ij}\mu_j$. Складывая оба равенства, получаем:

$$\mu_i(\alpha+\beta) = \sum_j (a_{ij} + b_{ij})\mu_j,$$

откуда видно, что числу $\alpha+\beta$ соответствует матрица $A+B$.

Чтобы получить матрицу, соответствующую произведению $\alpha\beta$, умножим первое из наших равенств на β и воспользуемся вторым равенством:

$$\mu_i\alpha\beta = \sum_s a_{is}\mu_s\beta = \sum_s a_{is}\sum_j b_{sj}\mu_j = \sum_j \left(\sum_s a_{is}b_{sj}\right)\mu_j.$$

Из полученного равенства видно, что произведению $\alpha\beta$ соответствует произведение AB матриц.

Единице соответствует единичная матрица

$$E = \begin{Vmatrix} 1\,0\ldots0 \\ 0\,1\ldots0 \\ \cdots \\ 0\,0\ldots1 \end{Vmatrix}.$$

Обратной к α величине $\frac{1}{\alpha}$ соответствует обратная матрица, которую мы будем обозначать символом A^{-1}. Нулю соответствует нулевая матрица

$$\begin{Vmatrix} 0\,0\ldots0 \\ \cdots \\ 0\,0\ldots0 \end{Vmatrix}.$$

Из того, что умножение чисел поля коммутативно, следует, что и умножение соответствующих им матриц коммутативно. Это имеет место, однако, только для матриц, соответствующих числам поля при определенном выборе базиса. Для произвольных матриц, как мы убедимся ниже, это не имеет места. Для них имеет место ассоциативный закон

$$A \cdot (BC) = (AB) \cdot C, \quad (1.11)$$

в справедливости которого нетрудно убедиться при помощи правила (1.10).

6. Как меняются матрицы, соответствующие одним и тем же числам, при перемене базиса? Пусть базис $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ переходит в $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$ посредством подстановки

$$\left.\begin{aligned} \mu_0 &= c_{00}\omega_0 + c_{01}\omega_1 + \ldots + c_{0,n-1}\omega_{n-1} \\ \mu_1 &= c_{10}\omega_0 + c_{11}\omega_1 + \ldots + c_{1,n-1}\omega_{n-1} \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \mu_{n-1} &= c_{n-1,0}\omega_0 + c_{n-1,1}\omega_1 + \ldots + c_{n-1,n-1}\omega_{n-1}. \end{aligned}\right\} \quad (1.12)$$

Обозначая матрицу подстановки (1.12) через C, будем символически записывать связь между нашими базисами так:

$$[\mu_0, \mu_1, \ldots, \mu_{n-1}] = C \cdot [\omega_0, \omega_1, \ldots, \omega_{n-1}]. \quad (1.13)$$

Нетрудно убедиться путем простой подстановки, что преобразование базиса $C[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ при помощи подстановки D равносильно преобразованию базиса $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ при помощи подстановки DC:

$$D\{C[\omega_0, \omega_1, \ldots, \omega_{n-1}]\} = DC[\omega_0, \omega_1, \ldots, \omega_{n-1}], \quad (1.14)$$

так что в дальнейшем фигурных скобок можно не писать.

Из (1.13) в случае обратимости подстановки C (т. е. когда определитель матрицы C не равен нулю) следует, что $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$ переходит в $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ посредством обратной подстановки C^{-1}:

$$[\omega_0, \omega_1, \ldots, \omega_{n-1}] = C^{-1}[\mu_0, \mu_1, \ldots, \mu_{n-1}]. \quad (1.15)$$

Из (1.7) видно, что соответствие числу θ матрицы Θ может быть записано так:

$$[\mu_0\theta, \mu_1\theta, \ldots, \mu_{n-1}\theta] = \Theta[\mu_0, \mu_1, \ldots, \mu_{n-1}]. \quad (1.16)$$

Переходя в обеих частях (1.16) к другому базису при помощи формулы (1.13), получим:

$$C[\omega_0\theta, \omega_1\theta, \ldots, \omega_{n-1}\theta] = \Theta C[\omega_0, \omega_1, \ldots, \omega_{n-1}],$$

или, совершая над обеими частями подстановку C^{-1}:

$$[\omega_0\theta, \omega_1\theta, \ldots, \omega_{n-1}\theta] = C^{-1}\Theta C[\omega_0, \omega_1, \ldots, \omega_{n-1}]. \quad (1.17)$$

Это равенство показывает, что при нашей перемене базиса числу θ соответствует матрица $C^{-1}\Theta C$.

Будем называть *эквивалентными* две матрицы Θ и Θ_1, если существует такая матрица C, что имеет место

$$\Theta_1 = C^{-1}\Theta C. \quad (1.18)$$

Мы убедились, что одному и тому же числу поля, но при разных базисах, всегда соответствуют эквивалентные матрицы.

Обратно, если две матрицы Θ и Θ_1 эквивалентны и Θ соответствуют числу θ при базисе $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$, то матрица $\Theta_1 = C^{-1}\Theta C$ соответствует тому же числу при базисе $C[\mu_0, \mu_1, \ldots, \mu_{n-1}]$.

7. Какой бы базис идеала мы ни взяли в основу, всегда целому числу поля будет соответствовать целочисленная матрица.

Мы видели, что это вытекает из определения идеала. Матрицы же C и C^{-1} не всегда бывают целочисленны. Обе одновременно могут быть целочисленными только в том случае, если они *унимодулярны*, т. е. если их определители равны ± 1. В самом деле, имеет место равенство

$$C \cdot C^{-1} = E. \quad (1.19)$$

Из теоремы об умножении определителей следует, что определитель произведения матриц равен произведению определителей матриц, в силу чего, вводя для определителя матрицы A обозначение $|A|$, мы получим из (1.19):

$$|C| \cdot |C^{-1}| = 1.$$

Если обе матрицы целочисленны, то их определители суть целые числа, что может быть только, если $|C| = \pm 1$, $|C^{-1}| = \pm 1$.

Будем называть две матрицы Θ, Θ_1 *эквивалентными в узком смысле*, если можно найти такую целочисленную унимодулярную матрицу C, чтобы имело место (1.18). Имеет место

Теорема 35. Матрицы Θ и Θ_1 эквивалентны в узком смысле тогда и только тогда, если базисы, при которых они соответствуют примитивному числу θ поля, суть базисы эквивалентных идеалов.

Доказательство. 1. Пусть числу θ соответствуют при базисах $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$ и $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ матрицы Θ и Θ_1. Пусть наши базисы суть базисы эквивалентных идеалов $\mathfrak{a}$ и $\mathfrak{b}$, между которыми имеет место соотношение

$$\beta\mathfrak{a} = \alpha\mathfrak{b}. \quad (1.20)$$

Это означает, что базисы $[\beta\mu_0, \beta\mu_1, \ldots, \beta\mu_{n-1}]$ и $[\alpha\omega_0, \alpha\omega_1, \ldots, \alpha\omega_{n-1}]$ являются базисами одного и того же идеала (1.20). Поэтому эти базисы переходят друг в друга посредством целочисленных подстановок, которые, будучи взаимно обратными, должны быть унимодулярны. Пусть

$$[\beta\mu_0, \beta\mu_1, \ldots, \beta\mu_{n-1}] = C[\alpha\omega_0, \alpha\omega_1, \ldots, \alpha\omega_{n-1}], \quad (1.21)$$
$$|C| = \pm 1.$$

Из определения матриц Θ и Θ_1 следует:

$$[\mu_0\theta, \mu_1\theta, \ldots, \mu_{n-1}\theta] = \Theta[\mu_0, \mu_1, \ldots, \mu_{n-1}]$$
$$[\omega_0\theta, \omega_1\theta, \ldots, \omega_{n-1}\theta] = \Theta_1[\omega_0, \omega_1, \ldots, \omega_{n-1}],$$

откуда

$$[\beta\mu_0\theta, \beta\mu_1\theta, \ldots, \beta\mu_{n-1}\theta] = \Theta[\beta\mu_0, \beta\mu_1, \ldots, \beta\mu_{n-1}]$$
$$[\alpha\omega_0\theta, \alpha\omega_1\theta, \ldots, \alpha\omega_{n-1}\theta] = \Theta_1[\alpha\omega_0, \alpha\omega_1, \ldots, \alpha\omega_{n-1}].$$

Пользуясь соотношением (1.21), будем иметь:

$$C^{-1}\Theta C[\alpha\omega_0, \alpha\omega_1, \ldots, \alpha\omega_{n-1}] = [\alpha\omega_0\theta, \alpha\omega_1\theta, \ldots, \alpha\omega_{n-1}\theta] = \\ = \Theta[\alpha\omega_0, \alpha\omega_1, \ldots, \alpha\omega_{n-1}],$$

откуда следует

$$\Theta_1 = C^{-1}\Theta C. \qquad (1.22)$$

2. Теперь предположим, что матрицы Θ и Θ_1, соответствующие числу θ при базисах идеалов $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$ и $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$, связаны соотношением (1.22) при $|C| = \pm 1$. Тогда при базисах $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ и $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$ числу θ соответствует одна и та же матрица Θ. Тогда элементы обоих базисов, стоящие на одинаковых местах, дают при делении одно и то же число. В самом деле, пусть $\Theta = \|a_{ik}\|$. По определению имеем:

$$\left.\begin{array}{r} (a_{00}-\theta)\mu_0 + a_{01}\mu_1 + \ldots + a_{0,n-1}\mu_{n-1} = 0 \\ a_{10}\mu_0 + (a_{11}-\theta)\mu_1 + \ldots + a_{1,n-1}\mu_{n-1} = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n-1,0}\mu_0 + a_{n-1,1}\mu_1 + \ldots + (a_{n-1,n-1}-\theta)\mu_{n-1} = 0. \end{array}\right\} \qquad (1.23)$$

Станем рассматривать эти равенства как систему однородных линейных уравнений для определения $\mu_0, \mu_1, \ldots, \mu_{n-1}$. Ранг этой системы равен $n-1$, так как в противном случае θ удовлетворяла бы уравнению степени ниже n, что противоречит ее примитивности. Поэтому любые два решения системы (1.23) отличаются лишь общим множителем. Таковыми решениями являются $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$ и $C[\omega_0, \omega_1, \ldots, \omega_{n-1}]$, которые, отличаясь лишь множителем, суть базисы эквивалентных идеалов. Но так как $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ и $C[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ являются базисами одного и того же идеала, то $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$ и $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ суть базисы эквивалентных идеалов, ч. и т. д.

8. Если мы в роли числа θ будем брать систему $\omega_0, \omega_1, \ldots, \omega_{n-1}$ чисел, образующих фундаментальный базис поля, то соответствующие им матрицы $\Omega_0, \Omega_1, \ldots, \Omega_{n-1}$ будут целочисленны тогда и только тогда, если в качестве базиса $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$ мы возьмем базис какого-нибудь идеала поля. В самом деле, мы уже видели, что если этот базис есть базис идеала, то матрицы $\Omega_0, \Omega_1, \ldots, \Omega_{n-1}$ целочисленны. Обратно, если эти матрицы целочисленны, то совокупность чисел

$$\mu_0 x_0 + \mu_1 x_1 + \ldots + \mu_{n-1}x_{n-1},$$

где $x_0, x_1, \ldots, x_{n-1}$ пробегают все целые рациональные значения, составляет идеал поля k. В самом деле, совершенно очевидно, что сумма и разность чисел такой совокупности тоже принадлежат к этой совокупности. Чтобы доказать, что произведение числа совокупности на любое целое число поля принадлежит к совокупности, достаточно доказать это для каждого из чисел $\omega_0, \omega_1, \ldots, \omega_{n-1}$, составляющих фундаментальный базис поля k. Но это вытекает из

$$[\mu_0\omega_i, \mu_1\omega_i, \ldots, \mu_{n-1}\omega_i] = \Omega_i[\mu_0, \mu_1, \ldots, \mu_{n-1}]$$

и из того, что матрицы Ω_i целочисленны.

Рассмотрим всевозможные преобразования C, переводящие совокупность матриц $\Omega_0, \Omega_1, \ldots, \Omega_{n-1}$ в целочисленные матрицы

$$C^{-1}\Omega_0 C, \quad C^{-1}\Omega_1 C, \ldots, C^{-1}\Omega_{n-1}C. \qquad (1.24)$$

Если совокупность (1.24) может быть получена из $\Omega_0, \Omega_1, \ldots, \Omega_{n-1}$ путем унимодулярного преобразования C, будем говорить, что совокупности *лежат в одном классе*. Так как каждой целочисленной системе типа (1.24) соответствует базис какого-нибудь идеала поля, и две системы типа (1.24) лежат в одном классе тогда и только тогда, если соответствующие их базисам идеалы эквивалентны, то число классов матриц (1.24) равно числу идеальных классов поля, и мы приходим к теореме:

Теорема 36. Число различных систем целочисленных матриц, соответствующих числам фундаментального базиса, равно числу идеальных классов поля, если мы системы, эквивалентные в узком смысле, не будем считать различными.

9. Если мы вместо системы матриц, соответствующих фундаментальному базису поля, рассмотрим систему матриц, соответствующих какому-нибудь базису другого типа, то все сказанное останется справедливым, если мы соответственным образом изменим понятия идеала и идеального класса. Идеалом мы в этом случае должны называть совокупность чисел, воспроизводящихся при сложении, а также при умножении не на все целые числа поля, а только на те, которые выражаются через заданный базис (последние числа воспроизводятся при трех первых арифметических действиях; такого рода совокупности называются *кольцами*). Для выяснения понятия идеального класса обратим внимание на то, что два идеала $\mathfrak{a}$ и $\mathfrak{b}$ могут считаться эквивалентными в том и только в том случае, если можно подобрать такие числа α и β, чтобы $\beta\mathfrak{a}$ и $\alpha\mathfrak{b}$ были одинаковыми *идеалами нашего кольца*. А для этого необходимо, чтобы α и β входили в это кольцо.

10. Пример. Возьмем рассмотренное в § 3.2 поле $K(\sqrt{-5})$. Его фундаментальный базис есть $[1, \sqrt{-5}]$. Базис $[3, 2+\sqrt{-5}]$ есть базис идеала, что можно проверить, умножая его элементы на 1 и $\sqrt{-5}$:

$$3\sqrt{-5} = -2\cdot 3 + 3(2+\sqrt{-5}),$$
$$(2+\sqrt{-5})\cdot\sqrt{-5} = -5+2\sqrt{-5} = -3\cdot 3 + 2(2+\sqrt{-5}).$$

Беря $\theta = \sqrt{-5}$, найдем матрицы Θ и Θ_1, соответствующие θ при базисах $[\omega_0, \omega_1] = [1, \sqrt{-5}]$ и $[\mu_0, \mu_1] = [3, 2+\sqrt{-5}]$:

$$\omega_0\theta = \omega_1,$$
$$\omega_1\theta = -5\omega_0,$$

откуда

$$\Theta = \begin{Vmatrix} 0, & 1 \\ -5, & 0 \end{Vmatrix},$$

$$\mu_0\theta = -2\cdot\mu_0 + 3\mu_1$$
$$\mu_1\theta = -3\cdot\mu_0 + 2\mu_1,$$

откуда

$$\Theta_1 = \begin{Vmatrix} -2, & 3 \\ -3, & 2 \end{Vmatrix}.$$

Покажем, что матрицы Θ и Θ_1 не эквивалентны в узком смысле т. е. что нельзя найти унимодулярной целочисленной матрицы

$$C = \begin{Vmatrix} x, & y \\ z, & u \end{Vmatrix},$$

дающей $\Theta_1 = C^{-1}\Theta C$. Последнее равенство перепишем так: $C\Theta_1 = \Theta C$, или

$$\begin{Vmatrix} x, & y \\ z, & u \end{Vmatrix}\cdot\begin{Vmatrix} -2, & 3 \\ -3, & 2 \end{Vmatrix} = \begin{Vmatrix} 0, & 1 \\ -5, & 0 \end{Vmatrix}\cdot\begin{Vmatrix} x, & y \\ z, & u \end{Vmatrix},$$

откуда

$$-2x-3y=z,\ 3x+2y=u,\ -2z-3u=-5x,\ 3z+2u=-5y.$$

Два последних уравнения являются следствиями двух первых, в силу чего матрица C общего вида такова:

$$\begin{Vmatrix} x, & y \\ -2x-3y, & 3x+2y \end{Vmatrix}.$$

Условие ее унимодулярности:

$$3x^2+4xy+3y^2 = \pm 1$$

не может быть удовлетворено никакими целыми рациональными значениями x, y, так как это условие можно переписать так:

$$(3x+2y)^2+5y^2 = \pm ?.$$

Отсюда следует, что матрицы Θ и Θ_1 эквивалентны, но не эквивалентны в узком смысле, а потому идеал $[3, 2+\sqrt{-5}]$ не эквивалентен $[1, \sqrt{-5}]$, т. е. не является главным идеалом.

§ 2. Единицы алгебраических полей

1. Задавая главный идеал, мы определяем число, на которое делятся все входящие в этот идеал числа, с точностью до единицы поля. Поэтому имеет большое значение умение определять форму всех единиц. Это было проделано в общих чертах Леженом-Дирихле (G. Lejeune-Dirichlet), который доказал существование конечного числа основных единиц, т. е. таких единиц, что все единицы поля выражаются в виде их степеней. Доказательство Дирихле основано на рассмотрении логарифмов от единиц. Недавно Ван-дер-Варден (B. L. van der Waerden) нашел доказательство, свободное от применения логарифмов, которое мы и воспроизведем.

2. Предварительно докажем следующую теорему Кронекера, дополненную Оре (O. Ore):

Теорема 37. Для каждого поля существует такая константа $\delta > 0$, что всякое число поля α, удовлетворяющее вместе со всеми своими сопряженными $\alpha', \alpha'', \ldots, \alpha^{n-1}$ неравенствам

$$|\alpha^{(i)}| < 1+\delta, \qquad (i = 0, 1, 2, \ldots, n-1), \tag{2.1}$$

есть корень из единицы.

Доказательство. Существует лишь конечное число целых величин поля, абсолютно меньших вместе со своими сопряженными заданной величины. В самом деле, элементарно-симметрические функции от величин, сопряженные с такого рода числами, тоже не превосходят по абсолютному значению определенных границ. Так как они являются целыми числами, то существует лишь конечное число возможных чисел, удовлетворяющих этому условию. Поэтому существует лишь конечное число уравнений n-ой степени, корнями которых являются числа такого рода. Среди этих уравнений только часть имеет корни в нашем поле.

Пусть в нашем поле содержится R чисел α, удовлетворяющих условиям

$$|\alpha^{(i)}| < 2 \qquad (i = 0, 1, \ldots, n-1). \tag{2.2}$$

Выберем $\delta > 0$ так, чтобы имело место

$$(1+\delta)^R < 2, \tag{2.3}$$

и рассмотрим степени $1, \alpha, \alpha^2, \ldots, \alpha^R$, где α удовлетворяет условиям (2.1). В силу (2.3) все эти степени, числом $R+1$, удо-

влетворяют условиям (2.2). Но так как различных чисел, подчиненных условиям (2.2), всего R, то среди наших степеней должны попадаться одинаковые числа. Пусть $\alpha^s = \alpha^t$. Тогда $\alpha^{s-t} = 1$, т. е. α есть корень из единицы, ч. и т. д.

3. Теперь докажем следующую фундаментальную теорему Дирихле:

Теорема 38. Если среди полей $k, k', \ldots, k^{(n-1)}$, сопряженных с полем k, имеется r вещественных и s пар сопряженно-комплексных (так что $r+2s=n$), то, полагая $\nu = r+s$, можно найти в k $\nu-1$ единиц, называемых *основными*: $\eta_1, \eta_2, \ldots, \eta_{\nu-1}$, такого рода, что любую единицу поля k можно представить в виде

$$\varepsilon \cdot \eta_1^{m_1} \cdot \eta_2^{m_2} \ldots \cdot \eta_{\nu-1}^{m_{\nu-1}},$$

где ε корень из единицы и $m_1, m_2, \ldots, m_{\nu-1}$ — положительные или отрицательные целые показатели.

Доказательство. Рассмотрим систему линейных форм

$$y_i = \omega_0^{(i)} x_0 + \omega_1^{(i)} x_1 + \ldots + \omega_{n-1}^{(i)} x_{n-1} \quad (i=0, 1, \ldots, n-1), \tag{2.4}$$

где $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ — фундаментальный базис поля k. Ее определитель равен $\sqrt{|D|}$, где D — дискриминант поля k. Можно модифицировать теорему 23 так: каковы бы ни были положительные числа $c_0, c_1, \ldots, c_{n-1}$, связанные соотношением

$$c_0 \, c_1 \ldots c_{n-1} = \sqrt{|D|}, \tag{2.5}$$

можно придать $x_0, x_1, \ldots, x_{n-1}$ такие целые рациональные значения, не обращающиеся сразу в нуль, чтобы удовлетворялись неравенства

$$|y_i| \leqq c_i \qquad (i=0, 1, \ldots, n-1). \tag{2.6}$$

Для этого достаточно применить теорему 23 к системе форм

$$\frac{\sqrt[2n]{|D|}}{c_i} \cdot y_i \qquad (i=0, 1, \ldots, n-1), \tag{2.7}$$

определитель которой тоже равен $\sqrt{|D|}$. Получаемое значение формы y_0 есть целое число поля k, норма которого удовлетворяет неравенству

$$|N(y_0)| < \sqrt{|D|}. \tag{2.8}$$

Каждое y_0, подчиненное условиям (2.6) при различных системах c_i, в силу (2.8) делится на один из конечного числа идеалов. С другой стороны, выбирая различные системы чисел

$c_0, c_1, \ldots, c_{n-1}$ (безгранично уменьшая одно или несколько из них), мы будем получать бесчисленное множество чисел y_0 (будем только иметь в виду, что для сопряженно-комплексных форм y_i необходимо выбирать одинаковые значения c_i; таким образом для случая мнимого квадратичного поля эти рассуждения неприменимы). Из получаемых значений y_0 каждое ассоциировано с одним из конечного числа представителей. Частные получаемых ассоциированных чисел суть единицы поля, притом отличные от рациональной единицы. Выбором констант $c_0, c_1, \ldots, c_{n-1}$ мы можем получать единицы, которые по абсолютной величине сколь угодно велики, в то время как сопряженные с ними числа сколь угодно малы. Для этого нужно выбрать систему чисел

$$\alpha_1, \alpha_2, \ldots, \alpha_m, \tag{2.9}$$

нормы которых не превышают $\sqrt{|D|}$, и в качестве $c_1, c_2, \ldots, c_{n-1}$ взять числа, абсолютно меньшие всех чисел, сопряженных с числами (2.9). Разделяя полученное число типа (2.6) на то из чисел (2.9), которое с ним ассоциировано, получим единицу η, все сопряженные с которой величины абсолютно <1 и которая в силу $|N(\eta)|=1$ абсолютно >1 (если k — комплексное поле, то на сопряженно-комплексную величину, скажем η', мы не можем накладывать требования $|\eta'|<1$, так как $|\eta|=|\eta'|$. Тогда мы должны положить $c_1 = c_0$, а наши условия наложить только на константы $c_2, c_3, \ldots, c_{n-1}$).

Выделим ν сопряженных полей $k, k', k'', \ldots, k^{(\nu-1)}$, среди которых не было бы ни одной пары сопряженно-комплексных (т. е. выделяя из каждой пары сопряженно-комплексных полей по одному полю), и, пользуясь изложенным приемом, найдем такую систему единиц $\eta, \eta_1, \ldots, \eta_{\nu-2}$, чтобы имели место следующие неравенства:

$$\left.\begin{array}{l} |\eta|>1,\ |\eta'|<1,\ |\eta''|<1,\ \ldots,\ |\eta^{(\nu-2)}|<1,\ |\eta^{(\nu-1)}|<1 \\ |\eta_1|<1,\ |\eta_1'|>1,\ |\eta_1''|<1,\ \ldots,\ |\eta_1^{(\nu-2)}|<1,\ |\eta_1^{(\nu-1)}|<1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ |\eta_{\nu-2}|<1,\ |\eta'_{\nu-2}|<1,\ |\eta''_{\nu-2}|<1,\ \ldots,\ |\eta_{\nu-2}^{(\nu-2)}|>1,\ |\eta_{\nu-2}^{(\nu-1)}|<1. \end{array}\right\} \tag{2.10}$$

Докажем, что единицы $\eta, \eta_1, \ldots, \eta_{\nu-2}$ независимы, т. е. что между ними не может быть соотношения

$$\eta^{\rho_0} \cdot \eta_1^{\rho_1} \ldots \eta_{\nu-2}^{\rho_{\nu-2}} = 1 \tag{2.11}$$

с целыми рациональными $\rho_0, \rho_1, \ldots, \rho_{\nu-2}$. Вводя для отрицательных ρ_i обозначения $-\sigma_i$ и в случае нужды перенумеровывая поля и единицы, перепишем (2.11) так:

$$\eta^{\rho_0} \cdot \eta_1^{\rho_1} \ldots \eta_{\mu-1}^{\rho_{\mu-1}} = \eta_{\mu}^{\sigma_{\mu}} \cdot \eta_{\mu+1}^{\sigma_{\mu+1}} \ldots \eta_{\nu-2}^{\sigma_{\nu-2}}, \tag{2.12}$$

где $\rho_i \geqslant 0$, $\sigma_i \geqslant 0$. Аналогичные равенства получатся при переходе к сопряженным полям. Составим их для полей k', k'', ..., $k^{(\mu-1)}$, а также для сопряженно-комплексных с последними полями. Тогда, условившись обозначать через $\widetilde{\alpha^{(i)}}$ величину $\alpha^{(i)}$, если поле $k^{(i)}$ вещественно, и величину $\alpha^{(i)} \cdot \overline{\alpha^{(i)}} = |\alpha^{(i)}|^2$, если поле $k^{(i)}$ мнимое, перемножим полученные равенства:

$$\left[\prod_{i=0}^{\mu-1} \widetilde{\eta^{(i)}}\right]^{\rho_0} \cdot \left[\prod_{i=1}^{\mu-1} \widetilde{\eta_1^{(i)}}\right]^{\rho_1} \cdots \left[\prod_{i=0}^{\mu-1} \widetilde{\eta_{\mu-2}^{(i)}}\right]^{\sigma_{\mu-1}} = \left[\prod_{i=0}^{\mu-1} \widetilde{\eta_{\mu}^{(i)}}\right]^{\sigma_{\mu}} \cdots \left[\prod_{i=0}^{\mu-1} \widetilde{\eta_{\nu-1}^{(i)}}\right]^{\sigma_{\nu-1}}. \tag{2.13}$$

Здесь в правой части каждый множитель в квадратных скобках в силу (2.10) абсолютно меньше единицы. В левой же части каждый такой множитель абсолютно больше единицы, в чем можно убедиться, переписав равенство $N(\eta_s) = \pm 1$ так:

$$\prod_{i=0}^{\mu-1} \widetilde{\eta_s^{(i)}} \cdot \prod_{i=\mu}^{\nu-2} \widetilde{\eta_s^{(i)}} = \pm 1 \qquad (s = 0, 1, \ldots, \mu-1);$$

здесь второе произведение в силу (2.10) абсолютно меньше единицы. Итак (2.13), а с ним (2.12), возможно только в тривиальном случае $\rho_i = \sigma_i = 0$.

Докажем, что всякую единицу ε поля k можно привести путем умножения на степени единиц η, η_1, ..., $\eta_{\nu-2}$ к одной из некоторого конечного числа единиц. Предварительно докажем следующее:

Всякая единица ε, для которой имеет место

$$|\varepsilon^{(i)}| \leqq 1 \qquad (i = 0, 1, \ldots, \nu-2), \tag{2.14}$$

может быть приведена умножением на степени единиц η_i к единице H, для которой имеет место

$$1 < |H^{(i)}| \leqq a_i, \; a_i = |\eta_i^{(i)}| \qquad (i = 0, 1, \ldots, \nu-2). \tag{2.15}$$

В самом деле, рассмотрим всевозможные единицы типа

$$H = \varepsilon \cdot \eta^{k_0} \eta_1^{k_1} \ldots \eta_{\nu-2}^{k_{\nu-2}},$$

где $k_i \geqq 0$. Выберем из них те, для которых имеет место $|H^{(i)}| \leqq a_i$. Они существуют, в чем мы убедимся, полагая $k_i = 0$, так как $a_i > 1$. С другой стороны, их число конечно, так как в силу $|\eta_i^{(\nu-1)}| < 1$ мы имеем $|H^{(\nu-1)}| < |\varepsilon^{(\nu-1)}|$, и при фиксированном ε все сопряженные абсолютные значения единиц H ограничены:

$$|H^{(i)}| \leqq a_i \quad (i = 0, 1, \ldots, \nu-2); \quad |H^{(\nu-1)}| < |\varepsilon^{(\nu-1)}|. \tag{2.16}$$

Выберем среди всех этих H ту, для которой $|H^{(\nu-1)}|$ имеет наименьшее значение. Тогда непременно имеет место $|H^{(i)}| > 1$ $(i = 0, 1, \ldots, \nu-2)$, так как в противном случае, если бы например имело место $|H| \leqq 1$, то, беря в роли H единицу $H\eta$, мы бы опять удовлетворили всем требованиям (2.16), в то время как значение $|H^{(\nu-1)}\eta^{(\nu-1)}|$ в силу $|\eta^{(\nu-1)}| < 1$ было бы меньше, чем $H^{(\nu-1)}|$. Итак, единица H удовлетворяет всем условиям (2.15).

Беря в роли ε единицу 1, мы получим единицу

$$H_0 = \eta^{k_0} \eta_1^{k_1} \ldots \eta_{\nu-2}^{k_{\nu-2}},$$

удовлетворяющую условиям (2.15) и для которой $|H_0^{(\nu-1)}| < 1$. Умножая произвольную единицу ε на достаточно высокую отрицательную степень H_0, мы получим единицу εH_0^{-k}, для которой будут выполнены условия (2.14), в силу чего к ней можно применить наш результат. Получим единицу

$$H = \varepsilon H_0^{-k} \cdot \eta^{\tau_0} \cdot \eta_1^{\tau_1} \ldots \eta_{\nu-2}^{\tau_{\nu-2}} = \varepsilon \eta^{\tau_0 - k k_0} \cdot \eta_1^{\tau_1 - k k_1} \ldots \eta_{\nu-2}^{\tau_{\nu-2} - k k_{\nu-2}},$$

удовлетворяющую условиям (2.15), из которых в силу $N(H) = \pm 1$ вытекает $|H^{(\nu-1)}| < 1$. В силу ограниченности сопряженных значений таких единиц — конечное число. Пусть это будут $H_1, H_2, \ldots, H_s$. Тогда любая единица ε поля k может быть представлена в виде

$$\varepsilon = H_k \cdot \eta^{\rho_0} \cdot \eta_1^{\rho_1} \ldots \eta_{\nu-2}^{\rho_{\nu-2}} \qquad (k = 1, 2, \ldots, s), \tag{2.17}$$

где $\rho_0, \rho_1, \ldots, \rho_{\nu-2}$ — целые рациональные числа.

Все единицы поля образуют бесконечную абелеву группу относительно умножения. Единицы же вида $\eta^{\rho_0}, \eta_1^{\rho_1}, \ldots, \eta_{\nu-2}^{\rho_{\nu-2}}$ образуют подгруппу *конечного индекса* s. В теории бесконечных групп индекс определяется как число сопряженных систем в разложении группы по подгруппе. Представление (2.17) как раз показывает, что всякая единица поля входит в одну из s сопряженных систем (если, конечно, мы подобрали $H_1, H_2, \ldots, H_s$ так, что между ними нет соотношений типа $H_j = H_i \eta^{\sigma_0} \eta_1^{\sigma_1} \ldots \eta_{\nu-2}^{\sigma_{\nu-2}}$; в противном случае число сопряженных систем уменьшится). Ниже мы увидим, что в каждой бесконечной абелевой группе, образованной степенями конечного числа некоторых элементов (называемых *образующими элементами*), можно найти конечное число независимых элементов, частью конечного, частью бесконечного порядка, через степени которых выражаются все элементы группы. Число независимых элементов бесконечного порядка называется *рангом* группы.

Докажем, что ранг рассматриваемой нами группы точно равен

$\nu-1$. В виду доказанного нами существования $\nu-1$ независимых элементов он не может быть меньше $\nu-1$. С другой стороны, если бы ранг группы был больше $\nu-1$, то группа содержала бы, кроме η, η_1, ..., $\eta_{\nu-1}$, еще независимую от этих единиц единицу, например ε, и тогда бы ни одна из бесконечного числа единиц

$$\varepsilon\eta^{k_0}\eta_1^{k_1}\dots\eta_{\nu-2}^{k_{\nu-2}},\quad \varepsilon^2\eta^{k_0}\eta_1^{k_1}\dots\eta_{\nu-2}^{k_{\nu-2}},\quad \varepsilon^3\eta^{k_0}\eta_1^{k_1}\dots\eta_{\nu-2}^{k_{\nu-2}}\dots$$

не совпадала ни с одной другой; иными словами, наша группа распадалась бы на бесконечное число сопряженных комплексов по подгруппе $[\eta, \eta_1, \dots, \eta_{\nu-2}]$, что противоречило бы добытому нами результату. Таким образом, опираясь на недоказанную еще теорему об абелевых группах (теорема 39), мы доказали, что каждая единица поля k может быть представлена в виде произведения степеней некоторых $\nu-1$ единиц, не связанных между собой никакими зависимостями, и некоторого числа единиц, являющихся в группе элементами конечных порядков, т. е. корней из единицы. Это составляет содержание теоремы 38.

4. Теорема 39. Если бесконечная абелева группа воспроизводится композицией некоторого конечного числа элементов $A_1, A_2, \dots, A_m$, связанных несколькими зависимостями:

$$\left.\begin{aligned} A_1^{a_1}A_2^{a_2}\dots A_m^{a_m}&=1\\ A_1^{b_1}A_2^{b_2}\dots A_m^{b_m}&=1\\ \dots\dots\dots&\\ A_1^{f_1}A_2^{f_2}\dots A_m^{f_m}&=1, \end{aligned}\right\} \tag{2.18}$$

то в ней можно найти конечное число независимых элементов, конечного или бесконечного порядка, через которые выразятся все элементы группы.

Доказательство. Будем постепенно освобождаться от соотношений (2.18). Если в первом из них показатели $a_1, a_2, \dots, a_m$ имеют общий наибольший делитель d:

$$a_1=a_1'd,\quad a_2=a_2'd,\quad \dots,\quad a_m=a_m'd,$$

то элемент $C=A_1^{a_1'}A_2^{a_2'}\dots A_m^{a_m'}$ является элементом конечного порядка: $C^d=1$. В соотношении

$$A_1^{a_1'}A_2^{a_2'}\dots A_m^{a_m'}=C \tag{2.19}$$

выберем наименьший (или один из наименьших) показатель. Пусть это будет a_1'. Разделим остальные показатели на a_1' с остатком:

$$a_2'=a_1'q_2+r_2,\quad \dots,\quad a_m'=a_1'\cdot q_m+r_m$$

и введем на место A_1 элемент $\overline{A_1}=A_1\cdot A_2^{q_2}\dots A_m^{q_m}$ (система элементов $\overline{A_1}, A_2, \dots, A_m$ тоже является производящей группу, так как A_1, очевидно, выражается через $\overline{A_1}, A_2, \dots, A_m$). Соотношение (2.19) перепишется так:

$$\overline{A_1}^{a_1'}A_2^{r_2}\dots A_m^{r_m}=C.$$

Опять среди показателей выбираем наименьший и совершаем аналогичное преобразование. В конце концов в силу взаимной простоты показателей $a_1', a_2', \dots, a_n'$ мы, перейдя к производящей группу системе $B_1, B_2, \dots, B_m$, приведем соотношение (2.19) к виду

$$B_m=C;$$

выражая через $B_1, B_2, \dots, B_{m-1}, C$ элементы $A_1, A_2, \dots, A_m$ и подставляя в остальные соотношения (2.18), мы применим тот же процесс к какому-нибудь из них. Таким путем мы уничтожим все соотношения, кроме таких, которые связывают элементы конечных порядков. Последние образуют конечную абелеву группу.

Примечание. **Пользуясь доказанной в части I теоремой для конечных абелевых групп (часть I, стр. 42, теорема 30), мы сможем формулировать теорему 39 так:**

Всякая абелева группа с конечным числом производящих элементов разлагается в прямое произведение циклических групп конечных и бесконечных порядков.

Под циклической группой бесконечного порядка мы разумеем группу, образуемую всеми положительными и отрицательными степенями элемента бесконечного порядка.

5. Пример. Пусть производящие элементы абелевой группы будут A_1, A_2, A_3, и пусть между ними имеют место соотношения

$$A_1^4A_2^6A_3^8=1,\quad A_1^9A_2^{15}A_3^{12}=1. \tag{2.20}$$

Первое из этих соотношений мы перепишем так:

$$A_1^2A_2^3A_3^4=D,\quad D^2=1,$$

или так:

$$(A_1A_2A_3^2)^2A_2=D.$$

Делая замену $A_1A_2A_3^2=B_1$, откуда $A_1=B_1A_2^{-1}A_3^{-2}$, получим:

$$B_1^2A_2=D.$$

Выразим A_2, A_1, A_3 через B_1, D, A_3:

$$A_2=DB_1^{-2},\quad A_1=B_1^3D^{-1}A_3^{-2}$$

и подставим во второе соотношение (2.20), которое можно представить так:

$$A_1^3A_2^5A_3^4=C,\quad C^3=1,$$

$$B_1^9D^{-1}A_3^{-6}D^5B_1^{-10}A_3^4=C,$$

т. е.

$$B_1^{-1}D^4A_3^{-2}=C,$$

откуда

$$B_1=D^4A_3^{-2}C.$$

Подставим в выражения для A_2 и A_1:

$$A_2=A_3^4D^{-7}C^{-2},\quad A_1=A_3^{-8}D^{11}C^3,$$

или, принимая во внимание $D^2=1$, $C^3=1$:

$$A_2=A_3^4DC,\quad A_1=A^{-8}D.$$

Между A_3, D и C соотношений нет. Группа разложена в прямое произведение циклических групп бесконечного, второго и третьего порядков.

6. Пользуясь единицами, можно установить такой способ нормирования чисел поля, чтобы из всех ассоциированных между собой чисел нормированными оказывались ровно w, где w есть число корней из единицы, содержащихся в поле. Для этого с каждым числом α будем сопоставлять логарифмы абсолютных значений сопряженных с α чисел:

$$\left.\begin{aligned}\lambda=\delta\lg|\alpha|,\ \lambda'=\delta'\cdot\lg|\alpha'|,\ \lambda''=\delta''\lg|\alpha''|,\ldots,\lambda^{(\nu-1)}=\\ =\delta^{(\nu-1)}\cdot\lg|\alpha^{(\nu-1)}|,\end{aligned}\right\}\quad(2.21)$$

где k, $k',\ldots,k^{(\nu-1)}$ попрежнему обозначают сопряженные с k поля, среди которых нет ни одной пары сопряженно-комплексных, а $\delta^{(i)}$ равно 1, если поле $k^{(i)}$ вещественное и $\delta^{(i)}=2$, если $k^{(i)}$ комплексное. Отсюда следует:

$$\lambda+\lambda'+\ldots+\lambda^{(\nu-1)}=\lg|N(\alpha)|.\quad(2.22)$$

Для системы $\varepsilon,\varepsilon',\ldots,\varepsilon^{(\nu-1)}$ основных единиц поля введем специальное обозначение:

$$l_i,\ l_i',\ l_i'',\ldots,l_i^{(\nu-1)}\qquad(i=0,\ 1,\ 2,\ldots,\nu-2).\quad(2.23)$$

Определим для логарифмов числа α систему *показателей* $\xi,\ \xi_1,\ldots,\xi_{\nu-1}$, определяя их как решение системы линейных уравнений

$$\left.\begin{aligned}\lambda&=\xi l+\xi_1l_1+\ldots+\xi_{\nu-2}l_{\nu-2}+\xi_{\nu-1}\delta\\ \lambda'&=\xi l'+\xi_1l_1'+\ldots+\xi_{\nu-2}l_{\nu-2}+\xi_{\nu-1}\delta'\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ \lambda^{(\nu-1)}&=\xi l^{(\nu-1)}+\xi_1l_1^{(\nu-1)}+\ldots+\xi_{\nu-2}l_{\nu-2}^{(\nu-1)}+\xi_{\nu-1}\delta^{(\nu-1)}.\end{aligned}\right\}\quad(2.24)$$

Определитель этой системы не равен нулю. В самом деле, в противном случае существовали бы отличные от нуля значения $\xi,\ \xi_1,\ldots,\xi_{\nu-1}$, дающие $\lambda=\lambda'=\ldots=\lambda^{(\nu-1)}=0$.

Тогда, переходя от логарифмов к числам, мы получим:

$$\left|\varepsilon^{(i)}\right|^{\xi}\cdot\left|\varepsilon_1^{(i)}\right|^{\xi_1}\ldots\left|\varepsilon_{\nu-2}^{(i)}\right|^{\xi_{\nu-2}}=1\quad(i=0,\ 1,\ 2,\ldots,\nu-1).\quad(2.25)$$

Подобное соотношение невозможно для системы $\eta,\ \eta^{(1)},\ldots,\eta^{(\nu-2)}$, в чем мы убедимся, рассуждая, как в § 2.3, если принять во внимание, что для этих рассуждений не играет никакой роли то, что в (2.11) числа $\rho_0,\rho_1,\ldots,\rho_{\nu-2}$ предположены целыми. Число же $\xi_{\nu-1}$ равно нулю, в чем мы убедимся, складывая уравнения (2.24) и пользуясь тем, что

$$l_i+l_i'+\ldots+l_i^{(\nu-1)}=\lg|N(\varepsilon_i)|=\lg 1=0\,(i=0,\ 1,\ldots,\nu-2)\quad(2.26)$$

Но единицы $\eta,\ \eta_1,\ldots,\eta_{\nu-2}$ могут быть выражены через основные:

$$\eta_i=\zeta\varepsilon^{a_{0i}}\cdot\varepsilon_1^{a_{1i}}\ldots\zeta_{\nu-1}^{a_{\nu-1,i}}\ (i=0,\ 1,\ldots,\nu-2),\ \zeta^m=1,\quad(2.27)$$

откуда, обозначая $\lambda_i^{(j)}=\delta^{(j)}\cdot\lg|\eta_i^{(j)}|$ получим:

$$\lambda_i^{(j)}=a_{0i}l^{(j)}+a_{1i}l_1^{(j)}+\ldots+a_{\nu-2,i}\,l_{\nu-2}^{(j)}\begin{pmatrix}i=0,1,\ldots,\nu-2;\\ j=0,1,\ldots,\nu-1\end{pmatrix},\quad(2.28)$$

откуда

$$\left.\begin{aligned}\begin{vmatrix}\lambda, & \lambda_1,\ldots, & \lambda_{\nu-2}\\ \lambda', & \lambda_1',\ldots, & \lambda'_{\nu-2}\\ \ldots\ldots & \ldots\ldots & \ldots\ldots\\ \lambda^{(\nu-2)}, & \lambda_1^{(\nu-2)},\ldots, & \lambda_{\nu-2}^{(\nu-2)}\end{vmatrix}&=\begin{vmatrix}l, & l_1,\ldots, & l_{\nu-2}\\ l', & l_1',\ldots, & l'_{\nu-2}\\ \ldots\ldots & \ldots\ldots & \ldots\ldots\\ l^{(\nu-2)}, & l_1^{(\nu-2)},\ldots, & l_{\nu-2}^{(\nu-2)}\end{vmatrix}\times\\ \times\begin{vmatrix}a_{00}, & a_{01},\ldots, & a_{0,\nu-2}\\ a_{10}, & a_{11},\ldots, & a_{1,\nu-2}\\ \ldots\ldots & \ldots\ldots & \ldots\ldots\\ a_{\nu-2,0}, & a_{\nu-2,1},\ldots, & a_{\nu-2,\nu-2}\end{vmatrix}.\end{aligned}\right\}\quad(2.29)$$

Но определитель в левой части не равен нулю, а потому ни один из множителей правой части не может равняться нулю. Обозначая первый из них через $L(\varepsilon,\varepsilon_1,\ldots,\varepsilon_{\nu-2})$ и называя *регулятором* системы единиц $\varepsilon,\ \varepsilon_1,\ldots,\varepsilon_{\nu-2}$, мы убедимся, что определитель системы (2.24) равен $n\cdot L(\varepsilon,\varepsilon_1,\ldots,\varepsilon_{\nu-2})$. Для этого

сложим с последней строкой определителя системы (2.24) остальные строки и воспользуемся (2.26) и тем, что

$$\delta+\delta'+\ldots+\delta^{(\nu-1)}=n.$$

Абсолютная величина $L(\varepsilon, \varepsilon_1, \ldots, \varepsilon_{\nu-2})$ не зависит от выбора системы основных единиц. В самом деле, если $\eta, \eta_1, \ldots, \eta_{\nu-2}$ — другая система основных единиц и обе системы связаны соотношением (2.27), то имеет место (2.29), где второй множитель правой части есть целочисленный определитель, в силу чего $L(\eta, \eta_1, \ldots, \eta_{\nu-2})$ делится на $L(\varepsilon, \varepsilon_1, \ldots, \varepsilon_{\nu-2})$. Меняя ролями обе системы единиц, мы убедимся, что

$$|L(\eta, \eta_1, \ldots, \eta_{\nu-2})| = |L(\varepsilon, \varepsilon_1, \ldots, \varepsilon_{\nu-2})|.$$

В силу этого эту абсолютную величину называют *регулятором* поля и обозначают через L.

7. Показатели $\xi, \xi_1, \xi_2, \ldots, \xi_{\nu-1}$ числа α, определяемые системой уравнений (2.24), обладают следующими легко доказуемыми свойствами:

I. Если числам α и $\tilde{\alpha}$ соответствуют показатели соответственно $\xi, \xi_1, \ldots, \xi_{\nu-1}$ и $\tilde{\xi}, \tilde{\xi}_1, \ldots, \tilde{\xi}_{\nu-1}$, то произведению $\alpha\tilde{\alpha}$ соответствуют показатели

$$\xi+\tilde{\xi}, \xi_1+\tilde{\xi}_1, \ldots, \xi_{\nu-1}+\tilde{\xi}_{\nu-1}.$$

II. Показатель $\xi_{\nu-1}=\lg|N(\alpha)|$.

III. Чтобы имело место $\xi=\xi_1=\ldots=\xi_{\nu-1}=0$, необходимо и достаточно, чтобы α было корнем из единицы.

IV. Показатели единицы суть целые рациональные числа.

Последнее следует из того, что для основных единиц ε_i в роли α показатели суть 0, 0, ..., 1, 0...0. Показатель $\xi_{\nu-1}$ для единиц всегда в силу II равен нулю. Из этого также следует, что можно найти такую единицу, чтобы ее показатели $\xi, \xi_1, \ldots, \xi_{\nu-2}$ были равны любым заданным целым рациональным числам.

Возьмем теперь в роли α произвольное целое число поля k. Если его показатели суть $\xi, \xi_1, \ldots, \xi_{\nu-2}, \xi_{\nu-1}=\lg|N(\alpha)|$, то можно, притом однозначно, подобрать такие целые рациональные $q, q_1, \ldots, q_{\nu-1}$, чтобы имело место

$$0 \leqq \xi_i - q_i < 1. \tag{2.30}$$

Тогда показатели числа $\alpha\varepsilon^{-q}\cdot\varepsilon_1^{-q_1}\ldots\varepsilon_{\nu-2}^{q_{\nu-2}}$ будут все (кроме $\xi_{\nu-1}$) лежать между 0 и 1. Это число мы и будем называть

нормированным. Очевидно, что два ассоциированных нормированных числа отличаются множителем, имеющим нулевые показатели, т. е. единичные абсолютные значения сопряженных величин. Такие величины суть корни из единицы, и их, согласно нашему условию, всего w.

8. Для мнимых квадратичных полей $r=0$, $s=1$, а потому число независимых единиц $\nu-1=r+s-1$ равно нулю. Единицами могут быть только корни из единицы. Но в части I мы видели, что первообразные m-ые корни из единицы являются корнями неприводимого уравнения степени $\varphi(m)$. Найдем значения m, для которых $\varphi(m)=2$. Положив

$$m=2^{\alpha}\cdot p_1^{\alpha_1}\cdot p_2^{\alpha_2}\ldots p_k^{\alpha_k},$$

получим

$$2^{\alpha-1}p_1^{\alpha_1-1}(p-1)\,p_2^{\alpha_2-1}(p_2-1)\ldots p_k^{\alpha_k-1}(p_k-1)=2,$$

откуда следует, что при $p_i>3$ $\alpha_i=0$. Единственными решениями этого уравнения являются $\alpha=2$, $\alpha_1=0$; $\alpha=0$, $\alpha_1=1$ и $\alpha=1$, $\alpha_1=1$, т. е. $m=4$, $m=3$ и $m=6$.

Первообразные корни этих степеней удовлетворяют следующим уравнениям:

$$x^2+1=0, \quad x^2+x+1=0, \quad x^2-x+1=0.$$

Корни этих уравнений образуют поля $K(i)$ и $K(\sqrt{-3})$. Остальные мнимые квадратичные поля не имеют единиц, кроме ± 1.

9. Для вещественных квадратичных полей $r=2$, $s=0$, и число независимых единиц равно $\nu-1=r+s-1=1$. Так как поля вещественны, то, кроме ± 1, они не могут содержать корней из единицы. Если поэтому u есть наименьшая из больших единиц единица поля $K(\sqrt{D})$, то все единицы этого поля могут быть представлены в виде $\pm u^n$, где n может быть положительным и отрицательным числом. Записывая единицу поля k в форме $x+y\sqrt{D}$ в случае $D\equiv 2,3 \pmod 4$ и в форме $\frac{x+y\sqrt{D}}{2}$ [$x\equiv y\equiv 1 \pmod 2$] в случае $D\equiv 1 \pmod 4$, мы должны подчинить x и y следующим условиям:

$$x-Dy^2=\pm 1, \quad D\equiv 2,3 \pmod 4 \tag{2.31}$$

$$x^2-Dy^2=\pm 4, \quad D\equiv 1 \pmod 4, \; x\equiv y\equiv 1 \pmod 2. \tag{2.32}$$

Эти уравнения носят название *уравнений Пелля* и решаются с помощью теории непрерывных дробей, которую мы сейчас изложим.

10. ***Непрерывной дробью*** называется выражение вида

$$x = a + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{x_n}}}}, \tag{2.33}$$

где a — целое рациональное неотрицательное число, $a_1, a_2, \ldots, \ldots, a_{n-1}$ — целые рациональные положительные числа и x_n — вещественное число, не меньшее единицы. Всякое вещественное положительное число x можно представить в виде (2.33) с любым значением n, притом однозначно. Для этого нужно выделить в x целую часть a, рассмотреть обратную величину $x_1 = \frac{1}{x-a}$ к разности $x - a$ и выделить в ней целую часть a_1, с x_1 поступить точно так же, и т. д.

Этот процесс дает хорошие приближения к числу x, которые получаются, если в выражении (2.33) отбросить все члены (звенья) после a_{k-1}. Получаемая рациональная дробь называется k-ой ***подходящей дробью*** к x и обозначается через $\frac{P_k}{Q_k}$:

$$\frac{P_k}{Q_k} = a + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_{k-1}}}}. \tag{2.34}$$

Таким образом мы имеем:

$$\frac{P_1}{Q_1} = \frac{a}{1}, \quad \frac{P_2}{Q_2} = \frac{aa_1+1}{a_1}, \quad \frac{P_3}{Q_3} = \frac{aa_1a_2+a+a_2}{a_1a_2+1}, \ldots$$

Подходящие дроби вычисляются последовательно при помощи следующих рекуррентных соотношений:

$$\frac{P_{m+1}}{Q_{m+1}} = \frac{P_m a_m + P_{m-1}}{Q_m a_m + Q_{m-1}}. \tag{2.35}$$

Чтобы доказать их, предположим, что они справедливы для $m-1$ (для низших значений m их нетрудно проверить):

$$\frac{P_m}{Q_m} = \frac{P_{m-1}a_{m-1} + P_{m-2}}{Q_{m-1}a_{m-1} + Q_{m-2}}. \tag{2.36}$$

Но дробь $\frac{P_{m+1}}{Q_{m+1}}$ получится из $\frac{P_m}{Q_m}$, если мы на место a_{m-1} подставим $a_{m-1} + \frac{1}{a_m}$. Замечая, что P_{m-1}, P_{m-2}, Q_{m-1}, Q_{m-2} не содержат a_{m-1}, получаем:

$$\frac{P_{m+1}}{Q_{m+1}} = \frac{P_{m-1}\left(a_{m-1} + \frac{1}{a_m}\right) + P_{m-2}}{Q_{m-1}\left(a_{m-1} + \frac{1}{a_m}\right) + Q_{m-2}} = \frac{(P_{m-1}a_{m-1} + P_{m-2})a_m + P_{m-1}}{(Q_{m-1}a_{m-1} + Q_{m-2})a_m + Q_{m-1}}. \tag{2.37}$$

Полагая, что в равенстве (2.36) равны отдельно числители и знаменатели (мы имеем право это сделать, так как до сих пор мы не определяли отдельно P_m и Q_m):

$$P_m = P_{m-1}a_{m-1} + P_{m-2}, \quad Q_m = Q_{m-1}a_{m-1} + Q_{m-2} \tag{2.38}$$

и подставляя в (2.37), мы придем к формуле (2.35).

Докажем, что, определяя числители и знаменатели подходящих дробей при помощи формул (2.38), мы будем получать несократимые дроби, и одновременно выведем важную формулу

$$P_m Q_{m-1} - P_{m-1} Q_m = (-1)^m, \tag{2.39}$$

предположив ее известной для $m-1$ и пользуясь (2.38):

$$\begin{aligned} P_m Q_{m-1} - P_{m-1} Q_m &= (P_{m-1}a_{m-1} + P_{m-2}) Q_{m-1} - \\ &- P_{m-1}(Q_{m-1}a_{m-1} + Q_{m-2}) = \\ &= -(P_{m-1}Q_{m-2} - P_{m-2}Q_{m-1}). \end{aligned}$$

Отметим еще формулу

$$x = \frac{P_m x_m + P_{m-1}}{Q_m x_m - Q_{m-1}}. \tag{2.40}$$

Из нее мы получим:

$$x - \frac{P_m}{Q_m} = \frac{(-1)^{m-1}}{(Q_m x_m + Q_{m-1}) Q_m}. \tag{2.41}$$

Эта формула показывает, что погрешность, получаемая при замене x подходящей дробью $\frac{P_m}{Q_m}$, абсолютно меньше квадрата знаменателя последней и что знак этой погрешности есть $+$ или $-$, судя по тому, нечетно или четно m.

11. Докажем теорему, обратную последнему утверждению:

Если разность $\left|x - \frac{P}{Q}\right|$ меньше $\frac{1}{2Q^2}$, то дробь $\frac{P}{Q}$ является подходящей дробью разложения x в непрерывную дробь.

Разложим $\frac{P}{Q}$ в непрерывную дробь (конечную в силу рациональности $\frac{P}{Q}$):

$$\frac{P}{Q}=a+\frac{1}{a_1+\frac{1}{a_2+\cdots+\frac{1}{a_{m-1}}}}.$$

Пусть подходящая дробь, непосредственно предшествующая $\frac{P}{Q}$, есть $\frac{P_1}{Q_1}$, так что $PQ_1-P_1Q=(-1)^m$.

Определим x_m при помощи равенства

$$x=\frac{Px_m+P_1}{Qx_m+Q_1}. \tag{2.42}$$

Из

$$\left|x-\frac{P}{Q}\right|<\frac{1}{2Q^2}$$

следует

$$\frac{1}{(Qx_m+Q_1)Q}<\frac{1}{2Q^2},$$

откуда в силу $Q_1<Q$ имеет место $x_m>1$.

Но равенство (2.42 можно переписать так:

$$x=a+\frac{1}{a_1+\frac{1}{a_2+\cdots+\frac{1}{a_{m-1}+\frac{1}{x_m}}}}, \tag{2.43}$$

и в силу $x_m>1$ мы заключаем, что (2.43) есть разложение x в непрерывную дробь, а $\frac{P}{Q}$ — m-ая подходящая, ч. и т. д.

12. Пусть D — целое рациональное число, не имеющее кратных множителей. Докажем, что разложение $\sqrt{D}$ в непрерывную дробь периодично.

Начнем разлагать $\sqrt{D}$. Пусть $a<\sqrt{D}<a+1$.

Тогда $\sqrt{D}=a+\frac{1}{x_1}$, откуда

$$x_1=\frac{1}{\sqrt{D}-a}=\frac{\sqrt{D}+a}{D-a^2}.$$

Отметим следующие свойства x_1:

1) в числителе при $\sqrt{D}$ стоит единица;

2) знаменатель есть делитель нормы числителя.

Станем далее составлять x_2, x_3, ... Предположив свойства 1), 2) справедливыми для x_{m-1}, докажем их для x_m. Пусть

$$x_{m-1}=\frac{\sqrt{D}+b}{c}, \tag{2.44}$$

где c есть делитель $D-b^2$. Тогда

$$\frac{\sqrt{D}+b}{c}=f+\frac{1}{x_m},$$

откуда

$$x_m=\frac{c}{\sqrt{D}+b-cf}=\frac{c(\sqrt{D}-b+cf)}{D-(b-cf)^2}. \tag{2.45}$$

Знаменатель $D-(b-cf)^2=(D-b^2)+c(2bf-cf^2)$ в силу предположения 2) делится на c. После деления оба условия 1) и 2) выполняются.

Таким образом в качестве x_m мы будем получать числа вида $\frac{\sqrt{D}+b}{c}$, где $b<\sqrt{D}$, а $c<D-b^2\leqq D$. Такого рода чисел конечное число, а потому, начиная с некоторого места, они начнут повторяться.

Докажем, что величины x_m начнут повторяться с такой величины, для которой в представлении (2.44) $c=1$. Для этого обратим внимание на то, что в этом выражении $0<\sqrt{D}-b<c$. Действительно, предположив это выполненным для x_{m-1}, мы из равенства $\frac{\sqrt{D}+b}{c}>f$ получим $\sqrt{D}+b-cf>0$ [см. (2.45)]. Другое же неравенство $(\sqrt{D}+b-cf)<\frac{D-(b-cf)^2}{c}$ равносильно такому: $\sqrt{D}-b+cf>c$, которое вытекает из $\sqrt{D}-b>0$ и $f\geqq 1$. Это обстоятельство позволяет однозначно определить по x_m предыдущую величину x_{m-1}. В самом деле, если $x_m=\frac{\sqrt{D}+b}{c}$, то

$$x_{m-1}=f+\frac{1}{x_{m-1}}=f+\frac{c}{\sqrt{D}+b}=f+\frac{\sqrt{D}-b}{c_1}=\frac{\sqrt{D}-b+c_1f}{c_1},$$

где $c_1=\frac{D^2-b}{c}$, а f требуется определить. Но из условия $0<\sqrt{D}-b+c_1f<c$ величина f определяется однозначно. Поэтому, если, например, $x_m=x_n$, то $x_{m-1}=x_{n-1}$, $x_{m-2}=x_{n-2}$, и т. д. Повторение начнется с x_1, с которого начинает соблюдаться условие $0<\sqrt{D}-b<c$. Но

$$x_1=\frac{1}{\sqrt{D}-a}=\frac{\sqrt{D}+a}{D-a^2}.$$

Если также

$$x_{n+1}=\frac{\sqrt{D}+a}{D-a^2},$$

то $x_n=a_n+\frac{1}{x_{n+1}}=\sqrt{D}-a+a_n$, и из условия $0<\sqrt{D}+a-a_n<1$ мы получим $a_n-a=a$, откуда $a_n=2a$. Поэтому звенья разложения $\sqrt{D}$ в непрерывную дробь имеют периоды следующего вида:

$$\sqrt{D}=[a,\ a_1,\ldots,\ a_{n-1};\ 2a,\ a_1,\ldots,a_{n-1};\ 2a,\ a_1,\ldots a_{n-1};\ldots].$$

13. Пусть ξ, η удовлетворяют уравнению Пелля:

$$\xi^2-\eta^2D=\pm 1. \tag{2.46}$$

Тогда $\xi>\eta$,

$$\xi-\eta\sqrt{D}=\frac{\pm 1}{\xi+\eta\sqrt{D}},$$

откуда

$$\left|\frac{\xi}{\eta}-\sqrt{D}\right|=\frac{1}{\eta(\xi+\eta\sqrt{D})}<\frac{1}{2\eta^2},$$

откуда в силу § 2.11 следует, что $\frac{\xi}{\eta}$ есть подходящая дробь разложения $\sqrt{D}$ в непрерывную дробь. Пусть

$$\xi=P_m,\quad \eta=Q_m.$$

Тогда

$$\sqrt{D}=\frac{P_mx_m+P_{m-1}}{Q_mx_m+Q_{m-1}}. \tag{2.47}$$

Предположим, что

$$x_m=\frac{\sqrt{D}+b}{c}.$$

Подставляя в (2.47), получим

$$Q_m\frac{D}{c}+Q_m\frac{b}{c}\sqrt{D}+Q_{m-1}\sqrt{D}=P_m\frac{\sqrt{D}}{c}+P_m\frac{b}{c}+P_{m-1}.$$

Приравнивая рациональные и иррациональные члены, будем иметь:

$$P_m\frac{b}{c}+P_{m-1}=Q_m\frac{D}{c}.$$

$$Q_m\frac{b}{c}+Q_{m-1}=P_m\frac{1}{c}.$$

Умножая первое равенство на $-Q_m$, второе на P_m и складывая, имеем:

$$(-1)^m=(P_m^2-Q_m^2D)\frac{1}{c},$$

откуда в силу (2.46)

$$c=1.$$

Это показывает, что $x_m=\sqrt{D}+b$, т. е. что, начиная со следующего звена, начнет повторяться новый период:

$$x_m=2a+\cfrac{1}{a_1+\cfrac{1}{a_2+\cdots}}$$

Таким образом наименьшее решение уравнений Пелля дается подходящей дробью $\frac{P_n}{Q_n}$, соответствующей первому периоду:

$$\frac{P_n}{Q_n}=a+\cfrac{1}{a_1+\cfrac{}{\cdots+\cfrac{1}{a_{n-1}}}}.$$

Единица $u=P_n+Q_n\sqrt{D}$ является наименьшей из бо́льших 1 единицей поля $k(\sqrt{D})$, так что по доказанному ее степенями исчерпываются все единицы этого поля.

14. Если D имеет вид $4k+1$, то следует также найти единицы вида $\frac{\xi+\eta\sqrt{D}}{2}$, т. е. решить уравнение $\xi^2-\eta^2D=\pm 4$. Будем решать эту задачу, подыскивая наименьшую бо́льшую 1 единицу в форме $\xi+\eta\omega'=\xi+\eta\frac{-1+\sqrt{D}}{2}$. ω' удовлетворяет уравнению

$$\omega'^2+\omega'-\frac{D-1}{4}=\omega'^2+\omega'-m=0.$$

Перепишем условие

$$N(\xi+\eta\omega')=\xi^2+\xi\eta-\eta^2m=\pm 1$$

в таком виде:

$$\left|\frac{\xi}{\eta}-\frac{\sqrt{D}-1}{2}\right|=\frac{1}{\eta\left(\xi+\eta\frac{\sqrt{D}+1}{2}\right)}<\frac{1}{2\eta^2},$$

так как $\sqrt{D}\geqq\sqrt{5}$, $\xi\geqq\eta$. Поэтому $\frac{\xi}{\eta}$ равно подходящей дроби разложения $\omega'=\frac{\sqrt{D}-1}{2}$ в непрерывную дробь.

В этом разложении величины x_m тоже удовлетворяют условиям 1), 2), откуда следует, что периоды начнут повторяться с величины $x_n=\frac{\sqrt{D}+a}{2}=\omega'+\frac{a-1}{2}$, где a — нечетное число. Предположим, что решение имеет вид,

$$\xi=P_n,\ \eta=Q_n, \tag{2.48}$$

где $x_n=\alpha\cdot\omega'+\beta$, α, β — дробные рациональные числа. Имеем:

$$\omega'=\frac{P_n(\alpha\omega'+\beta)+P_{n-1}}{Q_n(\alpha\omega'+\beta)+Q_{n-1}},$$

откуда

$$\begin{gathered}Q_n\alpha(-\omega'+m)+Q_n\beta\omega'+Q_{n-1}\omega'=P_n(\alpha\omega'+\beta)+P_{n-1},\\ -Q_m\alpha+Q_n\beta+Q_{n-1}=P_n\alpha,\\ P_n\beta+P_{n-1}=Q_n\alpha_m.\end{gathered}$$

Умножая предпоследнее уравнение на P_n, последнее на $-Q_n$ и складывая, получим:

$$\alpha(P_n^2+P_nQ_n-Q_n^2m)=\pm1.$$

Таким образом, чтобы (2.47) было решением нашей задачи, необходимо и достаточно, чтобы имело место $\alpha=1$, т. е. чтобы $\frac{P_n}{Q_n}$ было подходящей дробью, завершающей некоторый полный период. Наименьшее решение мы получим, завершив первый период.

Если при этом Q_n окажется четным, то получится решение, которое может быть также получено разложением $\sqrt{D}$. Это всегда случится, если $D\equiv1\pmod 8$, но случается иногда при $D\equiv5\pmod 8$. От этого уравнения простой подстановкой можно перейти к уравнению $x^2-Dy^2=\pm4$. Для решений последнего Кэли (Cayley) составил таблицу, приводимую также в книге Д. А. Граве „Элементарный курс теории чисел“, Киев, 1913.

15. Пример. $D=\sqrt{13}$, $\omega'=\frac{\sqrt{13}-1}{2}$, $m=3$,

$$\omega'^2+\omega'-m=0.$$

Разлагаем ω' в непрерывную дробь:

$$\frac{\sqrt{13}-1}{2}=1+\frac{1}{x},\quad x=\frac{2}{\sqrt{13}-3}=\frac{\sqrt{13}+3}{2}=3+\frac{1}{x},$$

$$\frac{\sqrt{13}-1}{2}=1+\cfrac{1}{3+\cfrac{1}{3+\cdots}}$$

$$\frac{P_1}{Q_1}=\frac{1}{1},\ \xi-\eta\omega'=1-\frac{\sqrt{13}-1}{2}=\frac{3-\sqrt{13}}{2}.\quad N(\xi-\eta\omega')=-1.$$

Наименьшей большей 1 единицей является сопряженная единица $\frac{3+\sqrt{13}}{2}$. Эту единицу можно также получить, разлагая $\sqrt{13}$ и находя x_m вида $\frac{\sqrt{13}+a}{4}$:

$$\sqrt{13}=3+\frac{1}{x};\quad x=\frac{1}{\sqrt{13}-3}=\frac{\sqrt{13}+3}{4}$$

$$\frac{P_1}{Q_1}=\frac{3}{1},\quad u=\frac{3+\sqrt{13}}{2}.$$

§ 3. Аналитические функции Римана и Дирихле

1. Риманн изучил аналитический характер функции

$$\zeta(s)=\sum_{n=1}^{\infty}n^{-s}=1+\frac{1}{2^s}+\frac{1}{3^s}+\cdots, \tag{3.1}$$

рассматриваемой как функция комплексной переменной s. Чтобы избежать многозначности определения n^{-s}, условимся считать

$$n^{-s}=e^{-\lg n\cdot s},$$

где $\lg n$ — арифметический натуральный лпгарифм числа n. Ряд сходится, если $\sigma>1$, где $s=\sigma+it$. Имеет место следующее тождество Эйлера (Euler):

$$\sum_{n=1}^{\infty}n^{-s}=\left\{\prod_p(1-p^{-s})\right\}^{-1}, \tag{3.2}$$

где произведение в правой части распространяется на все простые числа p.

Для вывода этой формулы возьмем s вещественным (случай комплексного s нам не понадобится) и >1, и рассмотрим конечное произведение

$$Q_m^{(s)}=\prod_{p<M}\frac{1}{1-p^{-s}}.$$

Разлагая каждый множитель $\frac{1}{1-p^{-s}}$ в бесконечную прогрессию

$$\frac{1}{1-p^{-s}}=1+p^{-s}+p^{-2s}+p^{-3s}+\cdots$$

и перемножая почленно эти прогрессии, мы получим сумму членов вида $\left(p_1^{k_1}p_2^{k_2}\ldots p_m^{k_m}\right)^{-s}=m^{-s}$, где m — произведение всевозможных степеней простых чисел, не превышающих M. В силу однозначности разложения натуральных чисел на простые множители каждое m будет встречаться только по одному разу. Кратный ряд в силу абсолютной сходимости будет сходиться к одной и той же величине, независимо от порядка членов. Каждый член положителен, в силу чего имеют место неравенства

$$\sum_{n=1}^{M}n^{-s}<\frac{1}{\prod\limits_{p\leqslant M}(1-p^{-s})}<\sum_{n=1}^{\infty}n^{-s}. \tag{3.3}$$

Заставляя M стремиться к бесконечности, мы увидим, что левый член этого неравенства стремится к правому члену, а потому к нему же стремится и правый член, т. е. справедливо тождество (3.2).

2. При $s\to 1$ величина $\sum\limits_{n=1}^{\infty}n^{-s}$ стремится к бесконечности. Для выяснения быстроты этого возрастания просуммируем последующие легко выводимые неравенства:

$$\int_{n}^{n+1}\frac{dx}{x^s}<\frac{1}{n^s}<\int_{n-1}^{n}\frac{dx}{x^s}\qquad(n=2,3\ldots) \tag{3.4}$$

$$\int_{2}^{\infty}\frac{dx}{x^s}<\sum_{n=2}^{\infty}n^{-s}<\int_{1}^{\infty}\frac{dx}{x^s}$$

и прибавим к их частям неравенство

$$\int_{1}^{2}\frac{dx}{x^s}<1^{-s}=1:$$

$$\int_{1}^{\infty}\frac{dx}{x^s}<\sum_{n=1}^{\infty}n^{-s}<1+\int_{1}^{\infty}\frac{dx}{x^s},$$

т. е.

$$\frac{1}{s-1}<\zeta(s)<1+\frac{1}{s-1}. \tag{3.5}$$

Вводя обозначение $P(s-1)$ для функции, остающейся при $s=1$ ограниченной (при этом мы вводим один и тот же символ для разных функций такого рода), мы можем переписать (3.5) так:

$$\zeta(s)=\frac{1}{s-1}+P(s-1). \tag{3.6}$$

Отсюда видно, что при $s\to 1$ $\zeta(s)$ растет с тою же быстротой, что и $\frac{1}{s-1}$.

3. Логарифмируем тождество (3.2), пользуясь (3.6):

$$-\sum_{p}\lg(1-p^{-s})=\lg\left(\frac{1}{s-1}\right)+P(s-1). \tag{3.7}$$

Разлагая в ряд Тэйлора $-\lg(1-x)$, получим:

$$\left.\begin{aligned}-\lg(1-x)=x+\frac{x^2}{2}+\frac{x^3}{3}\ldots=x+\theta(x^2+x^3+\ldots)=\\ =x+\frac{\theta x^2}{1-x},\end{aligned}\right\} \tag{3.8}$$

где $0<\theta<1$.

Подставляя $x=p^{-s}$, будем иметь

$$-\sum_{p}\lg(1-p^{-s})=\sum_{p}p^{-s}+\theta\sum_{p}\frac{p^{-2s}}{1-p^{-s}}. \tag{3.9}$$

Вторая сумма правой части остается при $s\geqq 1$ ограниченной, так как

$$1-p^{-s}\geqq 1-p^{-1}\geqq\frac{1}{2},\quad\sum_{p}p^{-2s}\leqq\sum_{p}p^{-2}\leqq\sum_{n}n^{-2}=\frac{\pi^2}{6}.$$

Поэтому мы имеем право обозначить эту сумму символом $P(s-1)$. Из (3.8) и (3.9) мы получим следующее:

$$\sum_{p}p^{-s}=\lg\frac{1}{s-1}+P(s-1). \tag{3.10}$$

Из этого равенства следует сразу факт существования бесчисленного множества простых чисел (расходимость ряда $\sum\limits_{p}\frac{1}{p}$).

4. Чтобы доказать существование бесчисленного множества простых чисел в каждой арифметической прогрессии

$$ax+b, (a,\ b)=1,$$

Дирихле (Lejeune-Dirichlet) обобщил тождество (3.2), введя понятие *характеров чисел*. Введем более общее понятие *характеров конечной абелевой группы*. Пусть $\mathfrak{A}$ — конечная абелева группа, разлагаемая в прямое произведение циклических групп (см. часть I, стр. 42):

$$\mathfrak{A}=\mathfrak{A}_1\times\mathfrak{A}_2\times\ldots\times\mathfrak{A}_k, \tag{3.11}$$

где каждая из групп $\mathfrak{A}_i$ пусть будет порядка m_i:

$$\mathfrak{A}_i=1+A_i+A_i^2+\ldots+A_i^{m_i-1} \qquad (i=1,\ 2,\ldots,k). \tag{3.12}$$

Будем сопоставлять с каждым элементом A_i какой-нибудь m_i-ый корень из единицы ε_i. Выбор для каждого A_i можно сделать m_i различными способами, по числу различных m_i-ых корней из единицы. Независимо выбирая такой корень для каждого элемента A_i, мы получим всего

$$m=m_1\cdot m_2\ldots m_k \tag{3.13}$$

различных систем, каждую из которых мы будем называть характером группы A_i. Число m равно порядку группы $\mathfrak{A}$.

Фиксируя какой-нибудь определенный характер и считая его функцией от элементов A_i группы $\mathfrak{A}$, определим значение этой функции для любого элемента группы $\mathfrak{A}$. Из разложения (3.11) следует, что всякий элемент A можно, притом однозначно, представить в виде

$$A=A_1^{\omega_1}\cdot A_2^{\omega_2}\ldots A_k^{\omega_k}. \qquad (0\leqq\omega_i<m_i) \tag{3.14}$$

Определим характер $\chi(A)$ элемента A при помощи равенства

$$\chi(A)=\varepsilon_1^{\omega_1}\cdot\varepsilon_2^{\omega_2}\ldots\varepsilon_k^{\omega_k}. \tag{3.15}$$

В частности,

$$\chi(A_i)=\varepsilon_i.$$

Из равенства (3.15) следует важное соотношение

$$\chi(AB)=\chi(A)\cdot\chi(B). \tag{3.16}$$

Если теперь возьмем два различных характера $\chi_1(A)$ и $\chi_2(B)$ (всего мы имеем m различных характеров), то произведение $\chi_1(A)\,\chi(A)$ тоже является характером группы $\mathfrak{A}$. Таким образом характеры абелевой группы тоже образуют мультипликативную абелеву группу порядка m. Производящие элементы этой группы мы получим, беря в качестве $\chi(A_i)$ единицы

за исключением одного $\chi(A_i)$, значением которого берется первообразный m_i-ый корень из единицы:

$$\chi_i(A_1)=1,\ldots,\chi_i(A_{i-1})=1,\ \chi_i(A_i)=\varepsilon_i,\ \chi_i(A_{i+1})=1,\ldots,\chi_i(A_k)=1.$$

Роль единичного элемента здесь играет так называемый *главный характер*, т. е. функция $\chi_0(A)$, все значения которого равны 1. Так как порядок характера $\chi_i(A)$, как производящего элемента группы характеров, равен m_i, то группа характеров изоморфна с $\mathfrak{A}$.

5. Выведем два важных соотношения между характерами.

I. Рассмотрим выражение

$$\varphi=\sum_A\chi(A), \tag{3.17}$$

в котором характер χ один и тот же, а сумма распространена на все элементы группы $\mathfrak{A}$. Если χ—главный характер, т. е. $\chi(A)=1$, то очевидно $\varphi=m$. Если же χ отличен от главного, то существует элемент B, для которого $\chi(B)\neq1$. Умножая φ на $\chi(B)$ и пользуясь (3.16), получим:

$$\varphi\cdot\chi(B)=\sum_A\chi(A\cdot B).$$

Но так как AB пробегает одновременно с A всю группу $\mathfrak{A}$, то

$$\varphi\cdot\chi(B)=\varphi,$$

откуда

$$\varphi=0.$$

Таким образом

$$\sum_A\chi(A)=m, \tag{3.18}$$

если χ — главный характер, и $=0$—в противном случае.

II. Рассмотрим выражение

$$\psi=\sum_\chi\chi(A), \tag{3.19}$$

где элемент A один и тот же, а сумма распространена на все характеры группы $\mathfrak{A}$. Если A — единичный элемент, то очевидно $\psi=m$. В противном случае всегда можно найти характер χ_1, для которого $\chi_1(A)\neq1$. Умножая (3.19) на $\chi_1(A)$ и пользуясь тем, что $\chi(A)\,\chi_1(A)$ пробегает одновременно с $\chi(A)$ всю группу характеров, получим:

$$\psi\cdot\chi_1(A)=\psi,$$

откуда

$$\psi=0.$$

Итак

$$\sum_{\chi}\chi(A)=m, \tag{3.20}$$

если A — единичный элемент, и $=0$ — в противном случае.

6. Дирихле взял в роли группы $\mathfrak{A}$ мультипликативную группу классов сравнений по модулю a, взаимно простых с a, где a— разность рассматриваемой арифметической прогрессии $ax+b$. Под характером $\chi(n)$ числа n он понимает характер того класса, в котором лежит n. В случае же, если n не взаимно просто с a, будем полагать $\chi(n)=0$. Тогда в силу (3.16)

$$\chi(nn')=\chi(n)\cdot\chi(n'). \tag{3.21}$$

Далее, Дирихле ввел в рассмотрение функцию

$$L(s,\ \chi)=\sum_{n=1}^{\infty}\chi(n)\cdot n^{-s}. \tag{3.22}$$

Этот ряд абсолютно сходится при $s>1$. В силу (3.21) для него тоже имеет место тождество, аналогичное тождеству (3.2):

$$L(s,\ \chi)=\sum_{n=1}^{\infty}\chi(n)\cdot n^{-s}=\frac{1}{\prod\limits_{p}[1-\chi(p)\cdot p^{-s}]}, \tag{3.23}$$

где произведение распространяется на все простые числа p. Простые делители числа a в нем не фигурируют, так как для них $\chi(p)=0$.

Ряд (3.22) может быть также представлен следующим образом:

$$L(s,\ \chi)=\chi(1)\sum_{n_1}n_1^{-s}+\chi(k_2)\sum_{n_2}n_2^{-s}+\ldots+\chi(k_\varphi)\sum_{n_\varphi}n_\varphi^{-s}, \tag{3.24}$$

где $\varphi=\varphi(a)$, $k_1=1$, $k_2,\ldots,k_\varphi$ — совокупность взаимно простых с a вычетов по модулю a и n_i — числа, сравнимые с k_i по модулю a.

Рассмотрим каждую из сумм в правой части (3.24):

$$\sum_{n_i}n^{-s}=\sum_{m=0}^{\infty}(k_i+am)^{-s}.$$

Но

$$\int_{m}^{m+1}(k_i+ax)^{-s}\,dx<(k_i+a_m)^{-s}<\int_{m-1}^{m}(k_i+ax)^{-s}dx,$$

т. е.

$$\int_{0}^{\infty}(k_i+ax)^{-s}\,dx<\sum_{m=0}^{\infty}(k_i+am)^{-s}<\frac{1}{k_i^{s}}+\int_{0}^{\infty}(k_i+ax)^{-s}\,dx,$$

откуда

$$\sum_{n_i}n_i^{-s}=\frac{1}{(s-1)ak_i^{s-1}}+\frac{\theta}{k_i^{s}}, \tag{3.25}$$

где

$$0\leqslant\theta\leqslant1.$$

Разлагая $\frac{1}{k_i^{s-1}}$ в ряд Тэйлора (из двух членов), получим:

$$\frac{1}{k_i^{(s-1)}}=e^{-(s-1)\lg k_i}=1-(s-1)\lg k_1,\ .\ ,k_i^{-(\theta\ s\ -\ 1)},$$

где $0\leqslant\theta_1\leqslant1$. Равенство (3.25) принимает вид:

$$\sum_{n_i}n_i^{-s}=\frac{1}{(s-1)a}-\frac{\lg k_i}{a}\cdot k_i^{-(\theta\ s-1)}+\frac{\theta}{k_i^{s}}.$$

Подставляя в (3.24), мы в силу (3.18) получаем:

$$L(s,\ \chi)=\sum_{i}\chi(k_i)\left\{\frac{\lg k_i}{a}\,k_i^{-(\theta\ s-1)}+\frac{\theta}{k_i^{s}}\right\}. \tag{3.26}$$

Выражение в правой части остается конечным при $s=1$. Для нас важно также установить, что оно не стремится к нулю. Доказательство этого факта представляло большие трудности как для самого Дирихле, так и для позднейших авторов. Мы, следуя Веберу (H. Weber), убедимся в этом впоследствии (§ 4.5) косвенным путем, а пока примем этот факт на веру.

7. Из (3.26) следует, что логарифм выражения $|L(s,\ \chi)|$ остается ограниченным при стремлении s к единице. Принимая это во внимание и логарифмируя равенство (3.23), получим:

$$-\Re\left\{\sum_{p}\lg(1-\chi(p)\cdot p^{-s})\right\}=P(s-1). \tag{3.27}$$

В этой формуле символ $\Re$ обозначает „вещественная часть выражения в фигурных скобках“. Несмотря на многозначность определения логарифма от комплексной величины, вещественная часть логарифма однозначна в силу формулы

$$e^{u+iv}=e^{u}(\cos v+i\sin v),\ \lg1=2\pi\ ik,$$

откуда

$$\lg\{e^{u}(\cos v+i\sin v)\}=u+iv+2\pi ik,$$

т. е.

$$\lg(x+iy)=\lg|x+iy|+i\operatorname{arctg}\frac{y}{x}+2\pi ik.$$

Не делая предположения относительно необращения в нуль предела $\lim\limits_{s\to 1} L(s,\chi)$, мы вместо формулы (3.27) получим:

$$-\Re\left\{\sum_p \lg[1-\chi(p)p^{-s}]\right\}\leqq P(s-1). \tag{3.28}$$

Эту формулу следует понимать в таком смысле, что ее левая часть при $s\to 1$ или остается конечной, или стремится к отрицательной бесконечности.

Рассуждая, как в § 3.3, мы получим из формулы (3.28):

$$\Re\left\{\sum_p \chi(p)\cdot p^{-s}\right\}\leqq P(s-1). \tag{3.29}$$

Перепишем эту формулу так:

$$\Re\left\{\chi(1)\sum_{p_1}p_1^{-s}+\chi(k_2)\sum_{p_2}p_2^{-s}+\ldots+\right.$$
$$\left.+\chi(k_\varphi)\sum_{p_\varphi}p_\varphi^{-s}\right\}\leqq P(s-1), \tag{3.30}$$

где p_i обозначают простые числа, удовлетворяющие сравнению

$$p_i\equiv k_i\pmod a. \tag{3.31}$$

Просуммируем формулу (3.30) по всем характерам (кроме главного) и приложим к этой сумме формулу (3.10), которую можно, отбросив в ее левой части слагаемые p^{-s}, соответствующие простым делителям числа a, переписать так:

$$\sum_{p_1}p_1^{-s}+\sum_{p_2}p_2^{-s}+\ldots+\sum_{p_\varphi}p_\varphi^{-s}=lg\frac{1}{s-1}+P(s-1). \tag{3.32}$$

Тогда в силу (3.20) мы получим:

$$\varphi(a)\cdot\sum_{p_1}p_1^{-s}\leqq lg\frac{1}{s-1}+P(s-1). \tag{3.33}$$

Если при этом хоть в одной из формул (3.30) имеет место знак $<$ (т. е. если ее левая часть стремится к отрицательной бесконечности), то и в формуле (3.33) не может иметь место знак $=$. Поэтому если мы докажем (что мы впоследствии и сделаем), что в формуле (3.33) имеет место знак равенства, то этим будет доказано, что знак $=$ имеет место также во всех формулах (3.30).

8. Для дальнейшего более удобно иметь дело с однозначными функциями, а потому мы не логарифмируем формулы (3.23), а возьмем от нее логарифмическую производную. Но для этого предварительно надо убедиться, что левая часть формулы (3.23) представляет собой аналитическую функцию. В этом мы убедимся так. Делая в известной формуле

$$\Gamma(s)=\int_0^\infty e^{-t}t^{s-1}\,dt \tag{3.34}$$

(величину $t^{s-1}=e^{\lg t(s-1)}$ можно считать однозначной даже для комплексных значений s, если под $\lg t$ разуметь его арифметическую величину) подстановку $t=nx$, мы получим:

$$\frac{1}{n^s}=\frac{1}{\Gamma(s)}\int_0^\infty e^{-nx}x^{s-1}\,dx. \tag{3.35}$$

Подставляя в выражение $L(s,\chi)$, будем иметь:

$$L(s,\chi)=\sum_{n=1}^\infty\frac{\chi(n)}{n^s}=\frac{1}{\Gamma(s)}\int_0^\infty x^{s-1}\sum_{n=1}^\infty\chi(n)e^{-nx}\cdot dx=$$
$$=\frac{1}{\Gamma(s)}\int_0^\infty x^{s-1}\sum_{k=1}^{a=1}\frac{\chi(k)e^{-kx}}{1-e^{-ax}}\,dx. \tag{3.36}$$

Правая часть имеет конечный аналитический смысл при $s>0$, так как и числитель и знаменатель подинтегральной суммы обращаются при $x=0$ в нули, и знаменатель — нуль первого порядка. Это дает нам право диференцировать $L(s,\chi)$.

Аналогичную формулу мы получим для $\zeta(s)$:

$$\zeta(s)=\sum_{n=1}^\infty\frac{1}{n^s}=\frac{1}{\Gamma(s)}\int_0^\infty x^{s-1}\frac{e^{-x}}{1-e^{-x}}\,dx=\frac{1}{\Gamma(s)}\int_0^1 x^{s-2}\,dx+$$
$$+\frac{1}{\Gamma(s)}\int_0^1 x^{s-2}\frac{xe^{-x}-1+e^{-x}}{1-e^{-x}}\,dx. \tag{3.37}$$

В этом выражении второй интеграл остается конечным при $s>0$. Первый же интеграл равен при $s>1$

$$\frac{1}{\Gamma(s)}\cdot\frac{1}{s-1}.$$

9. Беря логарифмическую производную от обеих частей формулы (3.23), получим:

$$\frac{L'(s,\chi)}{L(s,\chi)} = -\sum_p \frac{\chi(p)\lg p \cdot p^{-s}}{1-\chi(p)p^{-s}}. \tag{3.39}$$

Принимая, что знаменатель $L(s,\chi)$ левой части не обращается при $s=1$ в нуль, мы убедимся, что правая часть остается при $s<1$ конечной. Переписывая ее следующим образом:

$$-\sum_p \frac{\chi(p)\lg p \cdot p^{-s}}{1-\chi(p)p^{-s}} =$$

$$= -\sum_p \chi(p)\lg p \cdot p^{-s} - \sum_p \frac{\chi(p^2)\lg p \cdot p^{-2s}}{1-\chi(p)p^{-s}}, \tag{3.40}$$

мы убедимся, что вторая сумма правой части сходится при $s \geqslant 1$.

Таким образом и первая сумма остается при $s=1$ конечной, и мы получаем:

$$\chi(1)\sum_{p_1}\lg p_1 p_1^{-s} + \chi(k_2)\sum_{p_2}\lg p_2 p_2^{-s} + \ldots +$$
$$+\chi(k_\varphi)\sum_{p_\varphi}\lg p_\varphi p_\varphi^{-s} = P(s-1). \tag{3.41}$$

Точно так же, находя логарифмическую производную от обеих частей формулы (3.2) и пользуясь (3.37), мы получим:

$$\sum_{p_1}\lg p_1 p_1^{-s} + \sum_{p_2}\lg p_2 p_2^{-s} + \ldots +$$
$$+\sum_{p_\varphi}\lg p_\varphi p_\varphi^{-s} = \frac{1}{s-1} + P(s-1). \tag{3.42}$$

Чтобы получить оценку какой-нибудь из сумм, входящих в (3.41) и (3.42), например $\sum_{p_u}\lg p_u p_u^{-s}$, умножим формулу (3.41) на $\chi^{-1}(k_u)$, просуммируем по всем неглавным характерам и приложим к сумме формулу (3.42). Тогда, принимая во внимание (3.19), мы получим:

$$\sum_\chi \chi(k_i)\chi^{-1}(k_u) = \sum_\chi \chi(k_i k_u^{-1}) = 0 \qquad (u \neq i)$$
$$\sum_\chi \chi(k_u)\chi^{-1}(k_u) = \sum_\chi 1 = \varphi(a),$$

откуда

$$\sum_{p_u}\lg p_u \cdot p_u^{-s} = \frac{1}{\varphi(a)} \cdot \frac{1}{s-1} + P(s-1). \tag{3.43}$$

Эта формула показывает, что сумма левой части, распространенная по всем простым числам вида $ax+k_u$, стремится к бесконечности, когда s стремится к 1. Но так как каждый член этой суммы остается конечным при всех значениях s, то отсюда мы должны заключить, что эта сумма содержит бесчисленное множество членов, и мы приходим к следующему знаменитому результату Дирихле:

Теорема 40. Всякая арифметическая прогрессия $ax+k$, где $(a,k)=1$, содержит бесчисленное множество простых чисел.

10. Если мы имеем какую-нибудь совокупность простых чисел p, то сумма $\sum_p \lg p \cdot p^{-s}$, распространенная на эту совокупность, растет при стремлении s к 1 не быстрее, чем $\frac{1}{s-1}$. Во многих случаях ее рост характеризуется членом $k \cdot \frac{1}{s-1}$, где k — правильная дробь. В этих случаях мы будем называть число k *плотностью* этой совокупности. Если в совокупность входят все простые числа, то ее плотность равна единице. Если совокупность содержит все простые числа прогрессии $ax+k$, где $(a,k)=1$, то формула (3.43) показывает, что плотность этой совокупности равна $\frac{1}{\varphi(a)}$.

Нетрудно убедиться в справедливости следующей теоремы:

Плотность совокупности, составленной из двух взаимно простых совокупностей простых чисел, равна сумме плотностей этой совокупности.

11. Приведенное доказательство теореме Дирихле оставляет место некоторой неудовлетворенности. В самом деле, факт расходимости ряда $\sum_{p_u} \lg p_u \cdot p_u^{-1}$ не дает возможности заключить, что в каком-нибудь конечном интервале мы непременно встретим простое число требуемого вида.

Кронекер и Мертенс (F. Mertens) решили задачу в этом смысле. Более детально изучив остаточный член формулы (3.43), они указали способы находить величины интервалов, внутри которых непременно содержатся простые числа, входящие в заданную прогрессию. Мы не будем останавливаться на их исследованиях.

§ 4. Функция Дедекинда

1. Дедекинд ввел в рассмотрение функцию

$$\zeta_k(s) = \sum_{\mathfrak{a}} |N(\mathfrak{a})|^{-s}, \tag{4.1}$$

в которой $\mathfrak{a}$ пробегает все идеалы заданного алгебраического поля k. Для тех значений s, для которых ряд сходится (если таковые значения имеются), мы получим, рассуждая, как в § 3, следующее разложение этой функции в произведение:

$$\zeta_k(s) = \sum_{\mathfrak{a}} |N(\mathfrak{a})|^{-s} = \frac{1}{\prod\limits_{\mathfrak{P}} \{1 - |N(\mathfrak{P})^{-s}\}}. \tag{4.2}$$

Произведение правой части сходится тогда и только тогда, когда сходится ряд $\sum\limits_{\mathfrak{P}} |N(\mathfrak{P})|^{-s}$. Но $|N(\mathfrak{P})| = p^f$, и число различных идеалов, имеющих нормой степень одного и того же числа p, не превышает степени поля n. Поэтому имеет место неравенство

$$\sum_{\mathfrak{P}} |N(\mathfrak{P})|^{-s} < n \sum_{p} p^{-s},$$

показывающее, что при $s > 1$ этот ряд сходится. Значит, произведение в правой части формулы (4.2) остается при $s > 1$ ограниченным. Отсюда следует, что и ряд в левой части (4.2) ограничен при $s > 1$, а потому в силу положительности своих членов он сходится.

2. Чтобы изучить поведение функции $\zeta_k(s)$ вблизи точки $s = 1$, разобьем сумму (4.1) на h частичных сумм (h—число идеальных классов поля k), в каждой из которых суммирование распространено на все идеалы, входящие в один определенный идеальный класс поля k. Выберем в каждом из h идеальных классов по представителю: $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_h$. Тогда, если $\mathfrak{b}$ пробегает все идеалы класса, противоположенного классу идеала $\mathfrak{a}$, то произведение $\mathfrak{a}\mathfrak{b}$ пробегает все главные идеалы, делящиеся на $\mathfrak{a}$. Другими словами, это произведение пробегает делящиеся на $\mathfrak{a}_i$ целые числа поля k, и притом из всех ассоциированных чисел каждое только один раз.

Найдем предел

$$\lim_{t \to \infty} \frac{T_i}{t}, \tag{4.3}$$

где T_i — число идеалов класса, обратного классу $\mathfrak{a}_i$, норма которых не превышает положительного числа t. Для этого рассмотрим базис $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$ идеала $\mathfrak{a}$. Если $\mathfrak{b}$ идеал, удовлетворяющий этим требованиям, то $\mathfrak{a}\mathfrak{b}$ ассоциирован

с некоторым числом $\alpha = \mu_0 x_0 + \mu_1 x_1 + \ldots + \mu_{n-1} x_{n-1}$ $x_0, x_1, \ldots, x_{n-1}$ — целые рациональные числа, подчиненные неравенству

$$|N(\mu_0 x_0 + \mu_1 x_1 + \ldots + \mu_{n-1} x_{n-1})| \leqq N(\mathfrak{a}_i) \cdot t. \tag{4.4}$$

Из всех чисел этого типа нужно выбрать некоторые таким образом, чтобы из каждой совокупности ассоциированных друг с другом чисел было взято по одному и только по одному представителю. Способ находить представителей из систем ассоциированных чисел был разобран в § 2.6 (нормированные числа). Именно, введем при помощи формул

$$\lambda = \delta \lg |\alpha|, \quad \lambda' = \delta' \lg |\alpha'|, \quad \ldots, \quad \lambda^{(\nu-1)} = \delta^{(\nu-1)} \lg |\alpha|^{(\nu-1)} \tag{4.5}$$

числа $\lambda, \lambda', \ldots, \lambda^{(\nu-1)}$, где $\alpha', \ldots, \alpha^{(\nu-1)}$ — сопряженные с α числа, а $\delta^{(i)}$ равно 1, если сопряженное поле $k^{(i)}$ вещественно, и 2, если оно мнимое. Затем из линейных уравнений

$$\left.\begin{aligned} \lambda &= \xi l + \xi_1 l_1 + \ldots + \xi_{\nu-2} l_{\nu-2} + \xi_{\nu-1} \delta, \\ \lambda' &= \xi l' + \xi_1 l_1' + \ldots + \xi_{\nu-2} l'_{\nu-2} + \xi_{\nu-1} \delta', \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \lambda^{(\nu-1)} &= \xi l^{(\nu-1)} + \xi_1 l_1^{(\nu-1)} + \ldots \\ &\ldots + \xi_{\nu-2} l_{\nu-2}^{\nu-1} + \xi_{\nu-1} \delta^{(\nu-1)}, \end{aligned}\right\} \tag{4.6}$$

где $l_j^{(i)}$ — логарифмы чисел, сопряженных с основными единицами поля, мы получим $\xi, \xi_1, \ldots, \xi_{\nu-2}$, называемые показателями числа α. Так при помощи умножения α на целесообразно подобранную единицу мы можем добиться того, чтобы эти показатели оказались удовлетворяющими неравенствам

$$0 \leqq \xi < 1, \quad 0 \leqq \xi_1 < 1, \ldots, \quad 0 \leqq \xi_{\nu-2} < 1, \tag{4.7}$$

и таких чисел, ассоциированных с α, будет всего w, где w — число корней из единицы (включая $+1$ и -1), входящих в k.

Таким образом число $w T_i$ равно числу точек $(x_0, x_1, \ldots, x_{n-1})$ с целыми координатами, заключенных внутри объема, ограниченного поверхностями (4.4) и (4.7) n-мерного пространства. При этом числа $\xi, \xi_1, \ldots, \xi_{\nu-1}$ определяются из соотношений (4.5) и (4.6).

Введем теперь подстановку

$$x_0 = y_0 \sqrt[n]{\tau}, \quad x_1 = y_1 \sqrt[n]{\tau}, \quad \ldots, \quad x_{n-1} = y_{n-1} \sqrt[n]{\tau}, \tag{4.8}$$

где

$$\tau = t \cdot N(\mathfrak{a}_i).$$

Если вместо $\alpha^{(i)} = \mu_0^{(i)} x_0 + \mu_1^{(i)} x_1 + \ldots + \mu_{n-1}^{(i)} x_{n-1}$ мы станем рассматривать числа $\beta^{(i)} = \mu_0^{(i)} y_0 + \mu_1^{(i)} y_1 + \ldots + \mu_{n-1}^{(i)} y_{n-1}$ и со-

ответственно вместо $\lambda^{(i)} - \rho^{(i)}$ и вместо $\xi_i - \eta_i$, определяемые из формул

$$\rho^{(i)} = \delta^{(i)} \cdot \lg |\beta^{(i)}| \tag{4.9}$$

$$\left.\begin{aligned} \rho &= \eta_1 l + \eta_{11} l_1 + \ldots + \eta_{\nu-2} l_{\nu-2} + \eta_{\nu-1} \delta \\ \rho' &= \eta_1 l' + \eta_{11}' l_1' + \ldots + \eta_{\nu-2} l'_{\nu-2} + \eta_{\nu-1} \delta' \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \rho^{(\nu-1)} &= \eta_1 l^{(\nu-1)} + \eta_{11} l_1^{(\nu-1)} + \ldots \\ &\ldots + \eta_{\nu-2} l_{\nu-2}^{(\nu-1)} + \eta_{\nu-1} \delta^{(\nu-1)}, \end{aligned}\right\} \tag{4.10}$$

то новые переменные связаны со старыми формулами:

$$\alpha^{(i)} = \beta^{(i)} \cdot \sqrt[n]{\tau}$$

$$\lambda^{(i)} = \rho^{(i)} + \frac{\delta^{(i)}}{n} \cdot \lg \tau$$

$$\xi = \eta, \quad \xi_1 = \eta_{11}, \quad \ldots, \quad \xi_{\nu-2} = \eta_{\nu-2}, \quad \xi_{\nu-1} = \eta_{\nu-1} + \frac{1}{n} \lg \tau.$$

Из (4.6) видно, что

$$\xi_{\nu-1} = \frac{1}{n}(\lambda + \lambda' + \ldots + \lambda^{(n-1)}) = \frac{1}{n} \lg N\,|\alpha|.$$

Поэтому неравенства (4.4) и (4.7) перепишутся в новых координатах так:

$$-\infty < \eta_{\nu-1} < 0, \tag{4.11}$$

$$0 \leqq \eta < 1, \quad 0 \leqq \eta_{11} < 1, \quad \ldots, \quad 0 \leqq \eta_{\nu-2} < 1. \tag{4.12}$$

Получается поверхность, не зависящая от t, и искомое число $w T_i$ равно числу точек внутри этой поверхности, координаты которых суть целочисленные кратные числа $\frac{1}{\sqrt[n]{\tau}}$. Согласно теории кратных интегралов, объем тела, ограниченного этой поверхностью, равен пределу числа такого рода точек, умноженного на $\left(\frac{1}{\sqrt[n]{\tau}}\right)^n = \frac{1}{\tau}$ (т. е. сумма объемов, помещаемых внутри поверхности малых кубов с ребрами длины $\frac{1}{\sqrt[n]{\tau}}$). Таким образом, обозначая объем тела через V, получим:

$$\lim_{\tau \to \infty} \frac{w T_i}{\tau} = V,$$

или

$$\lim_{t \to \infty} \frac{T_i}{t} = \frac{N(\mathfrak{a}_i)}{w} \cdot V. \tag{4.13}$$

Более детальное рассмотрение точек с координатами, кратными $\frac{1}{\sqrt[n]{\tau}}$, вблизи поверхностей (4.11), (4.12), дает более точную формулу:

$$T_i = t \cdot \frac{N(\mathfrak{a}_i)}{w} \cdot V + t^{1-\frac{1}{n}} \cdot S_t, \tag{4.14}$$

где S_t — величина, остающаяся конечной при возрастании t [см. H. Weber, Lehrbuch der Algebra, Bd. 2, 2-е изд., Braunschweig, 1899, стр. 712, формула (6)].

3. Обратимся к вычислению объема V тела, ограниченного поверхностями (4.11), (4.12). Вспомним формулу преобразования кратных интегралов:

$$\int\int \ldots \int dx_1\, dx_2 \ldots dx_n = \int\int \ldots \int \frac{d(x_1, x_2, \ldots, x_n)}{d(y_1, y_2, \ldots, y_n)}\, dy_1\, dy_2 \ldots dy_n, \tag{4.15}$$

где

$$\frac{d(x_1, x_2, \ldots, x_n)}{d(y_1, y_2, \ldots, y_n)} = \begin{vmatrix} \frac{\partial x_1}{\partial y_1}, \ldots, \frac{\partial x_n}{\partial y_1} \\ \ldots\ldots \\ \frac{\partial x_1}{\partial y_n}, \ldots, \frac{\partial x_n}{\partial y_n} \end{vmatrix} \tag{4.16}$$

есть якобиан системы функций $x_1, x_2, \ldots, x_n$ относительно $y_1, y_2, \ldots, y_n$. При этом мы полагаем систему функций однозначно обратимой и не уточняем вопроса о знаке, так что равенство (4.15) должно обозначать лишь равенство абсолютных значений обеих частей.

Перейдем в выражении нашего объема V от переменных $y_0, y_1, \ldots, y_{n-1}$ к $\eta, \eta_1, \ldots, \eta_{\nu-1}$, которые подчинены весьма простым неравенствам (4.11) и (4.12). Будем совершать переход постепенно. Из n сопряженных с k полей у нас $s = 2\nu - n$ вещественных и $n - \nu$ пар мнимых.

Сначала перейдем к переменным $\beta, \beta', \ldots, \beta^{n-1}$. Для удобства выкладок примем во внимание, что формула преобразования справедлива и тогда, если некоторые из переменных комплексны, $\beta^{(i)}$ связаны с y_i линейными соотношениями

$$\beta^{(i)} = \mu_0^{(i)} y_0 + \mu_1^{(i)} y_1 + \ldots + \mu_{n-1}^{(i)} y_{n-1} \quad (i = 0, 1, \ldots, n-1),$$

определитель которых есть квадратный корень из дискриминанта базиса $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$ идеала $\mathfrak{a}_i$ и потому равен $N(\mathfrak{a}_i)\sqrt{D}$, где D — дискриминант поля (см. § 1.2).

Поэтому

$$V=\int\int\dots\int dy_0dy_1\dots dy_{n-1}=\frac{1}{N(\mathfrak{a}_i)\sqrt{|D|}}\left|\int\int d\beta\,d\beta'\dots d\beta^{(n-1)}\right|.$$

Перейдем к полярным координатам. Пусть k, $k',\dots,k^{(s-1)}$ — вещественные поля, а k_{s+i}, $k_{\nu+i}(i=0,\ 1,\dots,n-\nu-1)$ — пары сопряженно-комплексных. Пусть

$$\beta=\pm r,\quad \beta'=\pm r',\dots,\beta^{(s-1)}=\pm r^{(s-1)}, \tag{4.17}$$

$$\beta^{(s+i)}=r_ie^{i\varphi_i},\quad \beta^{(\nu+i)}=r_ie^{-i\varphi_i}\ (i=0,\ 1,\dots,n-\nu-1) \tag{4.18}$$

будет наше преобразование. r, $r',\dots,r^{(s-1)}$, r_0, $r_1,\dots,r_{n-\nu-1}$ — положительные переменные. Это преобразование законно в силу того, что в неравенствах (4.11), (4.12) входят неявным образом только абсолютные значения переменных $\beta^{(i)}$, но одно не однозначно, так как каждой системе значений r, φ соответствует 2^s различных значений $\beta^{(i)}$, получаемых при различных комбинациях знаков в формулах (4.17). Поэтому перед преобразованием интеграл можно разбить на 2^s интегралов (в зависимости от знаков β, $\beta',\dots,\beta^{(s-1)}$), которые все равны между собой, и в конечном итоге нам просто придется ввести множитель $2^s=2^{2\nu-n}$.

Якобиан преобразования здесь равен произведению якобианов

$$\frac{d\beta^{(i)}}{dr^{(i)}}\text{ (равных единице) и }\frac{d(\beta^{(s+i)},\beta^{(\nu+1)})}{d(r_i,\varphi_i)}=\begin{vmatrix} e^{i\varphi_i} & e^{-i\varphi_i}\\ ir_ie^{i\varphi_i} & -ir_ie^{-i\varphi_i}\end{vmatrix}=-2ir_i,$$

откуда

$$V=\frac{2^{2\nu-n}}{N(\mathfrak{a}_i)\sqrt{|D|}}\cdot 2^{n-\nu}\cdot\int\int\dots\int r_0r_1\dots r_{n-\nu-1}\,drdr'\dots dr^{(s-1)}\times$$
$$\times dr_0\dots dr_{n-\nu-1}\cdot d\varphi_0d\varphi_1\dots d\varphi_{n-\nu-1}. \tag{4.19}$$

Так как ни подинтегральная величина, ни неравенства (4.11), (4.12) не зависят от $\varphi_0,\varphi_1,\dots,\varphi_{n-\nu-1}$, то мы сейчас можем произвести интегрирование по этим переменным в пределах от 0 до 2π:

$$V=\frac{2^n\pi^{n-\nu}}{N(\mathfrak{a}_i)\sqrt{|D|}}\int\int\dots\int r_0r_1\dots r_{n-\nu-1}\cdot drdr'\dots dr^{(s-1)}\times$$
$$\times dr_0\dots dr_{n-\nu-1}. \tag{4.20}$$

Перейдем к переменным $\rho^{(i)}$, связанным с r_i, $r^{(i)}$ формулами (4.9), которые можно переписать так:

$$r=e^{\rho},\ r'=e^{\rho'},\dots,r^{(s-1)}=e^{\rho^{(s-1)}}=e^{\rho^{(s-1)}},\ r_0=$$
$$=e^{\frac{1}{2}\rho^{(s)}},\dots,r_{n-\nu-1}=e^{\frac{1}{2}\rho^{(\nu-1)}} \tag{4.21}$$
$$(\delta=\delta'=\dots=\delta^{(s-1)}=1,\ \delta^{(s)}=\delta^{(s+1)}=\dots=\delta^{(\nu-1)}=2).$$

Якобиан этого преобразования равен

$$\frac{dr}{d\rho}\cdot\frac{dr'}{d\rho'}\cdots\frac{dr^{(s-1)}}{d\rho^{(s-1)}}\cdot\frac{dr_0}{d\rho^{(s)}}\cdots\frac{dr_{n-\nu-1}}{d\rho^{(\nu-1)}}=$$
$$=e^{\rho+\rho'+\dots+\rho^{(s-1)}+\frac{1}{2}\rho^{(s)}+\dots+\frac{1}{2}\rho^{(\nu-1)}}\cdot\frac{1}{2^{n-\nu}}.$$

Подставляя в (4.20) и пользуясь (4.21), получим:

$$V=\frac{2^n\cdot\pi^{n-\nu}}{N(\mathfrak{a}_i)\sqrt{|D|}}\cdot\frac{1}{2^{n-\nu}}\int\int\dots\int e^{\rho+\rho'+\dots+\rho^{(s-1)}+\rho^{(s)}+\dots+\rho^{(\nu-1)}}\times$$
$$\times d\rho\cdot d\rho'\dots d\rho^{(\nu-1)}. \tag{4.22}$$

Наконец, перейдем к переменным $\eta,\eta_1,\dots,\eta^{\nu-2},\eta^{\nu-1}$, пользуясь преобразованием (4.10). Якобиан этого преобразования, равный определителю линейной подстановки (4.10), равен, как мы это видели в § 2.6, $n\cdot L$, где L—регулятор поля k. Кроме того, складывая формулы (4.10), мы убедимся, что

$$\rho+\rho'+\dots+\rho^{(\nu-1)}=n\cdot\eta_{\nu-1},$$

и наш интеграл преобразуется в следующий:

$$V=\frac{2^\nu\cdot\pi^{n-\nu}}{N(\mathfrak{a}_i)\sqrt{|D|}}\,n\cdot L\cdot\int\int\dots\int e^{n\eta_{\nu-1}}\cdot d\eta\cdot d\eta_1\dots d\eta_{\nu-2}d\eta_{\nu-1}.$$

Этот интеграл, в силу независимости пределов интегрирования (4.11), (4.12) для каждой переменной от остальных переменных, а также вида подинтегральной функции, распадается на произведение простых интегралов:

$$V=\frac{2^\nu\cdot\pi^{n-\nu}}{N(\mathfrak{a}_i)\sqrt{|D|}}\,n\cdot L\int_0^1 d\eta\int_0^1 d\eta_1\dots\int_0^1 d\eta_{\nu-2}\cdot\int_{-\infty}^{0} e^{n\eta_{\nu-1}}\cdot d\eta_{\nu-1}.$$

Все интегралы-множители равны единице, за исключением последнего, равного $\frac{1}{n}$. Поэтому окончательно:

$$V=\frac{2^{\nu}\cdot\pi^{n-\nu}L}{N(\mathfrak{a}_i)\sqrt{|D|}}. \tag{4.24}$$

Подставляя в формулу (4.13), получим:

$$\lim_{t\to\infty}\frac{T_i}{t}=\frac{2^{\nu}\cdot\pi^{n-\nu}\cdot L}{w\cdot\sqrt{|D|}}. \tag{4.25}$$

Постоянная $g=\frac{2^{\nu}\cdot\pi^{n-\nu}L}{w\sqrt{|D|}}$ не зависит ни от идеального класса, ни тем более от выбора в нем представителя $\mathfrak{a}_i$. Поэтому предел отношения $\frac{T}{t}$, где T—число всех идеалов поля k, норма которых не превышает t, равен $g\cdot h$, где h—число классов поля k.

Этот факт служит исходным пунктом для определения числа классов h заданного поля. Для некоторых полей частного вида удалось получить из этого факта сравнительно легко вычисляемые формулы для числа классов, в общем же случае задача представляет большие трудности.

4. Вернемся к дедекиндовой ζ-функции. Будем соединять в один все члены ряда (4.1), соответствующие одному и тому же значению нормы $N(\mathfrak{a})$. Тогда, обозначая через $f(m)$ число идеалов, имеющих нормой число m, мы получим:

$$\zeta_k(s)=\sum_{m=1}^{\infty}f(m)\cdot m^{-s}. \tag{4.26}$$

Произведем над этим рядом так называемое абелево преобразование:

$$\begin{aligned}\zeta_k(s)&=f(1)\cdot 1^{-s}+f(2)\cdot 2^{-s}+f(3)\cdot 3^{-s}+\ldots=\\&=f(1)\,[1^{-s}-2^{-s}]+[f(1)+f(2)]\,[2^{-s}-3^{-s}]+\\&\quad+[f(1)+f(2)+f(3)]\,[3^{-s}-4^{-s}]+\ldots\end{aligned} \tag{4.27}$$

Замечая, что $T(t)=f(1)+f(2)+\ldots+f(t)$ есть как раз число идеалов поля k, норма которых не превышает числа t, получим:

$$\zeta_k(s)=\sum_{m=1}^{\infty}T(m)\,[m^{-s}-(m+1)^{-s}]. \tag{4.28}$$

Но из (4.14) следует, что числу $T(m)$ можно дать следующую асимптотическую оценку:

$$T(m)=g\cdot h\cdot m+\theta\cdot\sigma\cdot m^{1-\frac{1}{n}},$$

где σ—константа, а $|\theta|\leqq 1$. Подставим в (4.28):

$$\begin{aligned}\zeta_k(s)=g\cdot h\cdot\sum_{m=1}^{\infty}m\,[m^{-s}-(m+1)^{-s}]+\\+\theta_1\sigma\sum_{m=1}^{\infty}m^{1-\frac{1}{n}}\,[m^{-s}-(m+1)^{-s}].\end{aligned} \tag{4.29}$$

Первую из сумм правой части подвергнем обратному преобразованию:

$$\begin{aligned}gh\cdot\sum_{m=1}^{\infty}m\,[m^{-s}-(m+1)^{-s}]&=g\cdot h\,[1\,(1^{-s}-2^{-s})+2\,(2^{-s}-3^{-s})+\\&+3\,(3^{-s}-4^{-s})+\ldots]=g\cdot h\,[1^{-s}+2^{-s}+3^{-s}+\ldots]=gh\zeta(s).\end{aligned}$$

Таким образом мы пришли к римановой ζ-функции, которая в силу (3.6) может быть представлена в виде

$$g\cdot h\cdot\frac{1}{s-1}+P(s-1).$$

Аналогично преобразуем вторую сумму формулы (4.29):

$$\theta_1\sigma\sum_{m=1}^{\infty}m^{1-\frac{1}{n}}\,[m-(m+1)^{-s}]=\theta_1\sigma\sum_{m=1}^{\infty}[m^{1-\frac{1}{n}}-(m-1)^{1-\frac{1}{n}}]\,m^{-s}.$$

Для оценки выражения $m^{1-\frac{1}{n}}-(m-1)^{1-\frac{1}{n}}$ произведем ряд преобразований:

$$\begin{aligned}&m^{1-\frac{1}{n}}-(m-1)^{1-\frac{1}{n}}=\\&=\frac{m^{n-1}-(m-1)^{n-1}}{m^{\frac{(n-1)^2}{n}}+m^{\frac{(n-1)(n-2)}{n}}\cdot(m-1)^{\frac{n-1}{n}}+\ldots+(m-1)^{\frac{(n-1)^2}{n}}}.\end{aligned}$$

Уменьшим знаменатель правой части, отбросив все его члены, кроме первого, а числитель увеличим, подвергнув его следующему преобразованию:

$$\begin{aligned}m^{n-1}-(m-1)^{n-1}=[m-(m-1)]\,[m^{n-2}+m^{n-3}\cdot(m-1)+\ldots+\\+(m-1)^{n-2}]<(n-1)\,m^{n-2}.\end{aligned}$$

Итак:

$$m^{1-\frac{1}{n}}-(m-1)^{1-\frac{1}{n}}<\frac{(n-1)\,m^{n-2}}{m^{\frac{(n-1)^2}{n}}}=(n-1)\,m^{-\frac{1}{n}}.$$

Поэтому для исследуемого ряда мы получаем оценку:

$$\theta_1\sigma\sum_{m=1}^{\infty}[m^{1-\frac{1}{n}}-(m-1)^{1-\frac{1}{n}}]\,m^{-s}=\theta_2\sigma(n-1)\sum_{m=1}^{\infty}m^{-\frac{1}{n}-s}=$$

$$=\theta_2\sigma(n-1)\zeta\left(\frac{1}{n}+s\right)=P(s-1).$$

Объединяя оценку обеих сумм, мы получаем:

$$\zeta_k(s)=\frac{gh}{s-1}+P(s-1). \tag{4.30}$$

5. Логарифмируем формулу (4.2) и примем во внимание (4.30):

$$\sum_{\mathfrak{P}}\lg\left\{1-N(\mathfrak{P})^{-s}\right\}=-\lg\frac{1}{s-1}\pm P(s-1).$$

Пользуясь неравенством

$$-\lg(1+\rho)=\rho+\frac{\rho^2}{2}+\frac{\rho^3}{3}+\ldots<\rho+\frac{1}{2}(\rho^2+\rho^3+\ldots)=\rho+\frac{\rho^2}{2(1-\rho)},$$

где $0<\rho<1$, получим из этой формулы следующую:

$$\sum_{\mathfrak{P}}N(\mathfrak{P})^{-s}+\theta\sum_{\mathfrak{P}}\frac{N(\mathfrak{P})^{-2s}}{2(1-N(\mathfrak{P})^{-s})}=\lg\frac{1}{s-1}+P(s-1)$$

$$(0<\theta<1).$$

Вторая из сумм левой части сходится при $s>\frac{1}{2}$, в силу чего эту формулу можно переписать так:

$$\sum_{\mathfrak{P}}N(\mathfrak{P})^{-s}=\lg\frac{1}{s-1}+P(s-1). \tag{4.31}$$

Разобьем сумму левой части на две, относя к первой члены содержащие простые идеалы первой степени, а ко второй сумме остальные простые идеалы. Собирая в один член члены, содержащие простые идеалы с одной и той же нормой, мы получим из первой суммы $\sum_p \nu_p\cdot p^{-s}$, где суммирование распространено на все простые числа, а ν_p — числа простых идеальных множителей первой степени простого числа p. С другой стороны, во второй сумме $N(\mathfrak{P})\geqq p^2$, $N(\mathfrak{P})^{-s}\leqq p^{-2s}$, и число членов, содержащих одно и то же p, не превышает $\frac{n}{2}$, в силу чего величина второй суммы $\leqq\frac{n}{2}\sum p^{-2s}$, а этот ряд сходится при $s>\frac{1}{2}$ и потому может быть включен в $P(s-1)$. Таким образом мы приходим к следующему фундаментальному результату Кронекера:

$$\sum_p \nu_p p^{-s}=\lg\frac{1}{s-1}+P(s-1). \tag{4.32}$$

6. Рассмотрим тот частный случай, когда поле k нормально. Тогда все простые числа распадаются внутри k на простые идеалы одной и той же степени. В частности, если p содержит простые идеальные множители первой степени, то таковыми будут все его множители, и число их равно n. Группы разложения этих простых идеалов суть единичные группы, и мы получаем:

$$\sum_p p^{-s}=\frac{1}{n}\lg\frac{1}{s-1}+P(s-1), \tag{4.33}$$

где сумма левой части распространена на все простые числа, принадлежащие к классу единичной подстановки (см. главу I, § 10.2).

7. Теперь мы имеем возможность закончить доказательство теоремы Дирихле об арифметических прогрессиях (§ 3, теорема 40). Пусть задана прогрессия $ax+k$, $(a,k)=1$. Рассмотрим поле a-ых степеней из единицы. Это нормальное поле степени $\varphi(a)$. Из главы I, § 12.1 мы знаем, что простое число p принадлежит в поле к единичной подстановке тогда и только тогда, если оно удовлетворяет сравнению

$$p\equiv 1\,(\mathrm{mod}\,a),$$

т. е. лежит в прогрессии $ax+1$. Таким образом формула (4.33) приобретает для этого случая вид:

$$\sum_{p\equiv 1\,(\mathrm{mod}\,a)}p^{-s}=\frac{1}{\varphi(a)}\lg\frac{1}{s-1}+P(s-1). \tag{4.34}$$

Теперь, обращаясь (к § 3.7), мы видим, что формула (4.34) есть не что иное, как формула (3.33), доказанная *со знаком равенства*. Из рассуждений § 3.7 следует, что этим доказан факт, достаточный для доказательства теоремы 40 и принятый на веру в § 3. Действительно, из этого вытекает необращение в нуль $L(s,\chi)$ при $s=1$, что было нами принято в § 3.9.

Если простой идеал критический, т. е. если он является кратным множителем соответствующего простого числа, то он

будет входить в формулы (4.32), (4.33), (4.34) иначе. Мы просто откинем соответствующие им члены в левых частях этих формул. Этих членов конечное число, а потому их отбрасывание не повлияет на вид правых частей.

§ 5. Распределение простых чисел по отделам подстановок

1. В главе I, § 10.2 мы определили автоморфизм (подстановку) $\sigma=\left[\frac{K}{\mathfrak{P}}\right]$ нормального K, к которому *принадлежит* некритический простой идеал, при помощи сравнения

$$\alpha^{\sigma} \equiv \alpha^{p} (\mathrm{mod}\, \mathfrak{P}), \tag{5.1}$$

имеющего место для всех целых чисел α поля K. Степени этого автоморфизма составляют группу разложения простого идеала $\mathfrak{P}$, степень которого равна порядку подстановки σ.

Простые идеальные множители простого числа p принадлежат к сопряженным автоморфизмам, составляющим класс автоморфизмов. Мы условились обозначать этот класс символом $\left(\frac{K}{p}\right)$ и говорить, что простое число p принадлежит к классу $\left(\frac{K}{p}\right)$. Возникает вопрос о существовании и плотности (см. § 3.10) простых чисел, принадлежащих к заданному классу автоморфизмов группы Галуа $\mathfrak{G}$ поля K.

2. В этом параграфе мы докажем существование и определим плотность множества простых чисел, принадлежащих к ***отделу автоморфизмов*** группы $\mathfrak{G}$, т. е. к совокупности степеней автоморфизма σ, взаимно простых с ее порядком, а также сопряженных с ними автоморфизмов. Эта задача была решена Фробениусом (Frobenius).

Для ее решения мы будем постоянно применять формулу (4.32):

$$\sum_{p} \nu_p \cdot p^{-s} = \lg \frac{1}{s-1} + P(s-1) \tag{5.2}$$

к различным делителям поля K. Пусть σ — произвольно выбранный автоморфизм группы $\mathfrak{G}$, f—его порядок, тогда

$$\mathfrak{Z}=1+\sigma+\sigma^2+\ldots+\sigma^{f-1}$$

образованная им циклическая группа. В главе I, § 10, мы видели, что степень простого идеального множителя $\mathfrak{P}$ числа p, который содержит заданный простой идеал $\mathfrak{P}$ поля K и находится в делителе k поля K, принадлежащем к какой-нибудь группе $\mathfrak{H}$, равна числу смежных классов $\mathfrak{H}S$, содержащихся в комплексе $\mathfrak{H}\mathfrak{Z}$, где $\mathfrak{Z}$ — группа разложения идеала $\mathfrak{P}$. Чтобы эта степень

была равна единице, необходимо и достаточно, чтобы $\mathfrak{Z}$ входила в $\mathfrak{H}$.

Точно так же, для того чтобы степень простого идеала поля k, соответствующего комплексу $\mathfrak{H}S\mathfrak{Z}$, была равна единице, необходимо и достаточно, чтобы $S^{-1}\mathfrak{Z}S$ входила в $\mathfrak{H}$. Таким образом, чтобы определить число простых идеальных множителей простого числа p внутри k, надо разложить $\mathfrak{G}$ на комплексы по делителям $\mathfrak{H}$ и $\mathfrak{Z}$:

$$\mathfrak{G}=\mathfrak{H}\mathfrak{Z}+\mathfrak{H}S_2\mathfrak{Z}+\ldots+\mathfrak{H}S_a\mathfrak{Z},$$

и подсчитать, сколько из автоморфизмов

$$\sigma, S_2\sigma S_2^{-1}, \ldots, S_a\sigma S_a^{-1}$$

входит в $\mathfrak{H}$.

Возьмем в качестве $\mathfrak{H}$ группу $\mathfrak{Z}$, образованную степенями автоморфизма σ порядка f, а в качестве $\mathfrak{T}$—ее делитель порядка d, образованный подстановкой $\tau=\sigma^{\frac{f}{d}}$. Если $S_i\tau S_i^{-1}$ лежит в $\mathfrak{Z}$, то, имея порядок d, она будет лежать и в $\mathfrak{T}$, а потому S_i лежит в нормализаторе $\mathfrak{N}$ группы $\mathfrak{T}$ (в который должен входить в $\mathfrak{Z}$). Поэтому достаточно сосчитать число комплексов $\mathfrak{Z}S_i\mathfrak{T}$, входящих в $\mathfrak{N}$. Но так как $\mathfrak{T}$ является нормальным делителем $\mathfrak{N}$, то в силу $S_i\mathfrak{T}=\mathfrak{T}S_i$ и $\mathfrak{Z}\mathfrak{T}=\mathfrak{Z}$ каждый такой комплекс превращается в смежный класс $\mathfrak{Z}S_i$, и дело приводится к подсчету смежных классов в разложении $\mathfrak{N}=\mathfrak{Z}+\mathfrak{Z}S_2+\mathfrak{Z}S_3+\ldots$, т. е. определению индекса $(\mathfrak{N}:\mathfrak{Z})=\mathrm{Ord}\,\mathfrak{N}:f$.

Обозначим через n_d число автоморфизмов, входящих в класс τ и через k_d—число классов τ, входящих в отдел τ.

Обозначим через $\mathfrak{N}_1$ нормализатор автоморфизма τ. Тогда число различных автоморфизмов в классе τ равно индексу $\mathfrak{N}_1$, относительно $\mathfrak{G}$ (см. часть I, стр. 140, конец доказательства теоремы 75), откуда

$$\mathrm{Ord}\,\mathfrak{N}_1=\frac{n}{n_d}.$$

Остается определить индекс $(\mathfrak{N}:\mathfrak{N}_1)$. Если мы разложим $\mathfrak{N}$ на смежные классы по $\mathfrak{N}_1$:

$$\mathfrak{N}=\mathfrak{N}_1+\mathfrak{N}_1S_2+\ldots+\mathfrak{N}_1S_u,$$

то каждый из этих смежных классов переведет τ в степень τ, и все они будут отличны друг от друга. Поэтому, если мы рассмотрим классы, образованные всеми $\varphi(d)$ примитивными степенями автоморфизма τ (они образуют отдел автоморфизма τ), то по u классов среди этих $\varphi(d)$ классов окажутся совпадаю-

щими, и в отдел войдет всего $\frac{\varphi(d)}{u}$ различных классов, т. е. $k_d = \frac{\varphi(d)}{u}$, или

$$(\mathfrak{N} : \mathfrak{N}_1) = u = \frac{\varphi(d)}{k_d}.$$

Таким образом, если p принадлежит к одному из классов отдела τ, то внутри поля k, принадлежащего к $\mathfrak{Z}$, содержится ровно

$$\operatorname{Ord}\mathfrak{N} : f = (\mathfrak{N} : \mathfrak{N}_1) \cdot \operatorname{Ord}\mathfrak{N}_1 : f = \frac{\varphi(d) \cdot n}{k_d n_d \cdot f} \tag{5.4}$$

различных простых идеальных делителей числа p первой степени.

Применим к рассматриваемому полю k формулу (5.2). Для того, чтобы простое число p в разложении внутри k содержало простые идеальные множители первой степени, необходимо, чтобы класс автоморфизмов, к которому оно принадлежит внутри K, содержал автоморфизмы из $\mathfrak{Z}$. Другими словами, p должно принадлежать к одному из классов, образованных элементами группы $\mathfrak{Z}$. Эти классы образуют несколько отделов, каждый из которых вполне определяется порядком d автоморфизма $\tau = \sigma^{\frac{f}{d}}$, который в нем содержится. Поэтому, разбивая сумму левой части (5.2) на частичные суммы, соответственно названным отделам, мы в силу (5.4) перепишем формулу (5.2) так:

$$\sum_{d|f} \frac{\varphi(d) \cdot n}{k_d \cdot n_d f} \sum_{p_d} p_d^{-s} = \lg \frac{1}{s-1} + P(s-1), \tag{5.5}$$

где под p_d мы разумеем все простые числа, принадлежащие к отделу автоморфизма $\sigma^{\frac{f}{d}}$.

Беря в роли f любой делитель δ числа f (и соответственно в роли $\sigma - \sigma^{\frac{f}{\delta}}$, мы получим вместо (5.5):

$$\sum_{d|\delta} \frac{\varphi(d)}{k_d n_d} \sum_{p_d} p_d^{-s} = \frac{\delta}{n} \cdot \lg \frac{1}{s-1} + P(s-1). \tag{5.6}$$

Введем в рассмотрение числовую функцию $\mu(n)$ Мёбиуса (Möbius), определяя ее значения следующим образом:

$\mu(1) = 1$;
$\mu(n) = 0$, если n содержит кратные простые множители;
$\mu(n) = +1$ (или -1), если n содержит четное (или нечетное) число различных простых множителей.

Мы воспользуемся следующими свойствами функции $\mu(n)$:

I. $$\sum_{d|n} \mu(d) = 0 \qquad \text{при } n > 1.$$

В самом деле, пусть $n = p_1 p_2 \dots p_r$. Разобьем все делители числа n на 0-ую, 1-ую, ..., r-ую категории, в зависимости от числа простых множителей, которые эти делители содержат. Сумма $\Sigma\mu(d)$, распространенная на делители j-ой категории, равна $(-1)^j$, умноженной на число членов, т. е. $C_r^j(-1)^j$, где C_r^j — биномиальный коэфициент. Отсюда

$$\sum_{d|n} \mu(d) = 1 - C_r^1 + C_r^2 - \dots + C_r^j(-1)^j + \dots$$

$$\dots + (-1)^r = (1-1)^r = 0$$

II. $$\sum_{d|n} \mu\left(\frac{n}{d}\right) d = \varphi(n).$$

В справедливости этой формулы легко убедиться из формулы (2.4) (часть I, стр. 202).

Умножим (5.6) на $\mu\left(\frac{f}{\delta}\right)$ и просуммируем по всем $\delta|f$:

$$\sum_{\delta|f} \mu\left(\frac{f}{\delta}\right) \sum_{\delta|f} \frac{\varphi(d)}{k_d \cdot n_d} \sum_{p_d} p_d^{-s} =$$

$$= \frac{1}{n} \sum_{\delta|f} \mu\left(\frac{f}{\delta}\right) \cdot \delta \cdot \lg \frac{1}{s-1} + P(s-1).$$

Сумма в правой части в силу II дает $\varphi(f)$. В левой части переставим оба внешние знака суммы. При заданном d число $\frac{f}{\delta}$ в силу $d|\delta$ должно пробегать все делители числа $\frac{f}{d}$, в силу чего $\sum_{\frac{f}{\delta}\left|\frac{f}{d}\right.} \mu\left(\frac{f}{\delta}\right) = 0$ при $f > d$ и $= 1$ при $f = d$. В силу этого наша формула примет вид

$$\frac{\varphi(f)}{k_f \cdot n_f} \sum_{p_f} p_f^{-s} = \frac{\varphi(f)}{n} \lg \frac{1}{s-1} + P(s-1),$$

откуда окончательно:

$$\sum_{p_f} p_f^{-s} = \frac{k_f \cdot n_f}{n} \lg \frac{1}{s-1} + P(s-1). \qquad (5.7)$$

Эта формула выражает „закон плотности" Фробениуса:

Теорема 41. Существует бесчисленное множество простых чисел, принадлежащих к одному из классов отдела, образованного произвольно заданным автоморфизмом группы Галуа нормального поля. Плотность этой совокупности простых чисел равна частному отделения числа $k_f n_f$ автоморфизмов, содержащихся в этом отделе, на общее число автоморфизмов группы.

Существует такая же теорема относительно плотности простых чисел, принадлежащих к отдельным классам. Мы докажем ее в следующем параграфе.

3. Простым следствием этого результата является

Теорема 42. Существует бесчисленное множество таких простых чисел p, что заданный полином $f(x)$, группа Галуа которого содержит подстановку из циклов порядков $n_1, n_2, \ldots, n_k$, разлагается по модулю p на неприводимые по модулю p множители степеней $n_1, n_2, \ldots, n_k$.

Доказательство. Пусть K—поле, образованное корнями этого полинома. Заданной подстановке группы Галуа уравнения $f(x)=0$ соответствует вполне определенный автоморфизм группы Галуа поля K, и обратно. Отделу автоморфизма соответствует совокупность подстановок, состоящих из циклов тех же порядков $n_1, n_2, \ldots, n_k$. В силу теоремы 41 существует бесчисленное множество простых чисел, принадлежащих к одному из классов этого отдела. Пусть p будет одно из них, притом не входящее в дискриминант уравнения $f(x)=0$. Из главы I, § 10.3, мы убеждаемся, что полином $f(x)$ разлагается по модулю p на неприводимые по модулю p полиномы степеней $n_1, n_2, \ldots, n_k$, ч. и т. д.

4. Если два нормальных поля K_1 и K_2 имеют группы Галуа $\mathfrak{G}_1, \mathfrak{G}_2$, то по их поведению относительно всех простых чисел, как модулей, можно судить об их тождественности, родственности или взаимной простоте. Для этого рассмотрим их композит K. Пусть его группа будет $\mathfrak{K}$. Пусть внутри K поля K_1 и K_2 принадлежат соответственно к группам $\mathfrak{H}_1$ и $\mathfrak{H}_2$. Дополнительные группы $\mathfrak{K}/\mathfrak{H}_1$, $\mathfrak{K}/\mathfrak{H}_2$ изоморфны с $\mathfrak{G}_1, \mathfrak{G}_2$. Обе группы $\mathfrak{H}_1$, $\mathfrak{H}_2$ взаимно просты, так как в силу части I, стр. 91, теоремы 60, к их пересечению принадлежит композит полей K_1 и K_2, т. е. K. Пересечение K полей K_1 и K_2 принадлежит к композиту $\bar{\mathfrak{H}}$

групп $\mathfrak{H}_1$, $\mathfrak{H}_2$. Из того, что K_1 и K_2 нормальные поля, следует, что $\mathfrak{H}_1$ и $\mathfrak{H}_2$ суть нормальные делители группы $\mathfrak{K}$, в силу чего их элементы перестановочны (см. часть I, стр. 37, теорема 24). Таким образом

$$\bar{\mathfrak{H}} = \mathfrak{H}_1 \times \mathfrak{H}_2. \qquad (5.8)$$

Разложим $\mathfrak{K}$ на смежные классы по $\bar{\mathfrak{H}}$:

$$\mathfrak{K} = \bar{\mathfrak{H}} + \bar{\mathfrak{H}} S_2 + \ldots + \bar{\mathfrak{H}} S_a. \qquad (5.9)$$

Сопоставим с элементами этой группы элементы гомоморфной с ней группы $\frac{\mathfrak{K}}{\mathfrak{H}_1} = \mathfrak{G}_1$. Принимая во внимание, что в силу (5.8)

$$\frac{\bar{\mathfrak{H}}}{\mathfrak{H}_1} = \bar{\mathfrak{H}}_1'$$

изоморфно с $\mathfrak{H}_2$, мы будем иметь

$$\mathfrak{G}_1 = \bar{\mathfrak{H}}_1 + \bar{\mathfrak{H}}_1' S_2' + \ldots + \bar{\mathfrak{H}}_1' S_u', \qquad (5.10)$$

и аналогично для $\mathfrak{G}_2$:

$$\mathfrak{G}_2 = \bar{\mathfrak{H}}_2 + \bar{\mathfrak{H}}_2 S_2'' + \ldots + \bar{\mathfrak{H}}_2' S_u. \qquad (5.11)$$

Зададимся следующим вопросом: задано по автоморфизму в группах $\mathfrak{G}_1$ и $\mathfrak{G}_2$ полей K_1 и K_2. Существует ли в поле K такой автоморфизм, который, будучи применен к величинам из полей K_1 и K_2, произведет среди них заданные автоморфизмы? Для решения этого вопроса выясним, лежат ли заданные автоморфизмы в смежных классах разложений (5.10) и (5.11) с одинаковыми номерами или с разными. Если с разными, то вопрос решается в отрицательном смысле. В самом деле, автоморфизм поля K, лежащий в смежном классе $\bar{\mathfrak{H}} S_i$, вызывает среди величин полей K_1 и K_2 автоморфизмы, лежащие соответственно в смежных классах $\bar{\mathfrak{H}}_1' S_2'$ и $\bar{\mathfrak{H}}_2'' S_i''$. С другой стороны, если заданные автоморфизмы лежат в смежных классах с одинаковыми номерами, например, представляются в виде $T' S_i'$ и $T'' S_i''$, где T', T'' — автоморфизмы группы $\bar{\mathfrak{H}}_1'$ и $\bar{\mathfrak{H}}_2'$, то вопрос решается в положительном смысле. В самом деле, в силу изоморфизмов $\mathfrak{H}_1 \sim \bar{\mathfrak{H}}_1'$ и $\mathfrak{H}_2 \sim \bar{\mathfrak{H}}_2'$ можно найти в группах $\mathfrak{H}_1$ и $\mathfrak{H}_2$ автоморфизмы T_1, T_2, соответствующие соответственно T' и T''. Тогда автоморфизм T_2 оставит величины поля K_1 на местах, а над величинами поля K_2 произведет автоморфизм T''; точно также автоморфизм T_1 оставит величины поля K_2 на местах, а над величинами поля произведет автоморфизм T_1. Из этого следует, что автоморфизм $T_1 T_2 S_i$ удовлетворяет поставленным требованиям.

5. Пусть в полях K_1 и K_2 задано по отделу автоморфизмов. Требуется выснить, существуют ли простые числа p, принадлежащие к заданным отделам одновременно в обоих полях K_1 и K_2. Для решения этого вопроса узнаем, существует ли внутри

этих отделов по автоморфизму, лежащему в смежных классах с одинаковыми номерами в разложениях (5.10) и (5.11). В этом случае, как мы видели, можно найти автоморфизм S поля K, производящий над величинами полей K_1, K_2 эти автоморфизмы. Всем автоморфизмам отдела, образованного автоморфизмом S, будут внутри K_1 и K_2 соответствовать заданные отделы. Тогда, найдя простое число p, принадлежащее внутри K к отделу автоморфизма S (в силу теоремы 41 это всегда возможно), мы удовлетворим условиям поставленной задачи.

Разберем могущие здесь встретиться частные случаи.

I. Если K_2 есть делитель K_1, то $K=K_1$. Здесь для каждого автоморфизма поля K_1 мы получим вполне определенный автоморфизм поля K_2. В частности, если p принадлежит внутри K_1 к тождественному автоморфизму, то и внутри K_2 оно должно принадлежать к тождественному автоморфизму.

II. Если K_2 не входит делителем в K_1, то K_1 является настоящим делителем K. $\mathfrak{H}_1$ отлична от единичной группы. Простое число p, принадлежа внутри K к отделу автоморфизма, лежащего в $\mathfrak{H}_1$ и отличного от тождественного (и потому в силу взаимной простоты $\mathfrak{H}_1$, $\mathfrak{H}_2$ не лежащего в $\mathfrak{H}_2$) внутри K_1 принадлежит к тождественному автоморфизму, а внутри K_2 — к автоморфизму отличному от тождественного. Это позволяет нам высказать следующую теорему:

Теорема 43. Если заданы два нормальных поля K_1, K_2, то для того, чтобы K_2 было делителем K_1, необходимо и достаточно, чтобы всякое простое число p, разлагающееся внутри K_1 на простые идеалы первой степени, разлагалось и внутри K_2 на простые идеалы первой степени.

В частности, поля K_1 и K_2 совпадают тогда и только тогда, если совпадают множества простых чисел, разлагающихся внутри K_1 и соответственно внутри K_2 на простые идеалы первой степени.

Эта теорема была впервые доказана Бауэром (M. Bauer). Б. Н. Делоне применил ее к доказательству теоремы Кронекера-Вебера об абелевых полях.

III. Поля K_1 и K_2 взаимно просты. Тогда $\overline{\mathfrak{H}}=\mathfrak{R}=\mathfrak{H}_1\times\mathfrak{H}_2$, откуда следует, что существуют простые числа принадлежащие в каждом из полей K_1, K_2 к независимо выбранным отделам автоморфизмов. Этот результат был также получен Бауэром.

§ 6. Распределение простых чисел по классам подстановок

1. Для доказательства того, что простые числа распределяются равномерно (т. е. с одинаковой плотностью) по всем классам каждого отдела в любом алгебраическом поле, существует метод, носящий название расширения при помощи полей

деления круга. Этот метод состоит в рассмотрении полей, образованных из заданного путем присоединения к нему некоторых корней из единицы. Распределение простых чисел по классам такого поля соответствует их распределению по некоторым прогрессиям. Если мы вдобавок будем уметь находить плотность простых чисел внутри каждого отдела по прогрессиям, то рассмотрение целесообразно выбранных полей даст нам возможность решить поставленную задачу.

При проведении доказательства я буду пользоваться упрощениями, предложенными в работах М. Ф. Кравчука и Шрейера (O. Schreier).

2. Предварительно докажем несколько вспомогательных теорем.

Теорема 44. Пусть K—нормальное поле n-ой степени. Плотность множества простых чисел, принадлежащих внутри K к тождественной подстановке и одновременно лежащих в прогрессии $mx+1$, где m — произвольное целое число, равна $\frac{m_1}{\varphi(m)\cdot n}$, где m_1—степень пересечения полей K и $k\left(e^{\frac{2\pi i}{m}}\right)$.

Доказательство. Степень композита обоих полей равна $\frac{\varphi(m)\cdot n}{m_1}$. Согласно теореме Кронекера, плотность множества простых чисел, принадлежащих внутри этого композита к тождественной подстановке, равна $\frac{m_1}{\varphi(m)\cdot n}$. Но всякое простое число, принадлежащее внутри объемлющего поля к тождественной подстановке, принадлежит к ней и внутри делителей поля.

С другой стороны, композит двух делителей поля принадлежит к пересечению подгрупп, к которым принадлежат эти делители, и вместе с тем к единичной группе, так как основным полем является тот же композит. Поэтому простое число, принадлежа к единичной подстановке внутри K и $k\left(e^{\frac{2\pi i}{m}}\right)$, принадлежит внутри их композита к классу, лежащему внутри обеих подгрупп (обе они нормальны), и в силу их взаимной простоты к единичной подстановке. Таким образом равна $\frac{m_1}{\varphi(m)n}$ плотность множества простых чисел, одновременно принадлежащих к единичной подстановке внутри полей K и $k\left(e^{\frac{2\pi i}{m}}\right)$. Но в силу главы I, § 12, принадлежность простого числа к единичной подстановке внутри $k\left(e^{\frac{2\pi i}{m}}\right)$ равносильна его вхождению в прогрессию $mx+1$. Этим и доказывается справедливость теоремы.

3. Эту теорему нетрудно распространить на алгебраические поля общего типа. Пусть K_1 — произвольное алгебраическое поле, имеющее с полем $k\left(e^{\frac{2\pi i}{m_1}}\right)$ пересечение K_1 степени m_1.

Тогда композит $K_1 k$ имеет над K_1 относительную степень $f=\frac{\varphi(m)}{m_1}$. Если примитивные величины α_1 и β_1 полей K_1 и $K_1 k$ удовлетворяют уравнениям соответственно

$$f(x)=0, \quad F(y)=0,$$

то каждому корню первого уравнения соответствует f корней второго уравнения, получаемых один из другого при помощи подстановок относительной группы поля $K_1\frac{k}{K_1}$. Поэтому, если простое число p таково, что сравнение

$$f(x)\equiv 0 \pmod p \tag{6.1}$$

имеет ν_p рациональных корней, то могут встретиться два случая:

1. p есть число вида $km+1$. Тогда сравнение

$$x_m\equiv 0 \pmod p, \tag{6.2}$$

где x_m — неприводимый полином, корнем которого является $e^{\frac{2\pi i}{m}}$, имеет все рациональные корни, а потому сравнение

$$F(y)\equiv 0 \pmod p, \tag{6.3}$$

корни которого рационально выражаются через корни сравнений (6.1) и (6.2), будет иметь $f\cdot\nu_p$ рациональных корней.

2. p есть число вида $km+l$, $l\neq 1$. Тогда сравнение (6.2) не будет иметь рациональных корней. Но так как корни сравнения (6.2) рационально выражаются через корни сравнения (6.3), то последнее тоже не будет иметь рациональных корней.

С другой стороны, сравнение (6.3) имеет рациональные корни только в том случае, если это имеет место для (6.1). Поэтому формула Кронекера (4.32) для уравнения $F(y)=0$ будет иметь вид

$$\sum_p f\cdot\nu_p\cdot p^{-s}=\lg\frac{1}{s-1}+P(s-1),$$

или

$$\sum_p \nu_p\cdot p^{-s}=\frac{1}{f}\lg\frac{1}{s-1}+P(s-1), \tag{6.4}$$

где сумма в левой части распространена на простые числа p: 1) имеющие в поле K_1 простые идеальные делители первой степени и 2) удовлетворяющие сравнению

$$p\equiv 1 \pmod m. \tag{6.5}$$

Если же мы отбросим второе условие, то формула Кронекера для поля K_1 будет иметь вид

$$\sum_p \nu_p\cdot p^{-s}=\lg\frac{1}{s-1}+P(s-1). \tag{6.6}$$

В сопоставлении формул (6.4) и (6.6) и состоит обобщение теоремы 44.

3. Чтобы доказать равномерность распределения простых чисел, разлагающихся на простые идеалы первой степени, по другим прогрессиям $mx+s$, введем понятие *допустимого класса сравнений по модулю m*.

Допустимым для поля K_1 классом a сравнений по модулю m называется такой класс, что в поле K_1 существует идеал $\mathfrak{a}$, удовлетворяющий сравнению

$$N(\mathfrak{a})\equiv a \pmod m.$$

Легко понять, что допустимые классы образуют абелеву группу относительно умножения. Порядок F этой группы удовлетворяет неравенству

$$F\geqq f, \tag{6.7}$$

где $m_1=\frac{\varphi(m)}{f}$ — степень пересечения n_1 поля K_1 с $k\left(e^{\frac{2\pi i}{m}}\right)$. В самом деле, внутри поля $k\left(e^{\frac{2\pi i}{m}}\right)$ автоморфизмы поля Галуа соответствуют классам сравнений по модулю m. Пусть k_1 принадлежит к подгруппе порядка f. Выберем из нее любой автоморфизм, который пусть соответствует какому-нибудь классу сравнений a. Докажем, что этот класс допустим для k_1.

Пусть внутри $Kk\left(e^{\frac{2\pi i}{m}}\right)$ (K — норма K_1)

поле K_1 принадлежит к группе $\mathfrak{H}$

" $k\left(e^{\frac{2\pi i}{m}}\right)$ " " " $\mathfrak{K}$

" k_1 " " " $\mathfrak{K}_1$

} нормальные делители группы $\mathfrak{G}$ поля $Kk\left(e^{\frac{2\pi i}{m}}\right)$.

$\mathfrak{K}_1>\mathfrak{K}$. Группа $\frac{\mathfrak{K}_1}{\mathfrak{K}}$ изоморфна с группой допустимых классов $\mathfrak{K}$ есть композит групп $\mathfrak{K}$ и $\mathfrak{H}$. Это означает, что любой автоморфизм S группы $\mathfrak{K}_1$ может быть получен перемножением элементов из $\mathfrak{H}$ и из $\mathfrak{K}$.

Выберем простое число p, принадлежащее внутри $Kk\left(e^{\frac{2\pi i}{m}}\right)$ к отделу автоморфизма S. Один из автоморфизмов этого отдела, приложенный к величинам поля K, не меняет величин поля K_1.

в силу чего p содержит внутри K_1 простые идеальные делители первой степени. Пусть $\mathfrak{P}$ один из них. Тогда

$$N(\mathfrak{P}) = p.$$

С другой стороны, примененный к полю $e^{\frac{2\pi i}{m}}$ автоморфизм S производит любой автоморфизм группы $\frac{\mathfrak{R}_1}{\mathfrak{R}}$. Отдел же автоморфизма S производит внутри $e^{\frac{2\pi l}{m}}$ степени выбранного из $\frac{\mathfrak{R}_1}{\mathfrak{R}}$ автоморфизма, взаимно простые с f, в силу чего мы будем иметь

$$p \equiv a^t \pmod m, \quad (t, f) = 1.$$

Удовлетворяя сравнению

$$t \cdot u \equiv 1 \pmod f,$$

мы будем иметь:

$$N(\mathfrak{P}^u) = p^u \equiv a^{t \cdot u} a \equiv a \pmod m,$$

что доказывает, что класс сравнений a допустим. Таким образом существуют по крайней мере f допустимых классов сравнений, т. е. имеет место неравенство (6.7). Впоследствии мы докажем, что имеет место просто $F = f$.

4. Выделим из группы $\mathfrak{A}$ допустимых классов подгруппу $\mathfrak{A}_1$ классов, которые мы назовем *допустимыми в узком смысле*. Будем говорить, что a есть допустимый в узком смысле класс, если внутри поля K_1 существует целое число α, для которого имеет место $|N(\alpha)| \equiv a \pmod m$. Очевидно, что совокупность допустимых классов сравнений для одного идеального класса поля K_1 есть смежный класс разложения $\mathfrak{A}$ по $\mathfrak{A}_1$. Ассоциированные числа, т. е. отличающиеся множителем—единицей ε поля, лежат в одном и том же классе. В самом деле, $|N(\varepsilon)| = 1$.

5. Теперь обратимся к § 4 и построим функцию, аналогичную функции $\zeta_k(s)$, но с учетом тех классов сравнений, в которых лежат целые числа поля. Если $\omega_0, \omega_1, \ldots, \omega_{n-1}$ есть фундаментальный базис поля K_1, и $c_0, c_1, \ldots, c_{n-1}$ (целые рациональные)—координаты целого числа

$$\alpha = c_0\omega_0 + c_1\omega_1 + \ldots + c_{n-1}\omega_{n-1},$$

то для двух чисел α, α' сравнение

$$\alpha \equiv \alpha' \pmod m$$

имеет место тогда и только тогда, если для их координат имеет место

$$c_i \equiv c_i' \pmod m \qquad (i = 0,1, \ldots, n-1).$$

Обозначим через v число несравнимых по модулю m чисел поля, удовлетворяющих условию

$$|N(\alpha)| \equiv 1 \pmod m; \tag{6.8}$$

пусть $\alpha_1, \alpha_2, \ldots, \alpha_v$ будут представители таких чисел. Если a есть любой допустимый в узком смысле класс, то сравнение

$$|N(\alpha)| \equiv a \pmod m \tag{6.9}$$

будет тоже иметь v несравнимых между собой решений, которые можно получить, умножая одно из решений сравнения (6.9) на все решения сравнения (6.8).

Если мы таким образом выделим в каждом допустимом классе по v фиксированных решений и обозначим через F_1 число допустимых (в узком смысле) классов, то всякое взаимно простое с m число поля K_1 может быть представлено в форме

$$\beta + (x_0\omega_0 + x_1\omega_1 + \ldots + x_{n-1}\omega_{n-1})m, \tag{6.10}$$

где β — один из выбранных нами $F_1 v$ представителей.

6. Выберем какого-нибудь определенного представителя β и рассмотрим сумму

$$\sum_{\alpha} |N(\alpha)|^{-s}, \tag{6.11}$$

где α пробегают всевозможные числа типа (6.10), причем от ассоциированных друг с другом чисел α мы будем брать по одному представителю. Для этого будем поступать так же, как мы это делали в § 4.2. Только вместо неравенства (4.4) мы получим

$$|N[\beta + (x_0\omega_0 + x_1\omega_1 + \ldots + x_{n-1}\omega_{n-1})m]| \leqq t,$$

или

$$\left|N\left[\frac{\beta}{m} + x_0\omega_0 + x_1\omega_1 + \ldots + x_{n-1}\omega_{n-1}\right]\right| \leqq \frac{t}{m^n}. \tag{6.12}$$

Неравенства же (4.7) будут в силу своей однородности нулевого измерения иметь тот же вид.

Полагая в этих неравенствах

$$x_i = y_i \sqrt[n]{\tau}, \qquad (i = 0,1, \ldots, n-1), \tag{6.13}$$

где

$$\tau = \frac{t}{m^n},$$

мы приведем неравенства, подобные (4.4) и (4.7), к виду

$$\left|N\left(\frac{\beta}{\tau} + y_0\omega_0 + y_1\omega_1 + \ldots + y_{n-1}\omega_{n-1}\right)\right| \leqq 1 \tag{6.14}$$

$$0 \leqq \xi_i\left(\frac{\beta}{\tau} + y_0\omega_0 + \ldots + y_{n-1}\omega_{n-1}\right) < 1. \tag{6.15}$$

Увеличивая t до бесконечности, мы для оценки искомого предела $\lim_{t\to\infty}\frac{T_i}{t}$ получим то же выражение (4.25), с тою разницей, что здесь

$$\frac{T}{t}=\frac{1}{m^n}\frac{T_i}{\tau},$$

в силу чего искомое выражение получается в m^n раз меньше.

$$\lim_{t\to\infty}\frac{T_i}{t}=\frac{1}{m^n}\cdot\frac{2^{\nu}\pi^{n-\nu}\cdot L}{w\cdot\sqrt{|D|}}=\frac{1}{m^n}\cdot g. \tag{6.16}$$

Кроме того, мы здесь будем иметь член $\frac{\beta}{\tau}$, выражающий, что начало отсчета в решетке сдвинуто. Но так как этот член с возрастанием t стремится к нулю, то на величину объема он не оказывает влияния.

Суммируя левую часть по всем v решениям сравнения (6.9), мы получим для

$$\sum T_i=T^{(s)}$$

значение

$$\lim_{t\to\infty}\frac{T^{(s)}}{t}=\frac{v}{m^n}\cdot g, \tag{6.17}$$

не зависящее от выбора допустимого класса a.

Точно так же для определения выражения (6.17), соответствующего любому идеальному классу поля K_1, мы выбираем базис числа $\mathfrak{a}$, лежащего в обратном идеальном классе (см. § 4.2), и получаем то же выражение (6.17). В силу этого (см. § 4.4) каждая сумма $\sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$, распространенная на идеалы определенного идеального класса и определенного допустимого класса сравнений, имеет следующее выражение:

$$\sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}=\frac{v}{m^n}\cdot g\cdot\frac{1}{s-1}+P(s-1). \tag{6.18}$$

7. Мы уже видели, что каждому идеальному классу соответствует определенный смежный класс $A_1 a$, в котором лежат нормы его идеалов. Идеальные классы, у которых нормы идеалов лежат в A_1, составляют группу H_1, так как, если нормы идеалов $\mathfrak{a}$ и $\mathfrak{b}$, принадлежащие к идеальным классам A и B, лежат в группе H_1, то это же имеет место и для произведения $\mathfrak{ab}$. Пусть порядок этой подгруппы идеальных классов будет h_1. Тогда идеальные классы, у которых нормы идеалов лежат в $A_1 a$, составляют смежный класс разложения группы идеальных

классов по H_1, а потому число таких идеальных классов тоже равно h_1. Если поэтому мы объединим суммы (6.18), распространенные на идеалы всевозможных идеальных классов, но нормы которых будут лежать в определенном классе сравнений, то каждая такая сумма будет иметь выражение

$$\sum_{\mathfrak{a}} (N\mathfrak{a})^{-s}=\frac{h_1 v}{m^n}\cdot g\frac{1}{s-1}+P(s-1). \tag{6.19}$$

Различных сумм такого рода всего будет F.

8. Рассмотрим для группы A систему характеров (см. § 3.4) и введем обозначение $\chi(\mathfrak{a})$ для характера класса сравнения, в котором лежит норма идеала $\mathfrak{a}$. Умножая каждую сумму (6.19) на соответствующий характер и складывая, мы в силу (3,18) получим:

$$\sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}=F\cdot\frac{h_1 v}{m^n}\cdot g\frac{1}{s-1}+P(s-1) \tag{6.20}$$

$$\sum_{\mathfrak{a}}\chi(\mathfrak{a})\,N(\mathfrak{a})^{-s}=P(s-1), \tag{6.21}$$

где суммы распространены на все взаимно простые с m идеалы поля K_1, а $\chi(\mathfrak{a})$ в формуле (6.21) обозначает не главный характер.

Рассуждая так же, как при получении формул (3.29), мы получим:

$$\Re\Big\{\sum_{\mathfrak{P}}\chi(\mathfrak{P})\cdot N(\mathfrak{P})^{-s}\Big\}\leqq P(s-1) \tag{6.22}$$

$$\sum_{\mathfrak{P}} N(\mathfrak{P})^{-s}=\lg\frac{1}{s-1}+P(s-1), \tag{6.23}$$

где суммы распространяются на все простые идеалы поля K_1, за исключением конечного числа делителей числа m. Обозначая через $\mathfrak{P}_i$ простые идеалы, нормы которых лежат в классе сравнений a_i, мы сможем переписать формулы (6.22) и (6.23) так:

$$\Re\Big\{\chi(\mathfrak{P}_1)\sum N(\mathfrak{P}_1)^{-s}+\chi(\mathfrak{P}_2)\sum N(\mathfrak{P}_2)^{-s}+\ldots+\chi(\mathfrak{P}_F)\sum N(\mathfrak{P}_F)^{-s}\Big\}\leqq$$
$$\leqq P(s-1), \tag{6.24}$$

$$\sum N(\mathfrak{P}_1)^{-s}+\sum N(\mathfrak{P}_2)^{-s}+\ldots+\sum N(\mathfrak{P}_F)^{-s}=\lg\frac{1}{s-1}+$$
$$+P(s-1). \tag{6.25}$$

Принимая же во внимание, что в каждой сумме все члены, соответствующие простым идеалам выше первой степени, дают вместе $P(s-1)$ и что каждое простое число p представлено в суммах такое число ν_p раз, сколько простых идеалов первой

степени оно содержит (см. 4.4), мы представим формулы (6.21), (6.25) в следующем виде:

$$\Re\left\{\chi(a_1)\sum \nu_p p_1^{-s}+\chi(a_2)\sum \nu_p p_2^{-s}+\ldots+\right.$$
$$\left.+\chi(a_F)\sum \nu_p p_F^{-s}\right\}\leqq P(a-1) \tag{6.26}$$

$$\sum \nu_p p_1^{-s}+\sum \nu_p p_2^{-s}+\ldots+\sum \nu_p p_F^{-s}=$$
$$=\lg\frac{1}{s-1}+P(s-1). \tag{6.27}$$

Суммируя (6.26) и (6.27) почленно по всем характерам и принимая во внимание (3.20), мы получим после деления на F

$$\sum \nu_p p_1^{-s}\leqq\frac{1}{F}\lg\frac{1}{s-1}+P(s-1). \tag{6.28}$$

В этой формуле знак *равенства* может иметь место только в том случае, если он имеет место во *всех* формулах (6.26) (см. § 3.7). Но, с другой стороны, обращаясь к формуле (6.4), мы убеждаемся, что ее левая часть совпадает с левой частью формулы (6.28); отсюда следует:

$$\frac{1}{f}\lg\frac{1}{s-1}+P(s-1)\leqq\frac{1}{F}\lg\frac{1}{s-1}+P(s-1),$$

т. е.

$$f\geqq F.$$

Сравнивая с (6.7), получаем:

$$F=f. \tag{6.29}$$

Далее, формула (6.4) дает

$$\sum \nu_p p_1^{-s}=\frac{1}{F}\lg\frac{1}{s-1}+P(s-1),$$

а это есть не что иное, как формула (6.28) со знаком равенства.

Поэтому во всех формулах (6.26) должен иметь место знак равенства. Рассуждая так же, как в § 4.6, мы получим

$$\sum \nu_p p_i^{-s}=\frac{1}{f}\lg\frac{1}{s-1}+P(s-1),\qquad (i=1,2,\ldots,f), \tag{6.30}$$

т, е. получаем, что *простые идеалы первой степени любого алгебраического поля равномерно распределяются по всем допустимым классам сравнений.*

9. Пусть K — нормальное поле, $\mathfrak{G}$ — его группа Галуа порядка n, S — ее автоморфизм порядка f. Чтобы определить плотность

множества простых чисел, принадлежащих к классу автоморфизма S, выберем простое число p, удовлетворяющее условию

$$p=f^u\cdot v+1,$$

где u — некоторый весьма большой показатель, и рассмотрим поле $k_p=k\left(e^{\frac{2\pi i}{p}}\right)$. Это поле имеет циклическую группу Галуа порядка $p-1=f^u\cdot v$, которую мы обозначим через $\mathfrak{U}$.

Группа композита Kk_p изоморфна с прямым произведением

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

Выберем внутри $\mathfrak{U}$ произвольный автоморфизм $\mathfrak{U}$, ограничив его лишь условием, что его порядок ω делился на f. Для каждого ω будет существовать $\varphi(\omega)$ таких автоморфизмов. Рассмотрим автоморфизм SU группы $\mathfrak{R}$, образованную им циклическую группу $\mathfrak{Z}$ и принадлежащее к последней внутри Kk_p поле K_1. Если класс S состоит из n_f автоморфизмов группы $\mathfrak{G}$:

$$S_i\qquad (i=0,1,\ldots,n_f-1)$$

среди которых могут встречаться и степени автоморфизма S), а отдел S состоит из k_f классов

$$S_i,\ S_i^{\alpha},\ S_i^{\alpha'},\ \ldots,$$

то внутри группы $\mathfrak{R}$ класс SU будет состоять из n_f автоморфизмов

$$S_iU,\qquad (i=0,1\ldots,n_f-1), \tag{6.31}$$

а отдел SU — из $\varphi(\omega)$ классов

$$S_iU,\ S_i^{\beta}U^{\beta},\ S_i^{\beta'}U^{\beta'},\ \ldots, \tag{6.32}$$

где числа β, β', ... будут пробегать все взаимно простые с ω вычеты по модулю ω. В формуле (4.32) для поля $\tilde{K}_1$

$$\sum_p \nu_p p^{-s}=\lg\frac{1}{s-1}+P(s-1), \tag{6.33}$$

где сумма распространена на простые числа, принадлежащие к различным степеням класса S_iU. Стоящий в такой степени $S_i^{\alpha}U^{\alpha}$ множитель U^{α} указывает, в каком классе сравнений лежит принадлежащее к классу $S_i^{\alpha}U^{\alpha}$ простое число p. Для поля K_1 допустимые классы сравнений соответствуют степеням U, U^2, ..., U^{ω}, а потому их число равно ω, и если мы распространим

сумму на один из таких классов сравнений, то в силу (6.30) получим:

$$\sum \nu_p p^{-s} = \frac{1}{\omega} \lg \frac{1}{s-1} + P(s-1). \tag{6.34}$$

Если мы выберем в качестве U^α такую степень, что $(\alpha, \omega)=1$, т.е. что U^α тоже имеет порядок ω, то этим выбором мы указываем, что p принадлежит к отделу $S_i U$. Более того, так как все множители U^β в выражениях (6.32) различны, то мы выбором α однозначно определяем класс автоморфизмов, к которому могут принадлежать простые числа, входящие в сумму (6.34), так что сумма (6.34) может быть преобразована к следующему виду, получаемому из формулы (5.5), если мы положим в ней

$$\begin{gathered} \varphi(d) \longrightarrow \varphi(\omega), \\ n \longrightarrow n f^u v, \\ k_d \longrightarrow \varphi(\omega), \\ n_d \longrightarrow n f, \\ f \longrightarrow \omega: \end{gathered}$$

$$\frac{n f^u v}{n_f \omega} \sum_{p_f} p_f^{-s} = \frac{1}{\omega} \lg \frac{1}{s-1} + P(s-1), \tag{6.35}$$

так как остальные суммы в левой части (5.5) не будут содержать никаких членов p_d^{-s}. В левой части (6.35) сумма распространена на p_f, принадлежащие к определенному классу S_i^α внутри K и одновременно лежащие в определенном классе сравнений U^α по модулю p. Формулу (6.35) можно также переписать так:

$$\sum_{p_f} p_f^{-s} = \frac{n_f}{n f^u v} \lg \frac{1}{s-1} + P(s-1). \tag{6.36}$$

В частности, возьмем $\alpha=1$.

Если мы фиксируем класс S_i и заставим U пробегать все автоморфизмы группы $\mathfrak{U}$, порядок которых ω делится на f, то получим $\geqq f^u v - fv + 1$ формул, подобных (6.36), в которых суммы распространены на простые числа, принадлежащие к одному и тому же классу S_i автоморфизмов, но лежащие в различных $f^u v - fv + 1$ классах сравнений по модулю p. Суммируя эти формулы, мы в силу независимости их правых частей от ω получим:

$$\sum_{p_f} p_f^{-s} \geqq \left(1 - \frac{fv-1}{f^u v}\right) \frac{n_f}{n} \lg \frac{1}{s-1} + P(s-1), \tag{6.37}$$

где сумма не исчерпывает всех простых чисел, принадлежащих внутри K к классу S_i. Выбирая u все больше и больше, мы будем заставлять выражение в правой части в (6.37) стремиться к единице, в силу чего, обозначая через $\underline{\lim}$ нижний предел, получим:

$$\underline{\lim_{s \to 1}} \frac{\sum p_{s_i}^{-1}}{\lg \frac{1}{s-1}} \geqq \frac{n_f}{n}. \tag{6.38}$$

Аналогичные неравенства мы получим для простых чисел, принадлежащих к каждому из k_f классов отдела S_i.

Обозначая через $\overline{\lim}$ верхний предел и через $\Sigma_1, \Sigma_2, \ldots, \Sigma_{k_f}$ суммы, соответствующие простым числам, принадлежащим к отдельным классам нашего отдела, мы будем иметь в силу (5.7):

$$\overline{\lim} \frac{\Sigma_1}{\lg \frac{1}{s-1}} \leqq \overline{\lim} \frac{\Sigma_1 + \Sigma_2 + \ldots + \Sigma_{k_f}}{\lg \frac{1}{s-1}} - \overline{\lim} \frac{\Sigma_2}{\lg \frac{1}{s-1}} - \ldots -$$

$$- \frac{\Sigma_{k_f}}{\lg \frac{1}{s-1}} \leqq \frac{k_f n_f}{n} - (k_f - 1)\frac{n_f}{n} = \frac{n_f}{n},$$

откуда окончательно:

$$\underline{\lim_{s \to 1}} \frac{\sum p_{s_i}^{-1}}{\lg \frac{1}{s-1}} = \frac{n_f}{n}. \tag{6.39}$$

Эта формула дает искомое выражение для плотности.

10. Можно поставить вопрос также о плотности множества простых идеалов, принадлежащих уже не к классу, а к определенному автоморфизму, и выражение для плотности выиграет в простоте.

Для этого прежде всего заметим, что каждое простое число p, принадлежащее к классу автоморфизма S, всегда содержит простые идеальные множители, принадлежащие к каждому автоморфизму этого класса. Число такого рода простых идеалов, входящих в норму

$$N(\mathfrak{P}) = \mathfrak{P} \cdot \mathfrak{P}^{s_2} \ldots \mathfrak{P}^{s_n} = p^f \tag{6.40}$$

равно порядку нормализатора автоморфизма S. В самом деле, если идеал $\mathfrak{p}$ принадлежит к S, то идеал $\mathfrak{p}^{s_i}$ принадлежит к $S_i^{-1} S S_i$, а равенства

$$S_i^{-1} S S_i = S$$

требует принадлежности S_i к этому нормализатору. С другой стороны, индекс этого нормализатора относительно $\mathfrak{G}$ равен числу различных автоморфизмов класса S, т. е. n_f, откуда порядок нормализатора равен $\frac{n}{n_f}$. Но так как в выражение (6.40) каждый идеал входит f раз, то число различных простых идеальных делителей числа, принадлежащих к автоморфизму S, равно

$$a = \frac{n}{f \cdot n_f}. \tag{6.41}$$

Поэтому, если эти простые идеалы суть

$$\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_a,$$

и если мы подставим в сумму (6.39) вместо p одно из выражений

$$[N(\mathfrak{P}_1)]^{\frac{1}{f}}, [N(\mathfrak{P}_2)]^{\frac{1}{f}}, \ldots [N(\mathfrak{P}_a)]^{\frac{1}{f}},$$

то сумма

$$\sum N(\mathfrak{P})^{-\frac{s}{f}},$$

распространенная на все простые идеалы, принадлежащие к S, в a раз больше суммы, входящей в (6.39). Таким образом мы получим для этой суммы следующее выражение:

$$\lim_{s \to 1} \frac{\sum [N(\mathfrak{P})]^{-\frac{s}{f}}}{\lg \frac{1}{s-1}} = a \frac{n_f}{n} = \frac{1}{f}, \tag{6.42}$$

и мы приходим к теореме:

Теорема 45. *Множество простых идеалов, принадлежащих к автоморфизму S, имеет плотность $\frac{1}{f}$, где f — порядок автоморфизма S или, что то же, степень этих простых идеалов.*

11. В качестве приложения докажем теорему Гильберта о существовании бесчисленного множества простых идеалов с заданной вычетностью. Пусть k — нормальное поле, содержащее l-ые корни из единицы, где l — простое число; α — целое число поля k, $\mathfrak{p}$ — простой идеал, f — его степень, p^f — его норма. Если α не делится на $\mathfrak{P}$, то в силу обобщенной теоремы Ферма

$$\alpha^{p^f - 1} \equiv 1 \pmod{\mathfrak{p}}. \tag{6.43}$$

Из того, что k содержит l-ый корень ζ из единицы, следует, что $p^f - 1$ делится на l. В самом деле, наименьший показатель d, дающий для отдельных чисел β поля k

$$\beta^d \equiv 1 \pmod{\mathfrak{P}},$$

есть всегда делитель $p^f - 1$; но для ζ таким наименьшим показателем является l.

Из сравнения (6.43) следует:

$$\alpha^{\frac{p^f - 1}{l}} \equiv \zeta^c \pmod{\mathfrak{P}}.$$

Корень из единицы ζ^c обозначается символом $\left(\frac{\alpha}{\mathfrak{P}}\right)$, и таким образом

$$\alpha^{\frac{p^f - 1}{l}} \left(\frac{\alpha}{\mathfrak{P}}\right) \pmod{\mathfrak{P}}. \tag{6.44}$$

Для того, чтобы α было сравнимо по модулю $\mathfrak{P}$ с l-ой степенью числа из k (было вычетом l-ой степени), необходимо и достаточно, чтобы имело место

$$\left(\frac{\alpha}{\mathfrak{P}}\right) = 1.$$

Необходимость этого условия очевидна. Достаточность следует из того, что мультипликативная группа вычетов по модулю $\mathfrak{P}$, которые образуют конечное поле порядка p^f, циклическая (см. часть I, теорему 86). В самом деле, элемент циклической группы порядка $p^f - 1$, имеющий порядок $\frac{p^f - 1}{l}$, является l-ой степенью другого элемента.

Рассмотрим поле, полученное присоединением к k величины

$$\beta = \sqrt[l]{\alpha}.$$

Сопряженные с β величины можно представить в таком виде:

$$\beta, \beta\zeta, \beta\zeta^2, \ldots, \beta\zeta^{l-1}.$$

При возведении β в p^f-ую степень она переходит в величину, сравнимую по модулю $\mathfrak{P}$ с сопряженной величиной

$$\beta \left(\frac{\alpha}{\mathfrak{P}}\right).$$

В самом деле,

$$\beta^{p^f} = \beta^{p^f - 1} \cdot \beta = \alpha^{\frac{p^f - 1}{l}} \cdot \beta \equiv \left(\frac{\alpha}{\mathfrak{P}}\right) \beta \pmod{\mathfrak{P}}.$$

Таким образом значение символа $\left(\frac{\alpha}{\mathfrak{P}}\right)$ характеризует принадлежность $\mathfrak{P}$ к определенному автоморфизму относительного поля $k(\beta)/k$.

Теорема Гильберта может быть формулирована так:

Теорема 46. Дано t целых чисел поля k:

$$\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_t,$$

притом так, что произведение

$$\alpha_1^{m_1}\ \alpha_2^{m_2}\ldots\alpha_t^{m_t}$$

может только тогда быть l-ой степенью числа из k, если каждое из чисел $m_1,\ m_2,\ldots,\ m_t$ делится на l. Произвольно задав t l-ых корней из единицы:

$$\zeta^{c_1},\ \zeta^{c_2},\ \ldots,\ \zeta^{c_t},$$

можно найти в k бесчисленное множество простых идеалов $\mathfrak{P}$, удовлетворяющих условиям

$$\left(\frac{\alpha_1}{\mathfrak{P}}\right)=\zeta^{c_1},\ \left(\frac{\alpha_2}{\mathfrak{P}}\right)=\zeta^{c_2},\ldots,\left(\frac{\alpha_t}{\mathfrak{P}}\right)=\zeta^{c_t}.$$

Доказательство. Будем искать $\mathfrak{P}$ среди простых идеалов первой степени ($f=1$); иначе говоря, эти идеалы будут внутри k принадлежать к единичному автоморфизму.

Предварительно докажем, что поле $k(\beta_1,\ \beta_2,\ldots,\beta_t)$ имеет степень l^t относительно k, если

$$\beta_1=\sqrt[l]{\alpha_1},\ \beta_2=\sqrt[l]{\alpha_2},\ldots,\beta_t=\sqrt[l]{\alpha_t}.$$

Если бы эта степень была ниже, то одно из уравнений

$$z^l-\alpha_1=0,\ z^l-\alpha_2=0,\ldots,\ z^l-\alpha_t=0$$

должно было быть приводимым в поле, образованном из k присоединением корней остальных уравнений. В силу нормальности этого уравнения, оно должно распасться на множители одинаковых степеней; но так как l есть простое число, то степени могут быть только первыми.

Поэтому каждый корень этого уравнения рационально выражается через корни остальных уравнений.

Пусть каждое из первых ν уравнений остается неприводимым после присоединения корней остальных уравнений, в то время как $\beta_{\nu+1}$ рационально выражается через $\beta_1,\ \beta_2,\ldots,\beta_\nu$:

$$\beta_{\nu+1}=\varphi(\beta_1,\ \beta_2,\ldots,\beta_\nu). \tag{6.45}$$

Тогда относительная группа поля $k\ (\beta_1,\beta_2,\ldots,\beta_\nu)$ имеет порядок 2^ν и является прямым произведением циклических групп l-го порядка, образованных степенями автоморфизмов

$$\sigma_1=(\beta_1\longrightarrow\zeta\beta_1),\ \sigma_2=(\beta_2\longrightarrow\zeta\beta_2),\ldots,\ \sigma_\nu=(\beta_\nu\longrightarrow\zeta\beta_\nu).$$

Перепишем формулу (6.45) так:

$$\beta_{\nu+1}=\sum_{i=0}^{l-1}\beta_1^{\,i}\ \psi_i(\beta_2,\ldots,\beta_\nu). \tag{6.46}$$

Применим к (6.46) автоморфизм σ_1, переводящий β_1 в $\zeta\beta_1$ и оставляющий остальные β_i на месте. Тогда $\beta_{\nu+1}$ должно перейти в другой корень уравнения

$$z-\alpha^l_{\nu+1}=0;$$

пусть это будет $\zeta^c\beta_{\nu+1}$. Тогда

$$\zeta^c\beta_{\nu+1}=\sum_{i=0}^{l-1}\zeta^i\beta_1^{\,i}\psi_i(\beta_2,\ldots,\beta_\nu),$$

или

$$\beta_{\nu+1}=\sum_{i=0}^{l-1}\zeta^{i-c}\beta_1^{\,i}\psi_i(\beta_2,\ldots,\beta_\nu).$$

Полученное равенство опять подвергнем автоморфизму σ_1, и т. д., и просуммируем полученные формулы. Получим:

$$\beta_{\nu+1}=\beta_1^{\,c}\psi_c(\beta_2,\ldots,\beta_\nu).$$

Поступая аналогично с $\beta_2,\ldots,\beta_\nu$, мы приведем соотношение (6.45) к виду

$$\beta_{\nu+1}=A\,\beta_1^{c_1}\beta_2^{c_2}\ldots\beta_\nu^{c_\nu}\qquad(0\leqq c_i<l).$$

Возведя его в l-ую степень, получим:

$$\alpha_1^{\,-c_1}\alpha_2^{\,-c_2}\ldots\alpha_\nu^{c_\nu}\alpha_{\nu+1}=A^l,$$

что противоречит условиям теоремы.

Таким образом группа Галуа поля $k(\beta_1,\beta_2,\ldots,\beta^t)$ имеет порядок l^t и является прямым произведением циклических групп l-го порядка, образованных степенями автоморфизмов

$$\sigma_1=(\beta_1\longrightarrow\zeta\beta_1),\ \sigma_2=(\beta_2\longrightarrow\zeta\beta_2),\ldots,\ \sigma_t=(\beta_t\longrightarrow\zeta\beta_t),$$

каждый из которых, σ_i, меняет только одну величину, β_i, оставляя остальные на месте. Возьмем автоморфизм

$$\sigma=\sigma_1^{c_1},\ \sigma_2^{c_2}\ldots\sigma_t^{c_t},$$

где показатели $c_1, c_2, \ldots, c_t$ заданы в условии теоремы. В силу теоремы 45 в поле $k(\beta_1, \ldots, \beta_t)$ содержится бесчисленное множество простых идеалов $\mathfrak{P}$, принадлежащих к автоморфизму σ. Для них имеет место

$$\beta_i^p \equiv \zeta^{c_i}\beta_i \pmod{\mathfrak{P}} \quad (i=1, 2, \ldots, t).$$

Преобразуя эти сравнения при помощи любого автоморфизма нашей относительной группы Галуа, мы перейдем к таким же сравнениям по модулю сопряженных с $\mathfrak{P}$ простых идеалов. Все сопряженные с $\mathfrak{P}$ внутри $k(\beta_1, \ldots, \beta_t)$ простые идеалы принадлежат к тому же автоморфизму σ, так как относительная группа абелева. Поэтому все выражения

$$\beta_i^p \equiv \zeta^{c_i}\beta_i,$$

делясь на все сопряженные с $\mathfrak{P}$ внутри $k(\beta_1, \ldots, \beta_t)$ идеалы, делятся и на простой идеал $\mathfrak{P}_1$ поля k, делящийся на $\mathfrak{P}$, и мы получим

$$\beta_i^p \equiv \zeta^{c_i}\beta_i \pmod{\mathfrak{P}} \qquad (i=1,2,\ldots,t),$$

откуда следует

$$\left(\frac{\alpha_1}{\mathfrak{P}_1}\right)=\zeta^{c_1}, \quad \left(\frac{\alpha_2}{\mathfrak{P}_1}\right)=\zeta^{c_2}, \ldots, \left(\frac{\alpha_t}{\mathfrak{P}_1}\right)=\zeta^{c_t},$$

ч. и т. д.

12. Для выражения сумм

$$\Sigma p^{-s},$$

распространенных на простые числа, принадлежащие к определенному классу автоморфизмов, изложенным методом удалось найти главный член

$$\frac{n_f}{n} \lg \frac{1}{s-1},$$

но не удалось оценить остаточного члена. Артин (E. Artin) получил более точную формулу

$$\Sigma p^{-s} = \frac{n_f}{n} \lg \frac{1}{s-1} + P(s-1).$$

Соображения Артина основаны на результатах теории полей классов и в частности на артиновском общем законе взаимности, а потому не могут быть воспроизведены в настоящей части книги.

В следующей части я надеюсь изложить теорию относительно-абелевых полей, в которую входит и теория классов, и связать ее с результатами, полученными в последнее время по теории *алгебр* (или *гиперкомплексных чисел*).

УКАЗАТЕЛЬ ТЕОРЕМ

По теории алгебраических чисел и идеалов на русском языке имеются следующие книги:

Д. А. Граве. Арифметическая теория алгебраических величин. Часть I. Квадратичная область. Киев, 1910 (литогр.).

В. П. Вельмин. Теория алгебраических чисел. Варшава.

Е. Гекке. Теория алгебраических чисел. Харків—Київ, 1934 (укр.).

Главнейшие книги на иностранных языках:

G. Lejeune-Dirichlet (Dedekind). Vorlesungen über Zahlentheorie. 4. Aufl, Braunschweig, 1894.

В последнем дополнении этой книги изложены основы теории идеалов, послужившие началом для развития современной теории алгебраических чисел.

H. Weber. Lehrbuch der Algebra. Bd. 2. 2. Aufl. Braunschweig, 1899.

D. Hilbert. Die Theorie der algebraischen Zahlkörper. Jahresber. D. M. V. 4 1897). Также Ges. Abh. 1, стр. 63—363 („Zahlbericht").

Обширная монография, содержащая почти все результаты того времени и, главным образом, исследования самого Гильберта.

В ней содержатся в частности идеи теорни полей классов. Написана конспективно.

P. Bachmann. Zahlentheorie. Bd. 5. Arithmetik des allgemeinen Zahlkörpers. Lpz., 1905.

Большой курс, содержащий детальную теорию Дедекиндовых модулей.

K. Hensel. Theorie der algebraischen Zahlen. Lpz., 1908.

Оригинальный по идее курс, основанный на разложениях алгебраических чисел в расходящиеся степенные ряды (*p*-адические числа).

R. Fueter. Synthetische Zahlentheorie. Lpz., 1918.

E. Landau. Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale. Lpz. u B., 1918.

Небольшая книга, содержащая краткую теорию идеалов, но главным образом посвященвая деталям аналитической теории идеалов.

E. Hecke. Vorlesungen über die Theorie der algebraischen Zahlen. Lpz. u B., 1923.

Очень изящный курс, построенный на широком употреблении теории абелевых групп, конечных и бесконечных. Содержит вывод известной формулы Гекке.

E. Landau. Vorlesungen über Zahlentheorie. Bd. 3. Aus der algebraischen Zahlentheorie und über die Fermache Vermutung. Lpz., 1927.

Книга, написанная характерной для автора особой конспективной манерой. Содержит исследования А. Туэ о приближении непрерывных дробей к алгебраическим числам с применением к неопределенным уравнениям. Ее большой отдел о теореме Ферма содержал бы все самое важное, если бы автор не избегал теории групп.

Позднейшая теория алгебранческих чисел группирует свои интересы вокруг теории полей классов. В этой области учебников пока нет, но существует несколько фундаментальных обзоров и журнальных статей:

T. Takagi. Über eine Theorie des relativ Abel'schen Zahlkörpers. Journ. Coll. Sc. Tokyo, 41 (1920).

T. Takagi. Über das Reziprozitätsgesetz in einem beliebigen algebraischen Zahlkörper. Journ; Coll. Sc. Tokyo, 44 (1922).

H. Hasse. Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper:

Teil I: Klassenkörpertheorie. Jahresb. DMV, 35 (1926).

Teil Ia: Beweise zu Teil I. Jahresb. DMV, 36 (1927).

Teil II: Reziprozitätsgesetz. Jahresb. DMV, Ergänzungsband 6 (1930).

H. Hasse. Klassenkörpertheorie, 1933 (литогр. курс).

Cl. Chevalley. Sur la théorie du corps de classes dans les corps finis et les corps locaux. Thése, 1934.

Литература к отдельным параграфам:

Глава I

§ 3. Zolotareff. Sur la théorie des nombres complexes. Journ. de math. (3) 6 (1880).

Н. Чеботарев. Новое обоснование теорни идеалов (по Золотареву). Изв. Каз. Ф.-М. О. (31) 1 (1925).

§ 5. N. Tschebotarów. Kurzer Beweis des Diskriminantensatzes. Acta Arithm. 1 (1935).

В наиболее общей формулировке, далеко выходящей за пределы теории алгебраических чисел, доказательство дано у

E. Noether. Der Diskriminantensatz für die Ordnungen eines algebraischen Zahl-oder Funktionenkörpers. Journ. für Math., 157.

§ 7. H. Minkowski. Geometrie der Zahlen. Lpz., 1899.

§ 8. D. Hilbert. „Zahlbericht".

Н. Чеботарев. Доказательство теоремы Kronecker'a-Weber'a относительно абелевых областей. Мат. сб. 31 (1923).

A. Speiser. Die Zerlegungsgruppe. Journ. für Math., 149 (1920).

R. Fueter. Abelsche Körper in quadratisch imaginären Zahlkörpern. Math. Ann., 75 (1914).

§ 10. D. Hilbert. „Zahlbericht".

§ 11. Stickelberger. Verh. des I Int. Math.-Kongr. Zürich, 1897.

G. Voronoï. Verh. des III. Int. Math.-Kongr. Heidelberg, 1904.

§. 12. Mirimanoff. } Journ. für Math. 129.
K. Hensel. }

Глава II

§ 1. I. Schur, Sitzber. Berl. Akadem., 1922.

§ 2. B. L. van der Waerden. Ein logarithmenfreier Beweis des Dirichletschen Einheitssatzes. Abh. Hamb., 6 (1928).

В применении к квадратичным полям см.

Lejeune-Dirichlet. Vorlesungen über Zahlentheorie. 4 Aufl. Braunschweig, 1894.

В применении к кубическим полям:

Г. Вороной. Об одном обобщении алгорифма непрерывных дробей. Варшава, 1896.

§ 3. H. Weber. Lehrbuch der Algebra. Bd. 2. 2. Aufl., Braunschweig, 1899.

§ 3. 11. L. Kronecker. Vorlesungen über Zahlentheorie. Lpz., 1901.

F. Mertens. Dirichlet's Beweis des Satzes, dass... Sitzber. Wiener Akad., 106 (1897).

N. Tschebotarów. Studien über Primzahlendichtigkeiten I, II, Изв. Каз. Ф.-М. О. (3) 2 (1927), 3 (1928).

§ 4. H. Weber. Lehrbuch der Algebra, Bd. 2. 2. Aufl. Braunschweig, 1899.

§ 5. L. Kronecker. Über Irreducibilität von Gleichungen. Monatsber. Berl. Akad., 1880.

G. Frobenius. Über Beziehungen zwischen den Primidealen eines algebraischen Zahlkörpers und den Substitutionen seiner Gruppe. Sitzber. Berl. Akad., 1896.

E. Landau. Verteilung der Primzahlen in den Idealklassen. Math. Ann., 63 (1906).

§ 5. 5. M. Bauer. Arch. der Math. und Physik. (3) 6 (1903).

B. Delaunay. Zur Bestimmung der Zahlkörper durch Kongruenzen; eine Anwendung auf die Abelschen Gleichungen. Journ. für Math. 152.

§ 6. Н. Чеботарев. Определение плотности совокупности простых чисел, принадлежащих к заданному классу подстановок. Изв. Росс. акад. наук, 1923.

N. Tschebotaröw. Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. Math. Ann. 95 (1925).

М. Кравчук. Розподіл первісних чисел по підставленнях групп алгебричного рівняння. ВУАН. 1926.

O. Schreier. Über eine Arbeit von Herrn Tschebotaröw. Abh. Hamburg, 5 (1926).

O. Scholz. Die Abgrenzungssätze für Kreiskörper und Klassenkörper. Sitzber. Berl. Akad., 1931.

M. Deuring. Über den Tschebotareffschen Dichtigkeitssatz. Math. Ann., 110 (1934).

§ 6. 11. D. Hilbert. „Zahlbericht".

N. Tschebotaröw. Der Hilbertsche Satz. BYAH, 1922.

§ 6. 12. E. Artin. Über eine neue Art von L-Reihen. Abh. Hamb., 3 (1923)

E. Artin. Beweis des allgemeinen Reziprozitätsgesetzes. Abh. Hamb., 5 (1927)

УКАЗАТЕЛЬ ТЕРМИНОВ

Здесь указаны страницы книги, на которых приводимые термины упомянуты или разъяснены.

ЗАМЕЧЕННЫЕ ОПЕЧАТКИ

Страница	Строка	Напечатано	Следует читать	По чьей вине
23	5 снизу	$p^{\frac{ri+\nu}{si+1}}$	$p^{\frac{ri+\nu}{si+1}}$	редактор
31	6 сверху	χ	χ_k	„
69	1 „	λ_k	λ	тип.
„	4 „	$(\lambda^\sigma)+k1$	$(\lambda^\sigma)^{k+1}$	„
72	19 снизу	$\mathfrak{P}^{s^\nu}$	$\mathfrak{P}^{s_\nu}$	„
3	7 „	$f_1(a)$	$f_1(\alpha)$	„
73	6 „	$p^{f_1+f_2+\dots+f_k}$	$p^{f_1+f_2+\dots+f_k}$	„
80	12 сверху	$e^{\frac{\pi i}{4}}$	$e^{\frac{\pi i}{4}}$	„
94	7 сверху	$\left[\prod_{i=\nu}^{\mu-1}\tilde{\eta}_{\mu-2}^{(i)}\right]^{q_{\mu-1}}$	$\left[\prod_{i=0}^{\mu-1}\tilde{\eta}_{\mu-2}^{(i)}\right]^{p_{\mu-1}}$	„
112	9 „	$\mathfrak{Z}_l=\mathfrak{Z}_1\times\mathfrak{Z}_2\times\dots\times\mathfrak{Z}_k$	$\mathfrak{A}=\mathfrak{Z}_1\times\mathfrak{Z}_2\times\dots\mathfrak{Z}_k$	редактор
112	10 „	$\mathfrak{A}_l$	$\mathfrak{Z}_l$	тип.
112	11 „	$\mathfrak{A}_l$	$\mathfrak{Z}_l$	„
149	11 „	$\alpha^{\frac{pf-1}{l}}\left(\frac{\alpha}{\mathfrak{P}}\right)$	$\alpha^{\frac{pf-1}{l}}\equiv\left(\frac{\alpha}{\mathfrak{P}}\right)$	„

СОДЕРЖАНИЕ

Ответственный редактор *Н. С. Смирнов* Технический редактор *А. М. Усова*

Сдано в набор 11/V 1937 г. Подписана к печати 22/IX 1937 г.
Формат 60×92. Изд. № 243. Бум. листов 5, печ. листов 10. Тип. зн. в 1 бум. л.
Леноблгорлит № 3439. Тираж 3000. Учет. авт. л. 9,13 Заказ № 1727.

1-я тип. изд-ва Леноблисполкома и Ленсовета. 2-я Советская, 7